REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 20.03.2024	ADOZIONE
Rev. 1	Determina dell'Amministratore Unico del 05.08.2024	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231)

PARTE GENERALE

SOMMARIO

1 PREMESSA E DESCRIZIONE DEL QUADRO NORMATIVO

Con il decreto legislativo 8 giugno 2001, n. 231 ("Decreto" o "D.Lgs. 231/2001"), in attuazione della delega conferita al Governo con l'art. 11 della legge 29 settembre 2000, n. 300 è stata dettata la disciplina della "Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato".

In particolare, tale disciplina si applica agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica.

Il D.Lgs. 231/2001 trova la sua genesi primaria in alcune convenzioni internazionali e comunitarie ratificate dall'Italia che impongono di prevedere forme di responsabilità degli enti collettivi per talune fattispecie di reato.

Secondo la disciplina introdotta dal D.Lgs. 231/2001, infatti, le società possono essere ritenute "responsabili" per alcuni reati ivi indicati commessi o tentati, nell'interesse o a vantaggio delle società stesse, da esponenti di vertice (i c.d. soggetti "in posizione apicale" o semplicemente "apicali") e da coloro che sono sottoposti alla direzione o vigilanza di questi ultimi (art. 5, comma 1, del D.Lgs. 231/2001).

La responsabilità amministrativa delle società è autonoma rispetto alla responsabilità penale della persona fisica che ha commesso il reato e si affianca a quest'ultima.

Il D.Lgs. 231/2001 innova l'ordinamento giuridico italiano in quanto alle società sono ora applicabili, in via diretta e autonoma, sanzioni di natura sia pecuniaria che interdittiva in relazione a reati ascritti a soggetti funzionalmente legati alla società ai sensi dell'art. 5 del Decreto.

La responsabilità amministrativa della società è, tuttavia, esclusa se la società ha, tra l'altro, adottato ed efficacemente attuato, prima della commissione dei reati *de quibus*, modelli di organizzazione, gestione e controllo idonei a prevenire i reati stessi.

La responsabilità amministrativa della società è, in ogni caso, esclusa se i soggetti apicali e/o i loro sottoposti hanno agito nell'interesse esclusivo proprio o di terzi.

In base al D.Lgs. 231/2001, l'ente può essere ritenuto responsabile soltanto per la commissione dei reati espressamente richiamati dal D.Lgs. 231/2001 o da altri provvedimenti normativi ("Reati Presupposto") se commessi nel suo interesse o a suo vantaggio dai soggetti qualificati ex art. 5, comma 1, del Decreto stesso.

Le fattispecie di reato richiamate dal D.Lgs. 231/2001 sono in dettaglio riportate nell'apposito allegato 3 del Modello adottato da GETOPEN.

La Legge 30 novembre 2017, n. 179 recante «Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato» ha aggiunto nel corpo del Decreto una serie di ulteriori prescrizioni (nello specifico, art. 6, commi 2-bis, 2-ter e 2-quater), volte a garantire tutela e protezione a quanti, all'interno dell'ente, segnalino la commissione di condotte illecite potenzialmente rilevanti ai sensi del Decreto (c.d. whistleblowing).

L'approvazione definitiva di tale legge ha segnato una svolta non indifferente per una diffusione più pervasiva dei sistemi interni di segnalazione delle violazioni anche con riguardo al settore privato.

Tale normativa è stata altresì integrata dal d.lgs. 24/2023 di recepimento della direttiva (UE) 2019/1937 (Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.) che ha abrogato alcune disposizioni del d.lgs. n. 231/2001 e della legge n. 179/2017.

IN PARTICOLARE, L'ART. 4 DEL D.LGS. 24/2023 HA PREVISTO CHE:

- i soggetti del settore pubblico e i soggetti del settore privato, debbano attivare un proprio canale di segnalazione, che garantisca, anche tramite il ricorso a strumenti di crittografia,

la riservatezza dell'identità della persona segnalante e della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

- le segnalazioni siano effettuate in forma scritta, anche con modalità informatiche, oppure in forma orale. Le segnalazioni interne in forma orale sono effettuate attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole

GETOPEN ha approvato una procedura interna che disciplina il processo di trasmissione, ricezione, analisi e gestione delle Segnalazioni (cd. Whistleblowing) su informazioni, adeguatamente circostanziate, riferibili al Personale di GETOPEN e/o Terzi relative a violazioni di leggi e regolamenti, del Codice Etico e del Modello Organizzativo 231.

2 ACRONIMI AZIENDALI

AU	Amministratore Unico
RSPP	Responsabile del Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC/RPROG	Responsabile Tecnico/Responsabile Progettazione
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RGAD	Responsabili Gestione Archivi e Documenti
CDL	Consulente del Lavoro
REC	Responsabile Esterno Contabilità

PER L'IDENTIFICAZIONE DEI SOGGETTI CHE CORRISPONDONO AGLI ACRONIMI AZIENDALI SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI GETOPEN S.R.L..

3 PROFILO DELLA SOCIETA'

GetOpen S.r.l. è una azienda che si occupa: **1)** dello svolgimento di studi, ricerche, indagini e fornitura di servizi reali, finalizzati alla progettazione di nuove tecnologie e sistemi integrati per lo sviluppo sostenibile, la mitigazione dell'impatto dei cambiamenti climatici, la riduzione ed il contenimento dei consumi energetici e delle emissioni di inquinanti; **2)** dell'offerta di servizi energetici integrati per la realizzazione e gestione di iniziative di sviluppo sostenibile.

4 ESONERO DELLA RESPONSABILITA' DELL'ENTE

L'art. 6 del D. Lgs. 231/2001 stabilisce che l'ente, nel caso di reati commessi da Soggetti Apicali, non risponda qualora dimostri che:

- l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di proporne l'aggiornamento sia stato affidato ad un Organismo dell'ente dotato di autonomi poteri di iniziativa e controllo (Organismo di Vigilanza);
- le persone hanno commesso il reato eludendo fraudolentemente il suddetto Modello;
- non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Nel caso in cui il reato sia stato commesso da Soggetti Sottoposti, l'ente sarà ritenuto responsabile del reato solamente in ipotesi di carenza colpevole negli obblighi di direzione e vigilanza.

Pertanto, l'ente che, prima della commissione del reato, adotti e dia concreta attuazione ad un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi, va esente da responsabilità se risultano integrate le descritte condizioni di cui all'art. 6 del Decreto.

La mera adozione di un Modello di Organizzazione, tuttavia, non è di per sé sufficiente ad escludere detta responsabilità della Società, risultando necessario che il Modello sia effettivamente ed efficacemente attuato.

IN PARTICOLARE, AI FINI DI UN EFFICACE ATTUAZIONE DEL MODELLO, IL DECRETO RICHIEDE:

- una verifica periodica e l'eventuale modifica dello stesso quando siano emerse significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione o nell'attività;
- la concreta applicazione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso.

5 LE FATTISPECIE DI REATO

I Reati Presupposto sono espressamente enumerati nel D. Lgs. 231/2001. L'ente non può infatti 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 (art. 2).
Si elencano di seguito le "famiglie di reato" ricomprese nel D. Lgs. 231/2001 alla data di approvazione del presente documento, rinviando all'Allegato 1 "Annesso Tecnico al Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001" del presente documento il dettaglio delle singole fattispecie incluse in ciascuna famiglia:

1. Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (Art. 24)

2. Delitti informatici e trattamento illecito di dati (Art. 24-bis)

3. Delitti di criminalità organizzata (Art. 24-ter)

4. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (Art. 25)

5. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-bis)

6. Delitti contro l'industria e il commercio (Art. 25-bis.1)

7. Reati societari (Art. 25-ter)

8. Delitti con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle
leggi speciali (Art. 25-quater)

9. Pratiche di mutilazione degli organi genitali femminili (Art. 25-quater.1)

10. Delitti contro la personalità individuale (Art. 25-quinquies)

11. Reati di abuso di mercato (Art. 25-sexies)

12. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (Art. 25- septies)

13. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25-octies)

14. Delitti in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies.1)

15. Altre fattispecie in materia di strumenti di pagamento diversi dai contanti (Art. 25 octies.1 comma 2)

16. Delitti in materia di violazione del diritto d'autore (Art. 25-novies)

17. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25-decies)

18. Reati ambientali (Art. 25-undecies)

19. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies)

20. Razzismo e xenofobia (Art. 25-terdecies)

21. Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi esercitati a mezzo
di apparecchi vietati (Art. 25-quaterdecies)

22. Reati Tributari (Art. 25-quinquiesdecies)

23. Contrabbando (Art. 25-sexiesdecies)

24. Delitti contro il patrimonio culturale (Art. 25-septiesdecies)

25. Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (Art. 25- duodecies)

26. Reati transnazionali (L.146/2006).

27. Legge n.206 del 27 dicembre 2023 ”Disposizioni organiche per la valorizzazione, la promozione e la tutela del made in Italy” con modifiche all’Art. 517 c.p. (Vendita di prodotti alimentari con segni mendaci) che ha interessato sia l’Art.25-bis.1 (Delitti contro l’industria ed il commercio) del D.Lgs231/01 sia la fattispecie della Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (Art. 12, L. n. 9/2013) facente parte del Modello 231

28. Legge n.6 del 22 Gennaio 2024 “Disposizioni sanzionatorie in materia di distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici e modifiche agli articoli 518-duodecies, 635 e 639 del codice penale” che con le modifiche del testo del comma uno dell’Art.518-duodecies (Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici) ha interessato la fattispecie dei reati previsti dall’Art. 25-septesdecies (Delitti contro il patrimonio culturale) D.Lgs 231/01

29. D.L. n.19 del 2 marzo 2024 coordinato con la Legge di conversione 29 aprile 2024, n. 56 “Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza” che con le modifiche apportate all’Art. 512-bis c.p. (Trasferimento fraudolento di valori) ha interessato la fattispecie dei reati previsti dall’Art. 25-octies.1 (Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori) D.Lgs 231/01

30. D.Lgs n.87 del 14 giugno 2024 “Revisione del sistema sanzionatorio tributario, ai sensi dell'articolo 20 della legge 9 agosto 2023, n. 111” che con le modifiche apportate all’Art.

10-quater del D.Lgs n.74 del 10 marzo 2000 (Indebita compensazione) ha interessato la fattispecie dei reati previsti dall'Art. 25-quinquiesdecies (Reati tributari)

31. Legge n.90 del 28 giugno 2024 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" che ha introdotto, abrogato e modificato articoli del codice penale facenti parte dell'Art. 24 del D.Lgs 231/01 (Indebita percezione di erogazioni, truffa in danno dello stato o di un ente pubblico o dell'Unione Europea per il conseguimento di erogazioni pubbliche e frode informatica in danno dello stato o di un ente pubblico e frode nelle pubbliche forniture) e dell'Art. 24-bis del D.Lgs 231/01 (Delitti informatici e trattamento illecito di dati).

Per quest' ultima fattispecie di reato è stato interamente modificato anche il testo con l'inserimento del comma 1-bis e la modifica dei commi esistenti.

Inoltre, si precisa che il D.L. n. 20 del 10 Marzo 2023 ha introdotto alcune disposizioni urgenti in materia di flussi di ingresso legale dei lavoratori stranieri e di prevenzione e contrasto all'immigrazione irregolare.

Nello specifico: modifica Art. 12, commi 1 e 3 del D.Lgs n. 286/1998 – Disposizioni contro le immigrazioni clandestine; inserimento Art. 12-bis D.Lgs n. 286/1998 – Morte o lesioni come conseguenza di delitti in materia di immigrazione clandestina; modifiche Art. 22 del D.Lgs n. 286/1998 – Impiego di cittadini di paesi terzi il cui soggiorno è irregolare che hanno interessato le fattispecie di reato dell'Art. 25-duodecies "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare".

Mentre, il D.Lgs. n. 19 del 02.03.23 è intervenuto in merito alla "Attuazione della Direttiva (UE) 2019/2021 del Parlamento Europeo e del Consiglio, del 27 Novembre 2019 che modifica la Direttiva (UE) 2017/1132 per quanto riguarda le trasformazioni, le fusioni e le scissioni transfrontaliere".

In particolare, il citato provvedimento normativo ha apportato modifiche al testo dell'Art. 25-ter al comma 1; ha introdotto nell'art. 25-ter, il nuovo comma s-ter relativo al delitto di false o omesse dichiarazioni per il rilascio del certificato preliminare; ha inserito, nell'art. 25-ter, il nuovo reato "False o omesse dichiarazioni per il rilascio del certificato preliminare.

Con la legge n. 137 del 9 ottobre 2023 è stato convertito il d.l. 10 agosto 2023, n. 105, noto come "Decreto Giustizia" o "Decreto Omnibus-bis" e recante disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistratura e della pubblica amministrazione. Tra le plurime novità, l'intervento

legislativo aggiunge un altro tassello all'opera di ampliamento del catalogo dei reati presupposto della responsabilità amministrativa da reato degli enti ex d.lgs. 231/2001, contemplando ora anche i delitti di turbata libertà degli incanti (art. 353 c.p.), turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.) e trasferimento fraudolento di valori (art. 512-bis c.p.).

Ancora, gli emendamenti apportati in sede di conversione hanno mirato, inoltre, a rafforzare gli strumenti di natura penale a tutela dell'ambiente.

In particolare, la Legge di conversione ha previsto la trasformazione da illecito amministrativo a reato contravvenzionale della fattispecie di abbandono di rifiuti di cui all'art. 255 D.Lgs. n. 152/2006.

Un elenco completo dei reati suscettibili di configurare la responsabilità amministrativa della Società è riportato nell'allegato 2 del presente Modello "Reati sanzionati dal Decreto", predisposto ed aggiornato dal componente monocratico dell'Organismo di Vigilanza e pubblicato sul sito web www.getopen.it

6 I REATI COMMESSI ALL'ESTERO

In considerazione delle attività, anche di natura finanziaria, e comunque connesse al core business aziendale, svolte anche all'estero dalla Società e dai propri Dipendenti, risulta opportuno effettuare un richiamo esteso a quanto previsto dall'art. 4 del D. Lgs. 231/2001, e ai principi di territorialità previsti dal Codice penale.

L'ente può infatti essere considerato responsabile, in Italia, per la commissione, in territorio straniero, di taluni reati. In particolare, l'art. 4 del Decreto prevede che gli enti aventi la sede principale nel territorio dello Stato rispondano anche in relazione ai reati commessi all'estero nei casi e alle condizioni previsti dagli articoli da 7 a 10 del Codice penale, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

PERTANTO, L'ENTE È PERSEGUIBILE QUANDO:

- in Italia ha la sede principale, cioè la sede effettiva ove si svolgono le attività amministrative e di direzione, eventualmente anche diversa da quella in cui si trova l'azienda o la sede legale (enti dotati di personalità giuridica);
- nei confronti dell'ente non stia procedendo lo Stato del luogo in cui è stato commesso il fatto;

- la richiesta del Ministro della Giustizia, cui sia eventualmente subordinata la punibilità, sia riferita anche all'ente medesimo.

Tali regole riguardano i reati commessi interamente all'estero da Organi sociali, Soggetti Apicali o Soggetti Sottoposti. Per le condotte criminose che siano avvenute anche solo in parte in Italia, si applica il principio di territorialità ex art. 6 del Codice penale, in forza del quale "*il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione*".

7 ELEMENTI COSTITUTIVI DI ESCLUSIONE DELLA RESPONSABILITA' DELL'ENTE

Elemento costitutivo della responsabilità dell'ente è rappresentato dalla necessità che la condotta illecita ipotizzata sia stata posta in essere "nell'interesse o a vantaggio della società" e non "nell'interesse esclusivo proprio o di terzi".

Secondo la Relazione Ministeriale di accompagnamento al Decreto, la nozione di "interesse" ha fondamento soggettivo, indicando il fine in vista del quale il soggetto ha commesso il reato, mentre il "vantaggio" fa riferimento all'oggettiva acquisizione di un profitto da parte dell'ente.

Il vantaggio si caratterizza invece nei reati dolosi come complesso dei benefici - soprattutto di carattere patrimoniale - tratti dal reato, che può valutarsi successivamente alla commissione di quest'ultimo, anche in termini di risparmio di spesa. La nozione di vantaggio assume una connotazione differente nei reati colposi (reati in materia di salute e sicurezza e reati ambientali) nei quali l'evento lesivo non esprime l'interesse dell'ente e non si traduce in un vantaggio per lo stesso: in tali casi l'interesse o vantaggio dovrebbero piuttosto riferirsi alla condotta inosservante delle norme cautelari (es. nel risparmio di costi per la sicurezza ovvero nel potenziamento della velocità di esecuzione delle prestazioni o nell'incremento della produttività, sacrificando l'adozione di presidi antinfortunistici).

Venendo ai criteri soggettivi di imputazione della responsabilità all'ente per il fatto di reato, appare opportuno sottolineare che la responsabilità della persona giuridica viene ricollegata ad un difetto di organizzazione, consistente nel non avere posto in essere un piano di organizzazione, gestione e controllo idoneo a prevenire la commissione dei reati.

IL DECRETO PREVEDE INFATTI, AGLI ARTICOLI 6 E 7, UNA FORMA DI ESONERO DALLA RESPONSABILITÀ PER L'ENTE QUANDO QUESTO DIMOSTRI:

- di aver adottato ed efficacemente attuato un "Modello di Organizzazione, Gestione e Controllo" idoneo a prevenire la realizzazione dei reati;
- di aver istituito un Organismo di Vigilanza all'interno della società, dotato di completa autonomia di iniziativa e controllo, nonchè con specifici obblighi di vigilanza sul funzionamento, sull'osservanza del Modello e sul suo aggiornamento;
- che le persone che hanno commesso il reato abbiano agito eludendo fraudolentemente il Modello;
- che non vi siano state omissioni o insufficiente vigilanza da parte dell'Organismo di Vigilanza all'uopo preposto.

In particolare, per evitare la responsabilità, la società deve dimostrare l'assenza di colpa organizzativa, cioè che il reato è stato commesso nonostante essa avesse adottato tutte le misure idonee alla prevenzione dei reati ed alla riduzione del rischio di loro commissione.

RESTA INTESO CHE IL MODELLO PER AVERE EFFICACIA ESIMENTE DEVE RISPONDERE ALLE SEGUENTI ESIGENZE:

1. individuare le aree di rischio di commissione dei Reati attraverso un adeguato processo di valutazione dei rischi;
2. predisporre specifici protocolli al fine di programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
3. individuare modalità di gestione delle risorse finanziarie idonee a prevenire la commissione dei Reati;
4. prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;
5. configurare un sistema disciplinare sanzionatorio per la violazione delle norme del codice etico, nonché delle procedure previste dal Modello stesso.

L'adozione del Modello è responsabilità dell'organo dirigente.

Il Decreto prevede che i Modelli possono essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria.

8. I DESTINATARI DEL MODELLO 231/2001 DI GETOPEN

Le regole contenute nel Modello si applicano a coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo nella Società, ai dipendenti di GETOPEN, anche se distaccati all'estero per lo svolgimento dell'attività, nonchè a coloro i quali, pur non appartenendo a GETOPEN, operano su mandato o sono legati a GETOPEN

da contratti rientranti nella c.d. para-subordinazione nonché da contratti di somministrazione.

La Società comunica il presente Modello attraverso le modalità più idonee per l'effettiva conoscenza da parte di tutti i soggetti interessati, i quali devono rispettare puntualmente tutte le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con GETOPEN.

GETOPEN a tal fine organizza attività formative volte a far conoscere il Modello a tutti i soggetti interessati.

GETOPEN condanna qualsiasi comportamento che sia difforme alla legge e alle previsioni del Modello e del Codice Etico, anche qualora il comportamento sia realizzato nell'interesse di società ovvero con l'intenzione di arrecarle vantaggio.

Il modello si applica anche nei confronti dei Business Partners.

9 GLI OBIETTIVI E LA FUNZIONE DEL MODELLO

L'adozione del Modello ha come obiettivo quello di migliorare il proprio sistema di controllo interno, limitando in maniera significativa il rischio di commissione dei reati previsti dalla normativa in oggetto nel rispetto delle disposizioni di cui al D.Lgs. 231/2001 ed è teso a favorire:

• l'individuazione delle attività svolte dalle singole funzioni aziendali che per la loro particolare tipologia, possono comportare un rischio reato ai sensi del D.Lgs. 231/2001;

• l'analisi dei rischi potenziali con riguardo alle possibili modalità attuative dei reati rispetto al contesto operativo interno ed esterno in cui opera la Società;

• la valutazione del sistema dei controlli preventivi ed il suo adeguamento per garantire che il rischio di commissione dei reati sia ridotto ad un "livello accettabile";

• la definizione di un sistema di regole che fissi le linee di comportamento generali (Codice Etico) e specifiche (modelli, sistemi di gestione, linee guida, policy, procedure organizzative e parti speciali) volte a disciplinare le attività aziendali delle aree "sensibili";

• la definizione di un sistema di poteri autorizzativi e di firma che garantisca una puntuale e trasparente rappresentazione del processo aziendale di formazione e di attuazione delle decisioni;

• la definizione di un sistema di controllo in grado di segnalare tempestivamente l'esistenza e l'insorgere di situazioni di criticità generale e/o particolare;

• la definizione di un sistema di comunicazione e formazione per il personale che consenta la conoscibilità del Codice Etico, dei poteri autorizzativi, delle linee di dipendenza gerarchica, delle procedure, dei flussi di informazione e di tutto quanto contribuisce a dare trasparenza all'attività aziendale;

• l'attribuzione ad un Organismo di Vigilanza di specifiche competenze in ordine al controllo dell'effettivo funzionamento, dell'adeguatezza e dell'aggiornamento del Modello;

• la definizione di un sistema sanzionatorio relativo alla violazione delle disposizioni del Codice Etico e delle procedure previste o esplicitamente richiamate dal Modello.

10 LA STRUTTURA DEL MODELLO

Il presente Modello è costituito da una "Parte Generale", da singole "Parti Speciali" e dagli Allegati di seguito citati.

Le Parti Speciali sono state predisposte per alcune categorie di reato previste ai sensi del D.Lgs. 231/2001, laddove siano stati individuati profili di rischio-reato potenziali applicabili a GETOPEN, a seguito dell'identificazione dei processi societari "sensibili".

ATTUALMENTE LE PARTI SPECIALI SONO:

• **PMOG 01:** "Gestione rapporti con la P.A.";

• **PMOG 02:** "Gestione Tesoreria";

• **PMOG 03:** "Prevenzione dei reati societari e redazione ed approvazione del bilancio";

• **PMOG 04:** "Gestione del processo di selezione ed assunzione del personale"

• **PMOG 05:** "Prevenzione dei reati informatici e trattamento illecito di dati"

• **PMOG 06:** "Gestione omaggi e scelta del partner commerciali"

• **PMOG 07:** "Gestione dei contenziosi, accordi transattivi e comunicazioni all'autorità giudiziaria";

• **PMOG 08:** "Attività di prevenzione dei reati in materia di violazione dei diritti d'autore";

• **PMOG 09:** "Gestione attività di prevenzione dei reati ambientali";

• **PMOG 10:** "Gestione dei rischi in materia di salute e sicurezza sui luoghi di lavoro";

• **PMOG 11:** "Gestione attività di prevenzione delitti di criminalità organizzata";

Costituiscono parte integrante del Modello adottato da GETOPEN i seguenti documenti riportati in allegato:

- Il Codice Etico – **Allegato 1**;
- La clausola contrattuale – **Allegato 2**;
- L' elenco dei reati sanzionati dal D.Lgs. 231/01 - **Allegato 3**;

- La Composizione dell'Organismo di Vigilanza - **Allegato 4**;
- Costituzione, compensi, cause di (in)eleggibilità, decadenza e sospensione dei componenti dell'Organismo di Vigilanza - **Allegato 5**;
- Procedura Whistleblowing – **Allegato 6**.

11 MODALITÀ OPERATIVE SEGUITE PER L'IMPLEMENTAZIONE E AGGIORNAMENTO DEL MODELLO

La presente stesura costituisce la prima versione del Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/01, adottato con determina dell'Amministratore Unico di GETOPEN, aggiornato con le novità normative vigenti e, allo stesso tempo, facendo riferimento alla struttura organizzativa e alle attuali attività sensibili gestite dalla Società.
Il Modello è stato predisposto da GETOPEN tenendo presenti, come già anticipato, le prescrizioni del D.Lgs. 231/2001 e s.m.i..
Inoltre, sono state tenute in conto le indicazioni provenienti, fino ad oggi, dalla giurisprudenza in materia.
Sin dalla sua prima adozione, il Modello sarà oggetto di monitoraggio da parte dell'Organismo di Vigilanza pro-
tempore incaricato.

LE MODALITÀ OPERATIVE SEGUITE PER L'IMPLEMENTAZIONE E IL SUCCESSIVO AGGIORNAMENTO DEL MODELLO SONO STATE LE SEGUENTI:

- Mappatura, mediante incontri con il personale interessato, delle aree "sensibili" a rischio 231, identificazione dei profili di rischio potenziale, rilevazione del sistema di controllo interno esistente e Gap Analysis. I risultati di tale attività sono stati formalizzati in un report, che illustrano:

- le aree di rischio (anche dette "attività sensibili") rilevate, intendendosi per tali le attività il cui svolgimento potrebbe dare direttamente adito alla commissione di una delle fattispecie di reato contemplate dal Decreto 231;
- le attività "strumentali", ovvero le aree in cui, in linea di principio, potrebbero configurarsi le condizioni, le occasioni o i mezzi per la commissione dei reati in oggetto;
- il profilo di rischio potenziale (modalità o occasione di possibile commissione del reato);
- i meccanismi di controllo implementati dalla Società, valutandone l'adeguatezza ossia la loro attitudine a prevenire o individuare comportamenti illeciti;
- eventuali suggerimenti per integrare o rafforzare i meccanismi di controllo.

- Adozione del Codice Etico.
- Verifica ed eventuale istituzione e revisione, ove opportuno, del sistema di deleghe e procure.
- Identificazione ed eventuale integrazione del corpo procedurale aziendale con riferimento alle aree a rischio reato e/o strumentali citate.
- Adeguamento del sistema sanzionatorio previgente al fine di renderlo applicabile ed efficace anche con riferimento alle violazioni del Modello.
- Introduzione di specifiche "clausole contrattuali 231" da inserire nelle condizioni generali di contratto, al fine di tutelare GETOPEN e responsabilizzare il terzo.

12 PROCESSI SENSIBILI DI GETOPEN

In ragione della specifica operatività di GETOPEN è stata eseguita una mappatura dei rischi a seguito della quale sono state definite apposite Parti Speciali volte ad evidenziare il sistema di controllo interno a presidio dei suddetti reati.

Ciò posto, sulla base dell'analisi di cui sopra, le aree rilevanti individuate, per le quali sono state identificate idonee regole interne (parti speciali del presente Modello, politiche e procedure) ad integrazione del Codice Etico, sono le seguenti:

AREE RILEVANTI	*REGOLAMENTAZIONE*
GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE	PARTE SPECIALE 01 PARTE SPECIALE 04 PARTE SPECIALE 09
GESTIONE DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO	PARTE SPECIALE 10
GESTIONE DELLE TEMATICHE AMBIENTALI	PARTE SPECIALE 09 PARTE SPECIALE 10
GESTIONE E CONCESSIONE DI OMAGGI E LIBERALITÀ	PARTE SPECIALE 01 PARTE SPECIALE 6 PARTE SPECIALE 11

GESTIONE DEI FINANZIAMENTI (PUBBLICI E NON)	PARTE SPECIALE 01
APPROVVIGIONAMENTO DI BENI E SERVIZI	PARTE SPECIALE 01
GESTIONE DELLA TESORERIA	PARTE SPECIALE 02
GESTIONE DELLA CONTABILITÀ, DEL BILANCIO E DEGLI ADEMPIMENTI FISCALI (INCLUSA L'ARCHIVIAZIONE DEI DOCUMENTI CONTABILI)	PARTE SPECIALE 02 PARTE SPECIALE 03
GESTIONE DELLE OPERAZIONI SOCIETARIE ORDINARIE E STRAORDINARIE	PARTE SPECIALE 02 PARTE SPECIALE 03
GESTIONE DEI RAPPORTI E DEGLI ADEMPIMENTI VERSO SOCI E ORGANISMI DI CONTROLLO	PARTE SPECIALE 02
GESTIONE DELLE RISORSE UMANE	PARTE SPECIALE 04
GESTIONE DEI RIMBORSI SPESE E DELLE SPESE DI RAPPRESENTANZA	PARTE SPECIALE 03 PARTE SPECIALE 05
GESTIONE DEI SISTEMI INFORMATIVI E DELLE RISORSE INFORMATICHE AZIENDALI	PARTE SPECIALE 05

GESTIONE DEL CONTENZIOSO, DEI RAPPORTI CON LE AUTORITÀ GIUDIZIARIE E DEI RAPPORTI CON I SOGGETTI INDAGATI	PARTE SPECIALE 07
DEFINIZIONE E GESTIONE DELLE POLITICHE FISCALI	PARTE SPECIALE 01
GESTIONE DEGLI ASSET AZIENDALI	PARTE SPECIALE 03
GESTIONE ATTIVITA' DI PREVENZIONE DELITTI DI CRIMINALITA' ORGANIZZATA	PARTE SPECIALE 11

13 L'ORGANISMO DI VIGILANZA

In base alle previsioni del D. Lgs. 231/2001 – art. 6, comma 1, lett. a) e b) – la Società non risponde in relazione alla commissione di Reati Presupposto da parte dei soggetti qualificati ex art. 5 del D. Lgs. 231/2001, se l'organo dirigente ha, fra l'altro:

- adottato ed efficacemente attuato prima della commissione del fatto modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati;
- affidato il compito di vigilare sul funzionamento e sull'osservanza del Modello e di curarne l'aggiornamento a un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

L'affidamento dei suddetti compiti a un organismo dotato di autonomi poteri di iniziativa e controllo, unitamente al corretto ed efficace svolgimento degli stessi rappresentano, quindi, presupposti indispensabili per l'esonero dalla responsabilità prevista dal D. Lgs. 231/2001.

In assenza di indicazioni specifiche nel Decreto 231 circa la composizione dell'Organismo di Vigilanza, i relativi requisiti sono stati individuati dalla giurisprudenza, dalla dottrina e dalle Linee Guida di Confindustria e possono essere così identificati:

- **Professionalità:** il complesso di competenze di cui l'Organismo di Vigilanza deve essere dotato per poter svolgere efficacemente la propria attività, consistente in specifiche conoscenze in ambito giuridico, economico, delle tecniche di analisi e di valutazione dei rischi;
- **Autonomia e Indipendenza:** la libertà di iniziativa e l'assenza di qualsivoglia forma di interferenza o condizionamento che provenga dall'interno o dall'esterno dell'ente, avendo anche riguardo alla disponibilità delle risorse necessarie all'effettivo ed efficace svolgimento dell'incarico;
- **Onorabilità:** l'assenza di circostanze che possano minare o condizionare l'integrità dei membri dell'Organismo di Vigilanza compromettendone l'indipendenza e affidabilità;
- **Continuità di azione:** la costante e continuativa attività di controllo e verifica sull'attuazione del Modello 231 in modo da garantirne la reale efficacia.

La Società ha identificato il proprio Organismo di Vigilanza in un organo a composizione monocratico esterno.

13.1 NOMINA E REVOCA

L'OdV è istituito con determina dell'Amministratore Unico e ha la durata di un anno.

In ogni caso, il componente monocratico dell'Organismo rimane in carica fino alla nomina del successore.

La nomina quale componente dell'OdV è condizionata alla presenza dei requisiti soggettivi di onorabilità, indipendenza e professionalità nonché all'assenza di cause di incompatibilità con la nomina stessa.

Il componente monocratico dell'OdV è scelto tra soggetti dotati delle competenze professionali necessarie per l'espletamento delle funzioni.

Il componente monocratico dell'Organismo può ricoprire funzioni o cariche in ambito aziendale, purché queste non comportino a titolo individuale poteri gestionali di amministrazione attiva incompatibili con l'esercizio delle funzioni dell'Organismo.

COSTITUISCONO CAUSE DI INELEGGIBILITÀ O DECADENZA DEI COMPONENTI DELL'ORGANISMO DI VIGILANZA:

- la condanna o l'applicazione della pena su richiesta ex art.444 e ss. c.p.p. con provvedimento anche in primo grado, per uno dei reati previsti dal D. Lgs. 231/2001, o

che per la loro particolare gravità incidano sull'affidabilità morale e professionale del soggetto;

- la condanna, con provvedimento anche di primo grado, a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;
- la condizione giuridica di interdetto, inabilitato o fallito;
- l'applicazione di misure di prevenzione di cui alla Legge 27 dicembre 1956, n.1423 e successive modificazioni e integrazioni; e di misure antimafia di cui alla Legge 31 maggio 1965, n.575 e successive modificazioni e integrazioni.

Il componente monocratico dell'OdV deve dichiarare, sotto la propria responsabilità, di non trovarsi in alcuna delle situazioni di ineleggibilità, o in altra situazione di conflitto di 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 all'Amministratore Unico.

La cessazione della carica è determinata da rinuncia, decadenza, revoca o impedimento permanente e, per quanto riguarda i componenti nominati in ragione della funzione di cui siano titolari in ambito aziendale, dal venir meno della titolarità di questa.

La rinuncia da parte del componente monocratico dell'OdV può essere esercitata in qualsiasi momento e deve essere comunicata all'Amministratore Unico per iscritto, unitamente alle motivazioni che l'hanno determinata.

Ove il componente monocratico dell'Organismo incorra in una delle cause di incompatibilità sopra citate, l'Amministratore Unico della Società, esperiti gli opportuni accertamenti e sentito l'interessato, stabilisce un termine non inferiore a 30 giorni entro il quale deve cessare la situazione di incompatibilità. Trascorso tale termine senza che la predetta situazione sia cessata, l'Amministratore Unico deve revocare il mandato.

La revoca del mandato conferito al componente monocratico dell'Organismo compete all'Amministratore Unico, il quale può revocare per giusta causa, in qualsiasi momento.

PER GIUSTA CAUSA DI REVOCA DEVE INTENDERSI:

a.) l'interdizione o l'inabilitazione, ovvero una grave infermità che renda il componente monocratico dell'Organismo inidoneo a svolgere le proprie funzioni di vigilanza, o un'infermità che, comunque, comporti la sua assenza dal luogo di lavoro per un periodo superiore a sei mesi;

b.) l'attribuzione all'Organismo di funzioni e responsabilità operative incompatibili con i requisiti di autonomia di iniziativa e di controllo, indipendenza e continuità di azione, che sono propri dell'Organismo stesso;

c.) un grave inadempimento dei doveri propri dell'Organismo;

d.) una sentenza di condanna della Società ai sensi del Decreto, passata in giudicato, ovvero un procedimento penale concluso tramite c.d. "patteggiamento", ove risulti dagli atti "l'omessa o insufficiente vigilanza" da parte dell'Organismo, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;

e.) una sentenza di condanna passata in giudicato a carico del componente monocratico dell'Organismo per aver personalmente commesso uno dei reati previsti dal Decreto;

f.) una sentenza di condanna passata in giudicato, a carico del componente monocratico dell'Organismo, ad una pena che importi l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

Nei casi sopra descritti in cui sia stata emessa una sentenza di condanna, l'Amministratore Unico, nelle more del passaggio in giudicato della sentenza, potrà comunque disporre la revoca dei poteri del componente monocratico dell'Organismo.

Nel caso di particolare gravità, anche prima del giudicato, l'Amministratore Unico potrà disporre la sospensione dei poteri dell'Organismo di Vigilanza e la nomina di un componente ad interim.

L'Amministratore Unico è tenuto a nominare il nuovo membro dell'Organismo in sostituzione di quello cui sia stato revocato il mandato entro trenta giorni dalla data di deliberazione di revoca.

Il componente monocratico dell'Organismo potrà recedere in ogni momento dall'incarico mediante preavviso di almeno quattro mesi, da comunicarsi per iscritto, tramite pec, all'Amministratore Unico.

In caso di rinuncia, sopravvenuta incapacità, morte, revoca o decadenza del componente monocratico dell'Organismo di Vigilanza, l'Amministratore Unico provvederà, senza indugio, all'adozione dei più opportuni provvedimenti.

13.2. FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza è dotato di autonomi poteri di iniziativa e di controllo. Ad esso è affidato il compito di vigilare:

• sul funzionamento e sull'osservanza del Modello;

• sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei reati;

• sull'analisi circa il mantenimento nel tempo dei requisiti di solidità e funzionalità del Modello e quindi sull'opportunità di aggiornamento dello stesso, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative.

A TAL FINE, ALL'ORGANISMO DI VIGILANZA SONO ALTRESÌ AFFIDATI I COMPITI DI:

• verificare periodicamente la mappa delle aree a rischio reato al fine di adeguarla ai mutamenti delle attività e/o della struttura aziendale;

• verificare, anche sulla base dell'eventuale integrazione delle aree a rischio, la reale efficacia del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei Reati, proponendo - laddove ritenuto necessario - eventuali aggiornamenti del Modello, con particolare riferimento all'evoluzione e ai mutamenti della struttura organizzativa o dell'operatività aziendale e della normativa vigente;

• effettuare periodicamente verifiche, sulla base di un programma annuale comunicato al Consiglio di Amministrazione, volte all'accertamento di quanto previsto dal Modello; in particolare dovrà verificare che le procedure di controllo siano poste in essere e documentate in maniera conforme e che i principi etici siano rispettati. A tal fine, l'Organismo di Vigilanza è dotato di un generale potere ispettivo e ha libero accesso, senza la necessità di alcun consenso preventivo, salvi i casi in cui tale consenso sia reso necessario da leggi e regolamenti, a tutta la documentazione aziendale, nonchè la possibilità di acquisire dati ed informazioni rilevanti dai soggetti responsabili. Infine, l'Organismo di Vigilanza deve essere costantemente informato dai responsabili delle funzioni aziendali:

- sugli aspetti dell'attività aziendale che possono esporre GETOPEN al rischio di commissione di uno dei reati previsti dalla normativa vigente;
- sui rapporti con i consulenti e con i partner che operano per conto della Società nell'ambito di processi sensibili;
- sulle operazioni straordinarie della Società;

• predisporre semestralmente un rapporto da presentare all'Amministratore Unico al fine evidenziare le problematiche riscontrate ed individuare le azioni correttive da intraprendere;

• coordinarsi con le funzioni aziendali:

- per uno scambio di informazioni al fine di tenere aggiornate le aree a rischio reato;
- per controllare l'evoluzione delle aree a rischio reato al fine di realizzarne il costante monitoraggio;
- per i diversi aspetti attinenti all'attuazione del Modello (definizione di clausole contrattuali standard, formazione del personale, cambiamenti normativi ed organizzativi, ecc.);
- per garantire che le azioni correttive necessarie a rendere il Modello adeguato ed efficace vengano intraprese tempestivamente;

• raccogliere, elaborare e conservare tutte le informazioni rilevanti ricevute sul rispetto del Modello, nonchè aggiornare la lista delle informazioni che allo stesso devono essere trasmesse;

• coordinarsi con il responsabile della Funzione Risorse Umane per la definizione dei programmi di formazione per il personale e del contenuto delle comunicazioni periodiche da farsi ai dipendenti e agli organi sociali, finalizzate a fornire agli stessi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al D.Lgs. 231/2001;

• predisporre ed aggiornare con continuità lo spazio riservato nella rete Intranet della Società contenente tutte le informazioni relative al D.Lgs. 231/2001 e al Modello.

L'Organismo di Vigilanza, qualora emerga che lo stato di attuazione delle procedure operative sia carente, dovrà adottare tutte le iniziative necessarie per correggere questa condizione strutturale. A tal fine dovrà:

• sollecitare i responsabili delle funzioni aziendali al rispetto delle procedure aziendali;

• indicare direttamente quali correzioni e modifiche debbano essere apportate alle procedure aziendali;

• segnalare i casi più gravi di mancata attuazione del Modello ai responsabili delle singole funzioni aziendali.

Qualora, invece, dal monitoraggio dello stato di attuazione del Modello emerga la necessità di adeguamento, risultando peraltro lo stesso integralmente e correttamente attuato ma non idoneo allo scopo di evitare il rischio del verificarsi di taluno dei reati previsti dal D.Lgs.

231/2001, l'Organismo di Vigilanza dovrà attivarsi affinchè siano apportati in tempi brevi i necessari aggiornamenti.

L'autonomia e l'indipendenza, che necessariamente devono connotare le attività dell'Organismo di Vigilanza, rendono necessario prevedere alcune forme di tutela in suo favore al fine di garantire l'efficacia del Modello e di evitare che la sua attività di controllo possa ingenerare forme di ritorsione a suo danno. A tal fine il Consiglio di Amministrazione provvede a mettere a disposizione dell'Organismo di Vigilanza i mezzi, economici e non, che ne consentano la piena operatività.

Per ogni esigenza di ordine finanziario, l'Organismo di Vigilanza, nell'espletamento del proprio mandato, ha la facoltà di richiedere le risorse necessarie all'Amministratore Unico.

13.3. REPORTING DELL'ORGANISMO DI VIGILANZA VERSO IL VERTICE AZIENDALE

L'ORGANISMO DI VIGILANZA HA LA RESPONSABILITÀ NEI CONFRONTI DELL'AMMINISTRATORE UNICO DI:

• comunicare, all'inizio di ciascun esercizio, il piano delle attività che intende svolgere per adempiere ai compiti assegnatigli;

• comunicare periodicamente lo stato di avanzamento del programma definito ed eventuali cambiamenti apportati al piano, motivandoli;

• comunicare immediatamente eventuali problematiche significative scaturite dalle attività nonché dalle eventuali informazioni e segnalazioni ricevute;

• relazionare, almeno annualmente, in merito all'attuazione del Modello, segnalando la necessità di interventi migliorativi e correttivi del medesimo.

L'Organismo di Vigilanza potrà essere invitato a relazionare periodicamente all'Amministratore Unico in merito alle proprie attività.

Nel caso in cui, dagli accertamenti svolti dall'Organismo di Vigilanza, emergessero elementi tali da far risalire la commissione del reato o il tentativo di commissione del reato ad uno o più amministratori, l'Organismo di Vigilanza dovrà riferire tempestivamente all'Amministratore Unico.

L'Organismo di Vigilanza potrà richiedere di essere convocato dai suddetti organi per riferire in merito al funzionamento del Modello o a situazioni specifiche.

L'ORGANISMO DI VIGILANZA POTRÀ, INOLTRE, VALUTANDO LE SINGOLE CIRCOSTANZE:

• comunicare i risultati dei propri accertamenti ai responsabili delle funzioni aziendali qualora dalle attività dagli stessi poste in essere scaturissero aspetti suscettibili di

miglioramento. In tale fattispecie sarà necessario che l'Organismo di Vigilanza ottenga dai responsabili delle funzioni aziendali un piano delle azioni, con relativa tempistica, per le attività suscettibili di miglioramento nonchè le specifiche delle modifiche operative necessarie per realizzare l'implementazione;

• segnalare all'Amministratore Unico eventuali comportamenti/azioni non in linea con il Modello ed il Codice Etico al fine di:

- acquisire tutti gli elementi per effettuare eventuali comunicazioni alle strutture preposte per la valutazione e l'applicazione delle sanzioni disciplinari;
- dare indicazioni per la rimozione delle carenze onde evitare il ripetersi dell'accadimento.

Tali circostanze dovranno essere comunicate dall'Organismo di Vigilanza all'Amministratore Unico, nel più breve tempo possibile, richiedendo anche il supporto delle funzioni aziendali che possono collaborare nell'attività di accertamento e nell'individuazione delle azioni idonee ad impedire il ripetersi di tali circostanze.

13.4. INFORMAZIONI E SEGNALAZIONI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

INFORMAZIONI

In attuazione di quanto stabilito dall'art. 6, comma 2, punto d) del Decreto 231, l'Organismo di Vigilanza deve essere informato, mediante apposite informative da parte dei Destinatari, in merito a fatti aziendali straordinari o comunque rilevanti rispetto ai processi sensibili, ovvero situazioni che potrebbero far insorgere una responsabilità della Società ai sensi del D.Lgs. 231/2001.

Dovranno pertanto essere fornite all'Organismo di Vigilanza le informazioni previste nella procedura aziendale "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01". Tali flussi informativi dovranno essere comunicati inviando una mail all'indirizzo: getopen@getopen.it

Oltre a quanto previsto nella sopra citata procedura, devono in ogni caso essere comunicate all'Organismo di Vigilanza:

• le anomalie e criticità riscontrate dalle funzioni aziendali e dagli organi di controllo concernenti le attività di controllo effettuate, laddove rilevanti ai fini del presente Modello;

• i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si possa venire a conoscenza dello svolgimento di indagini per i reati previsti dal D.Lgs. 231/2001;
• le comunicazioni interne ed esterne riguardanti qualsiasi fattispecie che possa essere messa in collegamento con ipotesi di reato di cui al D.Lgs. 231/2001 (ad es. provvedimenti disciplinari avviati/attuati nei confronti dei dipendenti);
• le richieste di assistenza legale inoltrate dai dirigenti e/o dipendenti nei confronti dei quali la Magistratura procede per i reati previsti dal D.Lgs. 231/2001;
• le notizie relative a cambiamenti nella struttura organizzativa della Società;
• gli aggiornamenti relativi al sistema dei poteri aziendali;
• gli eventuali rilievi della Società di revisione sul sistema dei controlli interni, su fatti censurabili e sui documenti contabili della Società;
• qualsiasi incarico conferito al consulente esterno incaricato della predisposizione e della redazione del bilancio;
• gli eventuali richiami da parte delle Autorità di Vigilanza;
• la struttura organizzativa adottata in materia antinfortunistica e di igiene e salute sul lavoro;
• i documenti di valutazione dei rischi, redatti ai sensi del Testo Unico sulla Sicurezza sul Lavoro (D.Lgs. 81/2008), e i loro eventuali aggiornamenti e modifiche;
• le eventuali ispezioni e prescrizioni effettuate in materia antinfortunistica e di igiene e salute sul lavoro da parte delle Autorità di Vigilanza.

SEGNALAZIONI

GETOPEN supporta e incoraggia le segnalazioni da chiunque in buona fede abbia notizia certa o un ragionevole sospetto, fondato su elementi di fatto precisi e concordanti, che sia avvenuta o che possa avvenire una violazione del Modello o del Codice Etico, nonchè dei regolamenti e delle procedure interne di GETOPEN.
Per la gestione delle segnalazioni, GETOPEN adotta una specifica procedura (cosiddetta procedura “whistleblowing”) che tutti i Destinatari sono tenuti a conoscere ed applicare ove opportuno.
Si rimanda a tale procedura per la descrizione del processo di segnalazione e successiva gestione (fasi di valutazione, indagine, eventuale accertamento della violazione, eventuale definizione del provvedimento sanzionatorio e sua applicazione).

Giova qui ribadire che il principale canale di comunicazione che GETOPEN mette a disposizione per inviare le segnalazioni è la casella di posta elettronica "whistleblowing" [Email: odv@getopen.it]

I soggetti preposti al ricevimento di tali informazioni valutano, sulla base delle informazioni disponibili, che la segnalazione sia effettivamente "rilevante ai fini 231", e in tal caso informano tempestivamente l'Organismo di Vigilanza, demandando ad esso la valutazione. L'identità del segnalante è comunicata solo se e quando strettamente necessaria alla valutazione da parte dell'Organismo.

GETOPEN richiede che le segnalazioni vengano fatte in forma nominativa, impegnandosi a mantenere riservata l'identità del Segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti di GETOPEN o delle persone accusate erroneamente e/o in mala fede. GETOPEN si impegna a tutelare il Segnalante in buona fede contro qualsiasi forma di ritorsione, discriminazione o penalizzazione per motivi collegati, direttamente o indirettamente, alla Segnalazione. Atti di tale natura, diretti o indiretti, nei confronti del segnalante, sono vietati e potranno essere sanzionati secondo quanto previsto dal presente Modello.

Eventuali segnalazioni ricevute in forma anonima non saranno prese in considerazione.

Il Segnalante è responsabile della segnalazione fatta, che dovrà avere i requisiti di cui sopra (e quindi essere circostanziata e fondata su elementi di fatto precisi e concordanti). Sono vietate forme di "abuso" del whistleblowing, con segnalazioni manifestamente opportunistiche e/o effettuate con il solo scopo di danneggiare il Segnalato, e ogni altra ipotesi di utilizzo improprio o strumentale del meccanismo di segnalazione. Atti di tale natura nei confronti del soggetto segnalato sono vietati e potranno essere sanzionati secondo quanto previsto dal presente Modello.

L'Organismo di Vigilanza agirà secondo i principi di confidenzialità, tempestività di investigazione e azione, imparzialità e collegialità.

L'Organismo di Vigilanza dovrà valutare le informazioni ricevute e disporre le necessarie verifiche finalizzate ad accertare se, sulla base degli elementi in proprio possesso, è effettivamente avvenuta una violazione del Modello. Nel caso in cui l'Organismo riscontri una violazione del Modello informerà dell'esito dei suoi accertamenti gli Organi Aziendali competenti, che sono tenuti a dare corso al procedimento di contestazione degli addebiti secondo le procedure definite.

Ogni informazione, segnalazione, report ricevuti dall'Organismo di Vigilanza sono conservati in un apposito archivio (informatico o cartaceo). L'accesso all'archivio è

consentito al solo componente dell'Organismo. L'accesso da parte di soggetti diversi dal componente dell'Organismo deve essere preventivamente autorizzato da quest'ultimo.
Come specificato dalla procedura "whistleblowing", resta valida la possibilità di effettuare segnalazioni in modo verbale o in forma scritta (es. e-mail) direttamente al proprio superiore gerarchico / referente aziendale, nonchè agli organi / alle Funzioni aziendali preposte a specifiche funzioni di controllo.

13.5. VERIFICHE PERIODICHE

Oltre all'attività di vigilanza, che l'Organismo svolge continuamente sull'effettivo funzionamento e sulla corretta osservanza del Modello (e che si traduce nella verifica della coerenza tra i comportamenti concreti dei destinatari ed il Modello stesso), lo stesso periodicamente effettua specifiche verifiche sulla reale capacità del Modello alla prevenzione dei reati (eventualmente, qualora lo ritenga opportuno, coadiuvandosi con soggetti terzi).
Tale attività si può concretizzare in una verifica a campione dei principali atti societari e dei contratti di maggior rilevanza conclusi da GETOPEN in relazione ai processi sensibili e alla conformità degli stessi alle regole di cui al presente Modello.
Inoltre, viene svolta una review di tutte le informazioni e segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dall'Organismo di Vigilanza, degli eventi considerati rischiosi e della consapevolezza degli stakeholders rispetto alla problematica della responsabilità penale dell'impresa con eventuali verifiche a campione.
Le verifiche sono condotte dall'Organismo di Vigilanza che si avvale del supporto di altre funzioni interne che, di volta in volta, si rendano a tal fine necessarie.
Le verifiche e il loro esito sono oggetto di report semestrale all'Amministratore Unico.
In particolare, in caso di esito negativo, l'Organismo di Vigilanza esporrà, nel piano relativo all'anno, i miglioramenti da attuare.
Le verifiche sull'adeguatezza del Modello svolte dall'Organismo di Vigilanza sono concentrate sull'efficacia applicativa dello stesso all'interno degli assetti societari.
E' possibile compiere la verifica svolgendo attività di audit, svolta a campione, dei principali atti societari e dei contratti di maggior rilevanza conclusi dall'ente in relazione ai «processi sensibili» e alla conformità degli stessi a quanto prescritto dal Modello.
Con riferimento alle informazioni e segnalazioni ricevute nel corso dell'anno, alle azioni intraprese dall'Organismo di Vigilanza e dagli altri soggetti interessati, sugli eventi

considerati rischiosi verrà predisposto un report semestrale indirizzato all'Amministratore Unico, come riportato al precedente punto.

L'Organismo di Vigilanza stila con regolare cadenza un programma di vigilanza attraverso il quale pianifica la propria attività di verifica e controllo.

Il programma contiene un calendario delle attività da svolgere nel corso dell'anno prevedendo, altresì, la possibilità di effettuare verifiche e controlli non programmati.

Nello svolgimento della propria attività, l'Organismo di Vigilanza può avvalersi del supporto di funzioni e strutture interne alla Società e/o in outsourcing con specifiche competenze nei settori aziendali di volta in volta sottoposti a controllo.

All'Organismo di Vigilanza sono riconosciuti, nel corso delle verifiche ed ispezioni, i più ampi poteri al fine di svolgere efficacemente i compiti affidatigli come:

• Verificare e segnalare le necessità di modifica del Modello, quando intervengono mutamenti nell'organizzazione aziendale o nel modello di business che rendano il Modello non più aggiornato o che comportino nuovi potenziali "rischi 231".

Il Consiglio di Amministrazione è responsabile dell'aggiornamento del Modello e del suo adeguamento in relazione al mutamento degli assetti organizzativi, dei processi operativi nonchè alle risultanze dei controlli. L'Organismo di Vigilanza conserva, in ogni caso, precisi compiti e poteri in merito alla cura e promozione del costante aggiornamento del Modello.

È inoltre compito dell'Organismo di Vigilanza verificare l'aggiornamento del Modello in seguito al riscontro di carenze e/o lacune a seguito di verifiche sull'efficacia del medesimo.

• Verificare se è stata effettuata un'adeguata formazione e informazione del personale sugli aspetti rilevanti ai fini dell'osservanza della legge nello svolgimento dell'attività dell'organizzazione.

La comunicazione al personale e la sua formazione sono due importanti requisiti del Modello ai fini del suo buon funzionamento. Con riferimento alla comunicazione, essa deve riguardare ovviamente il Codice Etico ma anche gli altri strumenti quali i poteri autorizzativi, le linee di dipendenza gerarchica, le procedure, i flussi di informazione e tutto quanto contribuisca a dare trasparenza nell'operare quotidiano. La comunicazione deve essere: capillare, efficace, autorevole (cioè emessa da un livello adeguato) chiara e dettagliata, periodicamente ripetuta. Accanto alla comunicazione, deve essere sviluppato un adeguato programma di formazione rivolto al personale delle aree a rischio, appropriatamente tarato in funzione dei livelli dei destinatari, che illustri le ragioni di opportunità, oltre che giuridiche, che ispirano le regole e la loro portata concreta.

Verificare se sono state adottate misure materiali, organizzative e protocolli di comportamento atti a garantire lo svolgimento dell'attività nel rispetto della legge ed a scoprire ed eliminare tempestivamente eventuali situazioni irregolari.
Verificare l'attuazione di un idoneo sistema di controllo sull' attuazione del Modello organizzativo e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.
Infatti, il sistema delineato non può, per operare efficacemente, ridursi ad un'attività una tantum, bensì deve tradursi in un processo continuo e costante (o comunque svolto con una periodicità adeguata), da reiterare con particolare attenzione nei momenti di cambiamento aziendale (ampliamento di attività, acquisizioni, riorganizzazioni, ecc.).

14 FORMAZIONE E DIFFUSIONE DEL MODELLO

La Società, al fine di dare efficace attuazione al Modello, assicura l'idonea divulgazione dei contenuti e dei principi dello stesso all'interno e all'esterno della propria organizzazione.
In particolare, obiettivo di GETOPEN è estendere la comunicazione dei contenuti e dei principi del Modello non solo ai propri Dipendenti ma a tutti i Destinatari.
L'attività di comunicazione e formazione è improntata a principi di completezza, chiarezza, accessibilità e continuità al fine di consentire ai diversi Destinatari la piena consapevolezza delle disposizioni aziendali che sono tenuti a rispettare e delle norme etiche che devono ispirare i loro comportamenti.
L'attività di comunicazione e formazione è monitorata dall'OdV, cui sono assegnati, tra gli altri, i compiti di promuovere:
• le iniziative per la diffusione della conoscenza e della comprensione del Modello nonché per la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello;
• gli interventi di comunicazione e formazione sui contenuti del D. Lgs. 231/2001, sugli impatti della normativa sull'attività della Società e sulle norme comportamentali.

14.1 LA COMUNICAZIONE INIZIALE, FORMAZIONE E INFORMAZIONE DEI DIPENDENTI

L'adozione del presente Modello è comunicata a tutte le risorse presenti in azienda al momento dell'adozione stessa e inserita sul portale Intranet aziendale. Tutte le modifiche intervenute successivamente e le informazioni concernenti il Modello sono comunicate attraverso i medesimi canali informativi.

Ai nuovi assunti viene data copia del Modello, del Codice Etico e di tutti i regolamenti aziendali e gli stessi, con la sottoscrizione del contratto di assunzione, dichiarano di averne preso visione e di averli accettati. La Funzione Risorse Umane, inoltre, gestisce l'affiancamento iniziale delle nuove risorse in modo tale da garantire la corretta e completa visione della documentazione. Ai nuovi assunti, viene, altresì, precisata la necessità di prendere visione, periodicamente, dei suddetti documenti anche sul sito internet aziendale, così da verificare eventuali aggiornamenti e revisioni dei medesimi documenti in virtù delle eventuali nuove disposizioni normative in materia.

La formazione costituisce uno strumento imprescindibile per un'efficace implementazione del Modello 231 e per una diffusione capillare dei principi di comportamento e di controllo adottati da GETOPEN, al fine di garantire una ragionevole prevenzione dei reati di cui al Decreto 231.

I REQUISITI CHE LA FORMAZIONE DEVE RISPETTARE SONO I SEGUENTI:

- essere modulata in base ai destinatari e quindi adeguata alla posizione ricoperta e al livello di inquadramento dei soggetti all'interno dell'organizzazione;
- avvenire con periodicità coerente con la frequenza degli aggiornamenti del Modello a seguito delle modifiche normative di cui il Decreto 231 e dei cambiamenti organizzativi;
- essere obbligatoria e prevedere appositi meccanismi di controllo per verificare la presenza dei soggetti e l'apprendimento di ogni singolo partecipante.

In particolare, sono assicurati, per tutti i dipendenti, moduli, attività e progetti formativi sulle tematiche 231 sulla base delle seguenti logiche:

- formazione mirata, specificamente finalizzata all'aggiornamento e al miglioramento delle competenze in materia di Decreto 231 dei ruoli aziendali maggiormente coinvolti e con maggior grado di responsabilità, come definito nell'ambito del Modello 231;
- formazione diffusa rivolta a target molto ampi della popolazione aziendale in maniera tendenzialmente indifferenziata.

Per tutte le iniziative di formazione svolte è assicurata la tracciabilità anche mediante specifici sistemi informatici di rendicontazione.

In linea con quanto disposto dal Decreto 231 e dalle Linee Guida di Confindustria, la Società promuove un'adeguata diffusione del Modello 231, al fine di assicurarne la piena conoscenza da parte dei Destinatari.

IN PARTICOLARE, SI PREVEDE CHE LA COMUNICAZIONE SIA:

- effettuata mediante canali di comunicazione appropriati e facilmente accessibili sia dai dipendenti che dai Soggetti Terzi, quali il portale intranet e il sito internet della Società;
- tempestiva e differenziata, ove necessario, in termini di contenuto in rapporto ai diversi Destinatari.

GETOPEN attua azioni di sensibilizzazione nell'ambito dei rapporti intrattenuti con soggetti terzi, attraverso l'adozione di apposite clausole contrattuali che prevedono l'impegno esplicito di tali soggetti ad operare nel rispetto del Decreto 231 e a tenere un comportamento conforme ai principi e alle regole etico-comportamentali contenuti nel Modello 231, pena, nei casi più gravi, la risoluzione di diritto del contratto ai sensi dell'art. 1456 c.c.

Infine, GETOPEN comunica annualmente agli Stakeholder le informazioni relative alla gestione delle tematiche di responsabilità d'impresa nell'ambito del Bilancio di Sostenibilità.

14.2. INFORMAZIONE AI COLLABORATORI ED AI PARTNER

I consulenti ed i partner devono essere informati del contenuto del Modello e del Codice Etico e dell'esigenza di GETOPEN che il loro comportamento sia conforme ai disposti del D.Lgs. 231/2001.

Al fine di formalizzare l'impegno al rispetto dei principi del Modello e del Codice Etico da parte di terzi aventi rapporti contrattuali con la Società, è previsto l'inserimento nel contratto di riferimento di un'apposita clausola nelle condizioni generali di contratto.

---

15 SISTEMA DISCIPLINARE

Ai fini dell'efficace attuazione del modello di organizzazione, gestione e controllo, il Decreto 231 richiede la predisposizione di un adeguato Sistema Disciplinare (art. 6, comma 2, lett. e) e art. 7, comma 4, lett. b).

Il Sistema Disciplinare adottato da GETOPEN è finalizzato nel suo complesso a garantire il buon funzionamento dell'organizzazione e il regolare svolgimento dell'attività di impresa sanzionando il mancato rispetto dei principi, delle misure e regole comportamentali indicate nel Modello 231 stesso nonché nelle procedure ad esso relative.

In tale prospettiva il Modello 231 rappresenta parte sostanziale ed integrante delle obbligazioni che derivano dal contratto e rapporto di lavoro (per quanto riguarda il lavoro subordinato, anche ai sensi degli artt. 2104 e 2106 c.c.).

L'applicazione delle sanzioni disciplinari prescinde dalla circostanza che il comportamento imputato al lavoratore (sia egli subordinato, in posizione apicale o collaboratore) integri una violazione da cui scaturisca o possa scaturire un procedimento penale e/o l'applicazione di eventuali sanzioni di altra natura.

IL SISTEMA DISCIPLINARE È ADOTTATO DALLA SOCIETÀ IN COERENZA CON I SEGUENTI PRINCIPI:

- **Specificità ed autonomia:** il Sistema Disciplinare adottato da GETOPEN è finalizzato a sanzionare ogni violazione del Modello 231. Il Sistema Disciplinare è, pertanto, autonomo rispetto ad altre eventuali misure sanzionatorie, essendo la Società chiamata a sanzionare la violazione del Modello 231 indipendentemente dall'eventuale instaurazione di un procedimento penale e dall'esito del conseguente giudizio;

- **Compatibilità:** il procedimento di accertamento e di applicazione della sanzione devono essere coerenti con le norme di legge e con le regole contrattuali applicabili al rapporto in essere con la Società;

- **Idoneità:** il sistema dev'essere efficiente ed efficace ai fini della prevenzione del rischio di commissione di comportamenti illeciti, avendo particolare riguardo alle condotte rilevanti ai fini dell'integrazione dei reati presupposto del Decreto 231;

- **Proporzionalità:** la sanzione deve essere proporzionata alla violazione rilevata. La proporzionalità dovrà essere valutata alla stregua di due criteri: **(i)** la gravità della violazione e **(ii)** la tipologia di rapporto di lavoro in essere con il prestatore (subordinato, parasubordinato, dirigenziale, ecc.), tenuto conto della specifica disciplina sussistente sul piano legislativo e contrattuale;

- **Redazione per iscritto e idonea divulgazione:** il Sistema Disciplinare deve essere formalizzato e deve costituire oggetto di informazione e formazione puntuale per tutti i Destinatari.

Il rispetto delle disposizioni presenti nel Modello 231 è richiesto nell'ambito dei contratti di lavoro autonomo, anche coordinati e continuativi e/o etero organizzati e di lavoro subordinato, ferma restando per questi ultimi l'applicazione della disciplina di riferimento per quanto attiene alle sanzioni disciplinari (art. 7 della L. 20 maggio 1970, n. 300 - c.d. "Statuto dei Lavoratori" e CCNL applicabile).

Il procedimento disciplinare è avviato su impulso del Responsabile Risorse Umane o del datore di lavoro o a seguito di comunicazione da parte dell'OdV di inosservanza e/o presunte violazioni del Modello 231 alle funzioni preposte.
Lo svolgimento e la definizione del procedimento disciplinare sono affidati al datore di lavoro o alla Funzione aziendale all'uopo preposta.
Per i Destinatari che sono legati da contratti di natura diversa da un rapporto di lavoro dipendente, le misure applicabili e le procedure disciplinari sono coerenti con la legge e con le relative condizioni contrattuali.
Resta salva la facoltà per la Società di rivalersi per ogni danno e/o responsabilità che alla stessa possano derivare da comportamenti di dipendenti, componenti degli Organi Sociali e Soggetti Terzi in violazione del Modello 231.

15.1. DESTINATARI, LORO DOVERI E CONDOTTE RILEVANTI

I Destinatari hanno l'obbligo di uniformare la propria condotta ai principi e alle regole sancite nel Modello 231.
Ai fini del Sistema Disciplinare, costituisce condotta rilevante per l'applicazione delle sanzioni ogni azione od omissione posta in essere - anche in concorso con altri soggetti – in violazione ai suddetti principi e regole.
In particolare, a mero titolo esemplificativo e oltre quanto previsto dalla regolamentazione aziendale di riferimento e quale specificazione della stessa, costituisce illecito disciplinare:
- l'inosservanza o la violazione delle regole comportamentali previste dal Modello 231;
- l'omissione di segnalazioni all'OdV di violazioni del Modello 231 di cui si abbia avuto conoscenza;
- i comportamenti ritorsivi e/o discriminatori, diretti o indiretti, da parte dei lavoratori nei confronti del soggetto che effettui la segnalazione per motivi collegati, direttamente o indirettamente, alla segnalazione medesima;
- le violazioni delle misure poste a tutela del segnalante con riferimento al diritto di riservatezza;
- l'effettuazione con dolo o colpa grave di segnalazioni che si rivelino infondate.
Ogni comportamento in violazione delle previsioni del Modello 231 rappresenta, se accertato:
- nel caso di dipendenti, un inadempimento contrattuale in relazione alle obbligazioni che derivano dal rapporto di lavoro ai sensi degli artt. 2104 c.c. e 2106 c.c.;

- nel caso di Consiglieri e dell'OdV, l'inosservanza dei doveri loro imposti dall'ordinamento e/o dallo statuto;
- nel caso di Soggetti Terzi, un inadempimento contrattuale tale da legittimare, nei casi più gravi, la risoluzione di diritto del contratto ai sensi dell'art. 1456 c.c., fatta salva la possibilità di agire per ottenere il risarcimento del danno eventualmente subito.

Il procedimento per l'irrogazione delle sanzioni tiene dunque conto delle particolarità derivanti dalla qualifica del soggetto nei cui confronti si procede.

15.2 PRINCIPI GENERALI RELATIVI ALLE SANZIONI

L'applicazione delle sanzioni è ispirata al principio di gradualità e di proporzionalità rispetto alla gravità oggettiva delle violazioni commesse.

La determinazione della gravità della inosservanza o infrazione, oggetto di valutazione per l'individuazione della sanzione applicabile, è improntata al rispetto e alla valutazione di quanto segue:

- l'intenzionalità del comportamento da cui è scaturita l'inosservanza o l'infrazione del Modello 231 o il grado della colpa;
- la negligenza, l'imprudenza o l'imperizia dimostrate dall'autore in sede di commissione dell'inosservanza o l'infrazione, specie in riferimento alla effettiva possibilità di prevedere e/o prevenire l'evento;
- la rilevanza, la gravità e le eventuali conseguenze dell'inosservanza o della infrazione del Modello 231 (misurabili in relazione al livello di rischio cui la Società è esposta e diversificando, quindi, tra comportamenti non conformi e/o violazioni che non hanno comportato esposizione a rischio o hanno comportato modesta esposizione a rischio e violazioni che hanno comportato una apprezzabile o significativa esposizione a rischio, sino alle violazioni che hanno integrato un fatto di rilievo penale);
- la posizione rivestita dal soggetto agente all'interno dell'organizzazione aziendale, specie in considerazione del suo livello di responsabilità gerarchica e/o tecnica;
- eventuali circostanze aggravanti e/o attenuanti che possano essere rilevate in relazione al comportamento tenuto dal soggetto cui è riferibile la condotta contestata, tra le quali si annoverano, a titolo esemplificativo, **(i)** l'eventuale commissione di più violazioni con la medesima condotta (in tal caso, l'aggravamento sarà operato rispetto alla sanzione prevista per la violazione più grave), e **(ii)** la recidiva del soggetto agente);
- il concorso di più Destinatari, in accordo tra loro, nella commissione della violazione;
- altre particolari circostanze che caratterizzano l'infrazione.

L'iter di contestazione dell'infrazione e la comminazione della sanzione sono diversificati sulla base della categoria di appartenenza del soggetto agente.

15.3 SANZIONI DISCIPLINARI

15.3.1 SANZIONI PER I LAVORATORI DIPENDENTI

Le condotte dei lavoratori dipendenti non conformi alle norme comportamentali previste dal Modello costituiscono illeciti disciplinari e, in quanto tali, devono essere sanzionate.

Il lavoratore deve rispettare le disposizioni normative impartite dalla Società, al fine di evitare le sanzioni previste dal vigente Contratto Collettivo Nazionale, divulgate ai sensi e nei modi previsti dall'art. 7 della legge 20 maggio 1970, n. 300 (c.d. "Statuto dei Lavoratori").

La tipologia e l'entità del provvedimento disciplinare saranno individuate tenendo conto della gravità o recidività della mancanza o del grado di colpa e valutando in particolare:

- l'intenzionalità del comportamento o il grado di negligenza, imprudenza o imperizia, anche alla luce della prevedibilità dell'evento;
- il comportamento complessivo del lavoratore, verificando l'esistenza di eventuali altri simili precedenti disciplinari;
- le mansioni assegnate al lavoratore, nonché il relativo livello di responsabilità gerarchica e autonomia;
- l'eventuale condivisione di responsabilità con altri dipendenti che abbiano concorso nel determinare la violazione nonchè la relativa posizione funzionale;
- le particolari circostanze che contornano la violazione o in cui la stessa è maturata;
- la rilevanza degli obblighi violati e la circostanza che le conseguenze della violazione presentino o meno rilevanza esterna all'azienda;
- l'entità del danno derivante alla Società o dall'eventuale applicazione di sanzioni.

I provvedimenti disciplinari vengono applicati non solo in relazione alla gravità delle infrazioni, ma anche in considerazione di eventuali ripetizioni delle stesse; quindi le infrazioni, se ripetute più volte, danno luogo a provvedimenti disciplinari di peso crescente, fino alla eventuale risoluzione del rapporto di lavoro.

Vengono tenuti in considerazione a questo fine i provvedimenti comminati al lavoratore negli ultimi due anni.

I poteri disciplinari per i lavoratori dipendenti – accertamento delle infrazioni, procedimenti disciplinari e applicazione delle sanzioni – verranno esercitati, a norma di legge e di contratto, dal Datore di Lavoro.

Sono previste sanzioni disciplinari nei confronti di chi viola i principi alla base del meccanismo di segnalazione ("c.d. whistleblowing"), volti a tutelare sia il soggetto segnalante, sia il soggetto segnalato. In particolare:

- sanzioni disciplinari nei confronti di chi, essendone responsabile, non mantiene riservata l'identità del segnalante;
- sanzioni disciplinari nei confronti di cui attua o minaccia forme di ritorsione, discriminazione o penalizzazione per motivi collegati, indirettamente o direttamente, alla segnalazione;
- sanzioni disciplinari nei confronti di chi, abusando del maccanismo di whistleblowing, effettua segnalazioni manifestatamente opportunistiche allo scopo di danneggiare il Segnalato, effettuando con dolo o colpa grave segnalazioni che si rivelano infondate, fatta salva l'eventuale accertamento di responsabilità civile (ex art. 2043) o penale (per ipotesi di segnalazione calunniosa o diffamatoria ex codice penale).

***

Si riportano di seguito le correlazioni esistenti tra le mancanze specifiche e le sanzioni disciplinari che saranno applicate in caso di inosservanza, da parte del personale dipendente non dirigente, del Modello adottato dalla Società per prevenire la commissione dei reati previsti dal Decreto 231.

A) RIMPROVERO VERBALE

Nel caso di lieve inosservanza dei principi e delle regole di comportamento previsti dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello, correlandosi detto comportamento ad una "*lieve inosservanza delle norme contrattuali o delle direttive ed istruzioni impartite dalla direzione o dai superiori*".

B) AMMONIZIONI SCRITTE, MULTE E SOSPENSIONI

Incorre nei provvedimenti di ammonizione scritta, multa o sospensione il lavoratore che:

a) non si presenti al lavoro o abbandoni il proprio posto di lavoro senza giustificato motivo oppure non giustifichi l'assenza entro il giorno successivo a quello dell'inizio dell'assenza stessa salvo il caso di impedimento giustificato;

b) senza giustificato motivo ritardi l'inizio del lavoro o lo sospenda o ne anticipi la cessazione;

c) compia lieve insubordinazione nei confronti dei superiori;

d) esegua negligentemente o con voluta lentezza il lavoro affidatogli;

e) per disattenzione o negligenza guasti il materiale dello stabilimento o il materiale in lavorazione;

f) venga trovato in stato di manifesta ubriachezza, durante l'orario di lavoro;

g) fuori dell'azienda compia, per conto terzi, lavoro di pertinenza dell'azienda stessa;

h) contravvenga al divieto di fumare, laddove questo esista e sia indicato con apposito cartello;

i) esegua entro l'officina dell'azienda lavori di lieve entità per conto proprio o di terzi, fuori dell'orario di lavoro e senza sottrazione di materiale dell'azienda, con uso di attrezzature dell'azienda stessa;

l) in altro modo trasgredisca l'osservanza del presente Contratto o commetta qualsiasi mancanza che porti pregiudizio alla disciplina, alla morale, all'igiene ed alla sicurezza dello stabilimento.

L'ammonizione verrà applicata per le mancanze di minor rilievo; la multa e la sospensione per quelle di maggior rilievo.

L'importo delle multe che non costituiscono risarcimento di danni è devoluto alle esistenti istituzioni assistenziali e previdenziali di carattere aziendale o, in mancanza di queste, alla Cassa mutua malattia.

C) LICENZIAMENTO CON PREAVVISO.

In tale provvedimento incorre il lavoratore che commetta infrazioni alla disciplina ed alla diligenza del lavoro che, pur essendo di maggior rilievo di quelle contemplate nell'articolo 9, non siano così gravi da rendere applicabile la sanzione di cui alla lettera b).

A TITOLO INDICATIVO RIENTRANO NELLE INFRAZIONI DI CUI SOPRA:

a) insubordinazione ai superiori;

b) sensibile danneggiamento colposo al materiale dello stabilimento o al materiale di lavorazione;

c) esecuzione senza permesso di lavori nell'azienda per conto proprio o di terzi, di lieve entità senza impiego di materiale dell'azienda;

d) rissa nello stabilimento fuori dei reparti di lavorazione;

e) abbandono del posto di lavoro da parte del personale a cui siano specificatamente affidate mansioni di sorveglianza, custodia, controllo, fuori dei casi previsti al punto e) della seguente lettera b);

f) assenze ingiustificate prolungate oltre 4 giorni consecutivi o assenze ripetute per tre volte in un anno nel giorno seguente alle festività o alle ferie;

g) condanna ad una pena detentiva comminata al lavoratore, con sentenza passata in giudicato, per azione commessa non in connessione con lo svolgimento del rapporto di lavoro, che leda la figura morale del lavoratore;

h) recidiva in qualunque delle mancanze contemplate nell'articolo 9, quando siano stati comminati due provvedimenti di sospensione di cui all'articolo 9, salvo quanto disposto dall'ultimo comma dell'articolo 8.

D) LICENZIAMENTO SENZA PREAVVISO.

In tale provvedimento incorre il lavoratore che provochi all'azienda grave nocumento morale o materiale o che compia, in connessione con lo svolgimento del rapporto di lavoro, azioni che costituiscono delitto a termine di legge.

A titolo indicativo rientrano nelle infrazioni di cui sopra:

a) grave insubordinazione ai superiori;

b) furto nell'azienda;

c) trafugamento di schizzi o di disegni di macchine e di utensili o di altri oggetti, o documenti dell'azienda;

d) danneggiamento volontario al materiale dell'azienda o al materiale di lavorazione;

e) abbandono del posto di lavoro da cui possa derivare pregiudizio alla incolumità delle persone od alla sicurezza degli impianti o comunque compimento di azioni che implichino gli stessi pregiudizi;

f) fumare dove ciò può provocare pregiudizio all'incolumità delle persone od alla sicurezza degli impianti;

g) esecuzione senza permesso di lavori nell'azienda per conto proprio o di terzi, di non lieve entità e/o con l'impiego di materiale dell'azienda;

h) rissa nell'interno dei reparti di lavorazione

15.3.2 SOSPENSIONE CAUTELARE NON DISCIPLINARE

In caso di licenziamento per mancanze di cui al punto D) dell'articolo 10 (senza preavviso), l'azienda potrà disporre la sospensione cautelare non disciplinare del lavoratore con effetto immediato, per un periodo massimo di 6 giorni.

Il datore di lavoro comunicherà per iscritto al lavoratore i fatti rilevanti ai fini del provvedimento e ne esaminerà le eventuali deduzioni contrarie. Ove il licenziamento venga applicato, esso avrà effetto dal momento della disposta sospensione.

15.3.3 MISURE NEI CONFRONTI DEGLI AMMINISTRATORI

In caso di violazione accertata delle disposizioni del Modello, ivi incluse quelle della documentazione che di esso forma parte, da parte di uno o più amministratori, l'Organismo di Vigilanza è tenuto ad informare tempestivamente l'intero Consiglio di Amministrazione, affinchè provvedano ad assumere o promuovere le iniziative più opportune ed adeguate, in relazione alla gravità della violazione rilevata e conformemente ai poteri previsti dalla vigente normativa e dallo Statuto sociale.

In particolare, in caso di violazione delle disposizioni del Modello ad opera di uno o più Amministratori, il Consiglio di Amministrazione ha facoltà di procedere direttamente, in base all'entità e gravità della violazione commessa, all'irrogazione della misura sanzionatoria del richiamo formale scritto ovvero della revoca anche parziale dei poteri delegati e delle procure conferite nei casi più gravi, tali da ledere la fiducia della Società nei confronti del responsabile.

Infine, in caso di violazioni delle disposizioni del Modello ad opera di uno o più Amministratori, dirette in modo univoco ad agevolare o istigare la commissione di un reato rilevante ai sensi del D.Lgs. 231/2001 ovvero a commetterlo, le misure sanzionatorie (quali a mero titolo di esempio, la sospensione temporanea dalla carica e, nei casi più gravi, la revoca dalla stessa) dovranno essere adottate dall'Assemblea dei Soci, su proposta del Consiglio di Amministrazione.

A titolo esemplificativo e non esaustivo, commette una violazione rilevante ai fini del presente paragrafo l'Amministratore che:

• commetta gravi violazioni delle disposizioni del Modello e/o del Codice Etico, ivi inclusa l'omissione o il ritardo nella comunicazione all'Organismo di Vigilanza di informazioni dovute ai sensi del Modello e relative a situazioni non particolarmente a rischio o comunque ponga in essere tali comunicazioni in modo lacunoso o incompleto;

• ometta di vigilare adeguatamente sul comportamento dei dipendenti posti a proprio diretto riporto, al fine di verificare le loro azioni nell'ambito delle aree a rischio reato e, comunque, nello svolgimento di attività strumentali a processi operativi a rischio reato;
• non provveda a segnalare tempestivamente eventuali situazioni di irregolarità o anomalie inerenti il corretto adempimento delle procedure di cui al Modello di cui abbia notizia, tali da compromettere l'efficacia del Modello della Società o determinare un potenziale od attuale pericolo per la Società di irrogazione delle sanzioni di cui al Decreto 231;
• non individui tempestivamente, anche per negligenza o imperizia, eventuali violazioni delle procedure di cui al Modello e non provveda ad intervenire per il rispetto delle procedure e del Modello;
• attui o minacci forme di ritorsione, discriminazione o penalizzazione nei confronti di un dipendente o collaboratore, anche per motivi collegati, indirettamente o direttamente, ad una segnalazione;
• effettui con dolo o colpa grave segnalazioni di possibili violazioni che si rivelino infondate, fatta salva l'eventuale accertamento di responsabilità civile (ex art. 2043) o penale (per ipotesi di segnalazione calunniosa o diffamatoria ex codice penale);
• ponga in essere comportamenti tali da integrare le fattispecie di reato previste dal Decreto 231;
• ponga in essere qualsiasi situazione di conflitto di interessi – anche potenziale - nei confronti della Società o della Pubblica Amministrazione;
• distribuisca omaggi o regali a funzionari pubblici al di fuori di quanto previsto nel Codice Etico o accordi altri vantaggi di qualsiasi natura (ad es. promesse di assunzione);
• effettui prestazioni in favore dei partner che non trovino adeguata giustificazione nel contesto del rapporto costituito con i partner stessi;
• presenti dichiarazioni non veritiere ad organismi pubblici, nazionali e non, al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
• destini somme ricevute da organismi pubblici, nazionali e non, a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli a cui erano destinati;
• riconosca compensi in favore di collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;

• non osservi rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, o non agisca nel rispetto delle procedure interne aziendali che su tali norme si fondano;
• non assicuri il regolare funzionamento della Società e degli organi sociali o non garantisca o non agevoli ogni forma di controllo sulla gestione sociale previsto dalla legge, nonchè la libera e corretta formazione della volontà assembleare;
• non effettui con tempestività, correttezza e buona fede tutte le comunicazioni previste dalle leggi e dai regolamenti nei confronti delle autorità di vigilanza, o ostacoli l'esercizio delle funzioni di vigilanza da queste intraprese;
• assuma un comportamento non corretto o non veritiero con gli organi di stampa e di informazione. Inoltre, rientrano tra le gravi inosservanze l'omessa segnalazione all'Organismo di Vigilanza di qualsiasi violazione alle norme previste dal Modello di cui gli amministratori venissero a conoscenza, nonchè il non aver saputo – per negligenza o imperizia - individuare e conseguentemente eliminare violazioni del Modello e, nei casi più gravi, perpetrazione di reati.
Resta salvo in ogni caso il diritto della Società ad agire per il risarcimento del maggior danno subito a causa del comportamento dell'Amministratore.

15.3.4 MISURE DA ATTUARE NEI CONFRONTI DI COLLABORATORI ESTERNI ALLA SOCIETÀ

Ogni comportamento posto in essere da soggetti esterni a GETOPEN che, in contrasto con il presente Modello, sia suscettibile di comportare il rischio di commissione di uno degli illeciti per i
quali è applicabile il Decreto, determinerà, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di convenzione, la risoluzione anticipata
del rapporto contrattuale, fatta ovviamente salva l'ulteriore riserva di risarcimento qualora da tali comportamenti derivino danni concreti a GETOPEN, come nel caso di applicazione da parte dell'Autorità Giudiziaria delle sanzioni previste dal Decreto.

15.3.5 MISURE NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

Nei casi in cui l'Organismo di Vigilanza, per negligenza ovvero imperizia, non abbia saputo individuare, e, conseguentemente, adoperarsi per eliminare, violazioni del Modello e, nei casi più gravi, perpetrazione di reati, il Consiglio d'Amministrazione procederà agli accertamenti necessari e potrà assumere, a norma di legge e di statuto, gli opportuni

provvedimenti, ivi inclusa la revoca dell'incarico per giusta causa. Per l'approvazione di una delibera di revoca per giusta causa del componente l'Organismo di Vigilanza, è richiesto il voto favorevole di una maggioranza pari ai 2/3 dei membri del Consiglio.
Resta salvo in ogni caso il diritto della Società ad agire per il risarcimento del maggior danno subito a causa del comportamento dell'Organismo di Vigilanza.

15.4 Accertamento delle violazioni e procedimento disciplinare

15.4.1 Valutazione, indagine e accertamento della violazione

Le responsabilità e le modalità di valutazione, indagine e successivo accertamento della violazione sono definite nell'ambito della procedura "whistleblowing", cui si rimanda.

15.4.2 Irrogazione della sanzione a dipendenti (non dirigenti)

I soggetti interessati potranno essere convocati per chiarire i fatti e le situazioni contestate. In ogni caso l'addebito sarà formalizzato e comunicato al/agli interessati, garantendo ad essi la possibilità di opporsi e fornire la propria versione, con un congruo termine di replica in ordine alla propria difesa.
Resta inteso che saranno sempre rispettate le procedure, le disposizioni e le garanzie previste dall'art.7 dello Statuto dei Lavoratori, nonchè dal CCNL Metalmeccanica Industria applicato al personale dipendente di GETOPEN.
Al Responsabile delle Risorse Umane spetta in ogni caso l'attuazione del procedimento disciplinare e l'irrogazione della sanzione, proporzionata alla gravità della violazione commessa ed all'eventuale recidiva.
Nell'irrogazione della sanzione disciplinare sarà rispettato il principio della proporzionalità tra infrazione e sanzione e dovrà tenersi conto di eventuali circostanze attenuanti la gravità del comportamento (attività diretta a rimuovere o impedire le conseguenze dannose, entità del danno o delle conseguenze, etc.) e saranno valutate le circostanze specifiche.
L'esito di ogni procedimento disciplinare, derivante da inadempienze del Modello 231, è comunicato all'Organismo di Vigilanza.
Tutta la documentazione prodotta con riferimento alla rilevazione, accertamento e comunicazione di eventi potenzialmente oggetto di sanzione e alla relativa valutazione da parte del Responsabile di Funzione e del datore di lavoro, nonchè la notifica al dipendente della sanzione e l'eventuale contestazione, sono archiviate presso la Direzione Risorse Umane.

Si applicano le medesime regole e procedure sopra menzionate per quanto riguarda i dipendenti non dirigenti, fatti salvi i richiami normativi non applicabili per legge ai dirigenti.

La sanzione sarà determinata e successivamente irrogata, previa contestazione formale dell'addebito all'interessato, dai soggetti dotati di idonea procura, in forma congiunta.

15.4.3 ACCERTAMENTO DELLA VIOLAZIONE E PROVVEDIMENTI NEI CONFRONTI DI AMMINISTRATORI

Alla notizia di una rilevante inosservanza, da parte di uno o più Amministratori, delle norme previste dal Modello e/o dal Codice Etico o di comportamenti, durante lo svolgimento di attività a rischio ai sensi del Decreto 231, non conformi a quanto prescritto nel Modello stesso, l'Organismo di Vigilanza dovrà tempestivamente informare dell'accaduto l'intero Consiglio di Amministrazione, per l'adozione di ogni più opportuna iniziativa.

Il Consiglio di Amministrazione procederà agli accertamenti necessari e potrà assumere, a norma di legge e di statuto, gli opportuni provvedimenti quali, ad esempio, la convocazione dell'Assemblea dei soci per la revoca del mandato, e/o l'azione sociale di responsabilità ai sensi dell'art. 2393 c.c..

16 AGGIORNAMENTO DEL SISTEMA

Il Decreto 231 espressamente prevede la necessità di aggiornare il Modello d'organizzazione, gestione e controllo, al fine di rendere lo stesso costantemente adeguato alle specifiche esigenze dell'ente e della sua concreta operatività. Gli interventi di adeguamento e/o aggiornamento del Modello saranno realizzati essenzialmente in occasione di:

- innovazioni normative;
- violazioni del Modello e/o rilievi emersi nel corso di verifiche sull'efficacia del medesimo (che potranno anche essere desunti da esperienze riguardanti altre Società);
- modifiche della struttura organizzativa dell'ente, anche derivanti da operazioni di finanza straordinaria ovvero da mutamenti nella strategia d'impresa derivanti da nuovi campi di attività intrapresi.

Segnatamente, l'aggiornamento del Modello e, quindi, la sua integrazione e/o modifica, spetta al medesimo Consiglio di Amministrazione cui il legislatore ha demandato l'onere di adozione del Modello medesimo. La semplice "cura" dell'aggiornamento, ossia la mera

sollecitazione in tal senso e non già la sua diretta attuazione spetta invece all'Organismo di Vigilanza.

17 IL CODICE ETICO

Il Codice Etico e il Modello sono due strumenti complementari e integrati.

Il Codice Etico è stato adottato in via autonoma da GETOPEN con lo scopo di definire i principi di condotta degli affari della Società nonchè gli impegni e le responsabilità dei propri collaboratori; inoltre, tale strumento fornisce agli stessi soggetti informazioni in ordine alla soluzione di problemi di natura etica e commerciale.

Il Modello risponde, invece, a specifiche prescrizioni contenute nel D.Lgs. 231/2001 finalizzate a prevenire la commissione di particolari tipologie di reati.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 20.03.2024	ADOZIONE
Rev. 1	Determina dell'Amministratore Unico del 05.08.2024	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231)

PARTE SPECIALE -1-

SOMMARIO

1 OBIETTIVI E FUNZIONI DEL MODELLO

Gli artt. 24 e 25 del D. Lgs. 231/2001 contemplano una serie di reati previsti dal codice penale accomunati dall'identità del bene giuridico da essi tutelato, individuabile nell'imparzialità e nel buon andamento della Pubblica Amministrazione.

La costante attenzione del legislatore al contrasto della corruzione ha portato a ripetuti interventi in detta materia e nel corso del tempo sono state inasprite le pene e introdotti o, modificati alcuni reati.

Sono state, pertanto, analizzate, le fattispecie di illeciti presupposto per le quali si applica il Decreto e con riferimento a ciascuna categoria dei medesimi sono state identificate in GETOPEN le aree aziendali nell'ambito delle quali sussiste il rischio di commissione dei reati.

Per ciascuna di tali aree si sono quindi individuate le singole attività sensibili e qualificati i principi di controllo e di comportamento cui devono attenersi tutti coloro che vi operano anche nei casi in cui un pubblico ufficiale o un incaricato di pubblico servizio si rechi presso GETOPEN per effettuare accertamenti, ispezioni o verifiche di qualsiasi natura, legislativamente previste. Tra le ispezioni prese in esame nella presente procedura rientrano, a titolo meramente esemplificativo, gli accertamenti e le verifiche di tipo fiscale e tributario, in materia di lavoro, previdenza, igiene e sicurezza sui luoghi di lavoro, tutela dei dati personali, etc.

NELLO SPECIFICO, LA PRESENTE PROCEDURA HA LO SCOPO DI:

a) indicare le procedure che i collaboratori di GETOPEN sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo di Vigilanza, e ai responsabili delle funzioni aziendali che cooperano con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

2 ACRONIMI AZIENDALI

AU Amministratore Unico

RSPP	Responsabile del Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC/RPROG	Responsabile Tecnico
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
CDL	Consulente del Lavoro
REC	Responsabile Esterno Contabilità

PER L'IDENTIFICAZIONE DEI SOGGETTI CHE CORRISPONDONO AGLI ACRONIMI AZIENDALI SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI GETOPEN S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di GETOPEN S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di GETOPEN S.r.l.

4 CAMPO DI APPLICAZIONE RESPONSABILE DELLA PROCEDURA

Rientrano nel campo di applicazione della procedura tutti coloro (compresi i Responsabili di funzione ed i Consulenti esterni all'uopo incaricati) che entrano in contatto per qualsivoglia ragione con la Pubblica Amministrazione, anche nei casi di accertamenti, ispezioni e verifiche.

Tra i Responsabili di funzione ed i Consulenti all'uopo incaricati, rientrano:

1. RSPP (consulente esterno all'uopo incaricato dalla Società) per quanto riguarda le verifiche in materia di igiene e sicurezza sui luoghi di lavoro;
2. L'AU, con il supporto del REC, per quanto riguarda le verifiche in materia di lavoro e previdenza;
3. L'AU, con il supporto del REC, per quanto riguarda le verifiche di tipo fiscale e tributario;
4. L'AU, con il supporto del RAM/RRU e del RTEC, per verifiche in materia di gare.

In occasione delle ispezioni, i soggetti interessati possono avvalersi di professionisti esterni, scelti in relazione alla rilevanza e alle implicazioni giuridiche dell'ispezione, anche al fine di verificare la legittimità della stessa.

Resta inteso, che il responsabile della procedura è l'AU, il quale dovrà essere a conoscenza di tutti i procedimenti.

I relativi verbali dovranno essere sottoscritti dall'Amministratore Unico o dal professionista e/o funzione all'uopo incaricato con apposita delega o autorizzazione scritta.

5 LE TIPOLOGIE DI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (ART. 24 E ART. 25 DEL DECRETO)

Al fine di facilitare una migliore comprensione delle condotte penalmente rilevanti che la presente procedura ha lo scopo preciso di prevenire, di seguito si fornisce una breve descrizione dei reati nei reati nei rapporti con la Pubblica Amministrazione contemplati negli artt. 24 e 25 del D.Lgs. 231/01:

MALVERSAZIONE DI EROGAZIONI PUBBLICHE (ART. 316 -BIS C.P.)

Commette il reato di malversazione a danno dello Stato chiunque estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, destinati alla realizzazione di una o più finalità, non li destina alle finalità previste.

La condotta è costituita dalla destinazione di un bene a fini diversi da quello a cui era finalizzato.

In tal senso si differenzia dalla truffa aggravata, perché mentre qui il bene è conseguito legittimamente ma il suo uso è distorto, nella truffa gli artifici e i raggiri sono funzionali all'ottenimento della cosa, il cui possesso diventa perciò illegittimo.

INDEBITA PERCEZIONE DI EROGAZIONI PUBBLICHE (ART. 316-TER C.P.)

Il reato si configura allorquando, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri,

contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da uno a quattro anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso della sua qualità o dei suoi poteri. La pena è aumentata se il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000. In questa fattispecie, diversamente da quanto accade nel reato di malversazione a danno dello Stato o di altro Ente Pubblico (art. 316-bis c.p.), non ha alcuna rilevanza l'uso che viene fatto delle erogazioni, perfezionandosi il reato con il solo ottenimento degli indebiti finanziamenti.

Tale ipotesi di reato assume natura residuale rispetto alla più grave fattispecie di truffa in danno dello Stato (ex art. 640, comma 2, n. 1 c.p.), per la cui sussistenza è necessaria l'induzione in errore mediante artifici o raggiri.

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

CORRUZIONE PER UN ATTO D'UFFICIO O CONTRARIO AI DOVERI DI UFFICIO (ART. 318 - 319 E ART. 319-BIS C.P.)

L'ipotesi di reato di cui all'art. 318 c.p. si configura nel caso in cui un pubblico ufficiale per compiere

un atto del suo ufficio riceve per sé o per altri in denaro o altra utilità, una retribuzione che non gli è dovuta o ne accetta la promessa.

L'art. 319 c.p. punisce il pubblico ufficiale che, per omettere o ritardare un atto del suo ufficio, ovvero per compiere o aver compiuto un atto contrario ai propri doveri d'ufficio, riceve per sé o per altri denaro o altra utilità o ne accetta la promessa.

L'art. 319-bis c.p. dispone un aumento di pena se il fatto della corruzione ha per oggetto il conferimento di pubblici impieghi, stipendi, pensione o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene.

La condotta del pubblico ufficiale potrà quindi estrinsecarsi nel compimento sia di un atto dovuto sia di un atto contrario ai propri doveri. Tali disposizioni valgono

anche per l'incaricato di un pubblico servizio che rivesta la qualità di pubblico impiegato (art. 320 c.p.), oltre che per le persone indicate nell'art. 322 bis c.p.
Si ritiene opportuno, dal momento che il confine fra corruzione e concussione non è facilmente individuabile, riportare la differenza elaborata dalla giurisprudenza, la quale si fonda sul diverso modo di rapportarsi del privato nei confronti del pubblico ufficiale: nella corruzione il privato e il pubblico ufficiale agiscono su un piano di parità, mentre nella concussione emerge una disparità, in cui il privato subisce le pressioni del pubblico ufficiale.

CORRUZIONE IN ATTI GIUDIZIARI (ART. 319-TER C.P.)

Il reato si configura nel caso in cui i fatti di corruzione, di cui alle fattispecie che precedono, siano commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.
È opportuno evidenziare che nella nozione di Pubblico Ufficiale sono sussumibili, oltre al magistrato, anche altri soggetti quali il cancelliere, i testi e qualsiasi altro funzionario pubblico operante nell'ambito di un contenzioso.

ISTIGAZIONE ALLA CORRUZIONE (ART. 322 C.P.)

Il reato si configura nel caso in cui, nei confronti di un Pubblico Ufficiale o di un Incaricato di Pubblico Servizio, sia formulata la promessa o l'offerta di una somma di denaro o di un'altra utilità, qualora la promessa o l'offerta non siano accettate e riguardino, in via alternativa:
- il compimento di un atto d'ufficio;
- l'omissione o il ritardo di un atto d'ufficio;
- il compimento di un atto contrario ai doveri d'ufficio.

E', inoltre, penalmente sanzionata anche la condotta del Pubblico Ufficiale (o Incaricato di Pubblico Servizio) che solleciti una promessa o dazione di denaro o altra utilità da parte di un privato per le medesime finalità.
È necessario, inoltre, che la promessa di denaro o di altra utilità non siano accettate dal Pubblico Ufficiale, poiché, in caso contrario, deve ritenersi integrata una delle fattispecie di corruzione previste dagli artt. 318 e 319 c.p.

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

APPLICABILITÀ DELL'ARTICOLO 322TER (ART. 640-QUATER C.P. INTRODOTTO DALLA LEGGE N.90 DEL 28 GIUGNO 2024)

TRUFFA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO O DELLE COMUNITÀ EUROPEE (ART.640, COMMA 2, N.1

l'art. 322 ter dispone testualmente che "*Nei casi di cui agli articoli 640, secondo comma, numeri 1 e 2-ter, 640 bis e 640 ter, secondo comma, con esclusione dell'ipotesi in cui il fatto è commesso con abuso della qualità di operatore del sistema, si osservano, in quanto applicabili, le disposizioni contenute nell'articolo 322 ter*".

C.P.) - (ART. 640 MODIFICATO DAL D.LGS.N.75 DEL 14 LUGLIO 2020, DAL D.LGS. 150 DEL 10 OTTOBRE 2022 E DALLA LEGGE N.90 DEL 28 GIUGNO 2024) -.

Il reato si configura qualora, Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno. La pena è aumentata:

1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare;

2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o un'altra circostanza aggravante.

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

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

Il 'profitto' si ravvisa anche nella mancata diminuzione del patrimonio, per effetto, ad esempio, del godimento di un bene e, quindi, anche in assenza di un aumento

effettivo di ricchezza; lo stesso può anche non essere di natura patrimoniale, potendo consistere nel soddisfacimento di un interesse di natura morale.

Con l'ultima modifica apportata dalla Legge n.90 del 28 Giugno 2024 è stato introdotto il comma 2-ter) con cui si è estesa la punibilità anche quando il fatto e' commesso a distanza attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione.

A tal fine, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, è fatto espressamente divieto di fornire alla Pubblica Amministrazione, informazioni non veritiere o anche attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione.

TRUFFA AGGRAVATA PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE (ART. 640-BIS)

Il reato si configura se la truffa riguarda contributi, sovvenzioni, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

FRODE INFORMATICA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (ART. 640-TER C.P.)

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

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

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

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

FRODE NELLE PUBBLICHE FORNITURE (ART. 356 C.P.)

Il reato si configura nel caso in cui, chiunque, commette frode nell'esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo 355 c.p.

TRAFFICO DI INFLUENZE ILLECITE (ART. 346-BIS C.P.)

Il reato si configura nel caso in cui chiunque, fuori dei casi di concorso nei reati di cui agli articoli 318, 319, 319-ter e nei reati di corruzione di cui all'articolo 322-bis, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri.
La stessa pena si applica a chi indebitamente dà o promette denaro o altra utilità.

5.1 CRITERI PER IDENTIFICARE I PUBBLICI UFFICIALI/INCARICATI DI UN PUBBLICO SERVIZIO

PUBBLICO UFFICIALE

Ai sensi dell'art. 357, primo comma, Codice penale, è considerato pubblico ufficiale "agli effetti della legge penale" colui il quale esercita "*una pubblica funzione legislativa, giudiziaria o amministrativa*".
Il secondo comma definisce la nozione di "pubblica funzione amministrativa". Non si è compiuta invece un'analoga attività definitoria per precisare la nozione di "funzione legislativa" e "funzione giudiziaria" in quanto l'individuazione dei soggetti che rispettivamente le esercitano non ha di solito dato luogo a particolari problemi o difficoltà.
Pertanto, il secondo comma dell'articolo in esame precisa che, agli effetti della legge penale "*è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla*

manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi".

In altre parole, è definita pubblica la funzione amministrativa disciplinata da "norme di diritto pubblico", ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Il secondo comma dell'art. 357 c.p. traduce poi in termini normativi alcuni dei principali criteri di massima individuati dalla giurisprudenza e dalla dottrina per differenziare la nozione di "pubblica funzione" da quella di "servizio pubblico".

Pertanto, in via conclusiva, agli effetti della legge penale, è comunemente considerato come pubblico ufficiale qualsiasi soggetto che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi (a titolo esemplificativo, si considerano tali lo Stato, le Regioni, le Province, i Comuni, le istituzioni delle Comunità Europee, i giudici, i notai, i cancellieri, i segretari, ecc.).

INCARICATO DI PUBBLICO SERVIZIO

Ai sensi dell'art. 358 c.p. "*sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio.*

Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata, dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".

Gli incaricati di pubblico servizio sono dunque quei soggetti che, pur agendo nell'ambito di un'attività disciplinata nelle forme della pubblica funzione, mancano dei poteri tipici di questa, purché non svolgano semplici mansioni di ordine, né prestino opera meramente materiale.

Alla stregua della definizione normativa di incaricato di pubblico servizio, si rileva che le società per azioni a partecipazione pubblica nonché le società private che offrono un pubblico servizio, sono considerate a tutti gli effetti incaricati di pubblico

servizio ai fini della legge penale (ad esempio aziende di trasporto, aziende di servizi elettrici, ecc.).

Il "servizio", affinché possa definirsi pubblico, deve essere disciplinato - così come la "pubblica funzione" - da norme di diritto pubblico, tuttavia senza poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

La giurisprudenza ha individuato una serie di "indici rivelatori" del carattere pubblicistico dell'ente, per i quali è emblematica la casistica in tema di società per azioni a partecipazione pubblica.

IN PARTICOLARE, SI FA RIFERIMENTO AI SEGUENTI INDICI:

▪ la sottoposizione ad un'attività di controllo e di indirizzo a fini sociali, nonché ad un potere di nomina e revoca degli amministratori da parte dello Stato o di altri enti pubblici;

▪ la presenza di una convenzione e/o concessione con la pubblica amministrazione;

▪ l'apporto finanziario da parte dello Stato;

▪ la presenza dell'interesse pubblico in seno all'attività economica.

6 AREE DI RISCHIO E SOGGETTI DESTINATARI

I reati di cui sopra trovano il loro presupposto nell'avvenuta instaurazione di un rapporto tra la società e la pubblica amministrazione ed, in particolare con tutti quei soggetti che possono essere qualificati pubblici ufficiali o incaricati di pubblico servizio.

DI CONSEGUENZA LE AREE A RISCHIO CHE, IN RELAZIONE AI CITATI REATI, PRESENTANO MAGGIORE CRITICITÀ SONO:

• la gestione dei rapporti e degli adempimenti verso la Pubblica Amministrazione, quali a titolo esemplificativo:

- ✓ la gestione degli adempimenti in materia tributaria;
- ✓ la gestione del contenzioso giudiziale o amministrativo;
- ✓ la gestione degli adempimenti di legge in materia di trattamenti previdenziali ed assistenziali del personale dipendente;
- ✓ la gestione degli adempimenti in materia di salute, sicurezza, igiene degli impianti e dei luoghi di lavoro;

- ✓ gestione dei rapporti con i funzionari pubblici degli Enti competenti in materia fiscale, sanitaria, di sicurezza pubblica, etc;
- ✓ la gestione dei rapporti con gli altri enti pubblici per l'ottenimento di autorizzazioni, licenze, provvedimenti amministrativi e permessi necessari per l'esercizio delle attività aziendali;
- ✓ le operazioni straordinarie sul capitale sociale e riserva acconto futuro aumento di capitale;
- ✓ la gestione dei rapporti con i funzionari degli enti pubblici competenti nell'ambito dell'espletamento degli adempimenti previsti dalla normativa esistente;
- ✓ partecipazione a gare pubbliche per l'erogazione di servizi nei confronti di Enti Pubblici;

• l'approvvigionamento di beni, servizi e prestazioni;
• l'assegnazione di incarichi di consulenze esterne;
• la gestione dei rapporti con agenti e intermediari;
• la gestione degli investimenti immobiliari e degli acquisti connessi;
• la gestione di incassi e pagamenti e la gestione della tesoreria;
• la gestione dei rimborsi spese a dipendenti e collaboratori;
• la richiesta e la gestione di finanziamenti, con particolare riferimento a quelli pubblici.

Le disposizioni della presente procedura hanno per Destinatari tutti i soggetti coinvolti nei processi sopra identificati affinché gli stessi adottino regole di comportamento conformi a quanto prescritto, al fine di prevenire il verificarsi dei reati ivi considerati.

La presente parte speciale si riferisce a comportamenti posti in essere dai soggetti apicali e da coloro che su specifico incarico intrattengano rapporti con la pubblica amministrazione.

Obiettivo della presente parte speciale è che tutti i destinatari, nella misura in cui gli stessi siano coinvolti nello svolgimento delle attività rientranti nelle Aree a

rischio e in considerazione della diversa posizione e dei diversi obblighi che ciascuno assume nei confronti di GETOPEN, si conformino alle regole di condotta previste nella presente procedura, al fine di prevenire e impedire il verificarsi di reati nei rapporti con la pubblica amministrazione.

IN PARTICOLARE, LA PRESENTE PARTE SPECIALE HA LA FUNZIONE DI:

▪fornire un elenco dei principi generali e dei principi procedurali specifici cui i destinatari, così come sopra individuati, devono attenersi per una corretta applicazione del Modello;

▪fornire all'Organismo di Vigilanza ed all'Amministratore Unico chiamato a collaborare con lo stesso, gli strumenti operativi necessari al fine di esercitare le attività di controllo, monitoraggio e verifica allo stesso demandate.

7 PRINCIPI GENERALI DI COMPORTAMENTO

Come su esposto, la presente procedura si applica in via diretta agli organi sociali, ai soggetti apicali ed ai dipendenti di GETOPEN, mentre si applica in forza di apposite ed eventuali clausole contrattuali ai consulenti, ai fornitori ed ai partner.
Ai suddetti soggetti è fatto divieto di porre in essere, concorrere o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del D.Lgs. 231/2001); sono, altresì, proibite le violazioni ai principi ed alle procedure aziendali indicate nella presente procedura oltre che ai principi contenuti nel Codice Etico.
La presente parte speciale, conformemente a quanto previsto nel Codice Etico, nelle procedure e nelle norme aziendali, prevede a carico dei citati destinatari, sempre in considerazione della loro posizione e dell'esercizio delle loro funzioni, espletate nell'ambito delle Aree a rischio, l'espresso divieto di:

▪porre in essere comportamenti tali da configurare i reati di cui agli artt. 24- 25 del D.Lgs. 231/01;

▪porre in essere condotte che, se anche non costituenti reato, siano considerate ai margini di quanto previsto dalle fattispecie penali;

▪trovarsi in qualsiasi situazione di conflitto di interesse nei confronti della pubblica amministrazione, in relazione a quanto previsto dalle citate ipotesi di reato.

PERCIÒ IN PARTICOLARE È FATTO DIVIETO DI:

▪effettuare elargizioni di denaro a pubblici funzionari, ai loro familiari o a soggetti da loro indicati, che siano in grado d'influenzare l'indipendenza di giudizio o indurre ad assicurare un vantaggio per GETOPEN o per i propri clienti;

▪ distribuire omaggi, regali o prestazioni di qualsiasi natura a rappresentanti della pubblica amministrazione, al di fuori di qualsiasi prassi aziendale (così come specificato nel Codice etico);

▪ effettuare o acconsentire ad elargizioni o promesse di denaro, beni o altra utilità di qualsiasi genere ad esponenti della pubblica amministrazione o a soggetti terzi da questa indicati o che abbiano con questi rapporti diretti o indiretti di qualsiasi natura e/o vincoli di parentela o di affinità. In particolare, non possono essere prese in considerazione, per esempio, contributi elettorali, trattamenti privilegiati provenienti da esponenti della pubblica amministrazione;

▪ effettuare prestazioni che non trovano adeguata giustificazione in relazione all'incarico da svolgere o all'attività propria di GETOPEN;

▪ destinare somme ricevute da organismi pubblici, nazionali o eventualmente comunitari a titolo di erogazione, contributi o finanziamenti agevolati per scopi diversi da quelli a cui erano destinati;

▪ presentare dichiarazioni non veritiere, incomplete o comunque in grado di indurre in errore gli organismi pubblici locali o nazionali;

▪ accedere senza autorizzazione ai sistemi informativi della pubblica amministrazione per ottenere e/o modificare informazioni nell'interesse o a vantaggio di GETOPEN.

DI CONSEGUENZA, AI FINI DELL'ATTUAZIONE DEI COMPORTAMENTI DI CUI SOPRA:

▪ i rapporti con la pubblica amministrazione nelle suddette Aree a rischio devono essere gestiti in modo unitario, procedendo a conferire incarico a uno o più persone determinate eventualmente mediante una delega formale emessa dall'Amministratore Unico;

▪ i contratti pattuiti con società nell'ambito delle Aree a rischio della presente parte speciale devono essere redatti per iscritto con l'indicazione del compenso pattuito o altrimenti indicare i criteri specifici in base ai quali lo stesso viene determinato e devono essere proposti, negoziati, verificati o approvati dall'Amministratore Unico;
▪ gli incarichi conferiti a consulenti esterni devono essere anch'essi redatti per iscritto con l'indicazione del compenso pattuito o altrimenti indicare i criteri specifici in base ai quali lo stesso viene determinato e devono essere proposti, negoziati, verificati o approvati dall'Amministratore Unico di GETOPEN;
▪ nessun tipo di pagamento può essere fatto in contanti o in natura, tranne quelli relativi alla gestione della cassa interna. Dovrà risultare da apposita documentazione la giustificazione della spesa e l'indicazione del destinatario;
▪ le dichiarazioni rese ad organismi pubblici devono essere veritiere, univoche e complete;
▪ coloro che svolgono una funzione di supervisione e/o di controllo su adempimenti connessi alle succitate attività (pagamento di fatture, bonifici in uscita, ecc.) devono porre attenzione sugli adempimenti stessi e riferire tempestivamente all'Organismo di Vigilanza eventuali situazioni di irregolarità o anomalie;
▪ ad ispezioni giudiziarie o da parte di Organismi di Vigilanza e ad attività analoghe devono partecipare i soggetti a ciò espressamente delegati da parte dell'Amministratore Unico. Di tutto il procedimento relativo devono essere redatti appositi verbali da trasmettere in copia all'Organismo di Vigilanza.
Sono fatte salve le procedure di maggiore tutela previste all'interno di GETOPEN per lo svolgimento di attività rientranti nelle Aree a rischio.

7.1 REGOLE PROCEDURALI SPECIFICHE

Si indicano di seguito i principi procedurali che in relazione ad ogni singola situazione delineata nelle Aree a rischio, i destinatari della presente parte speciale sono tenuti a rispettare e che – ove opportuno – devono essere integrati da specifiche procedure aziendali soggette a comunicazione all'Organismo di Vigilanza.

NELL'IPOTESI IN CUI SIANO RISCONTRATE ANOMALIE, IL DESTINATARIO:

▪ informa l'Organismo di Vigilanza dell'operazione a rischio;

▪ tiene a disposizione dello stesso la documentazione;

▪ informa lo stesso dell'avvenuta chiusura dell'operazione.

All'Organismo di Vigilanza è demandato il compito di definire altre forme di comunicazione, nell'ipotesi in cui sia necessario adottare ulteriori cautele.

In ogni caso devono essere rispettati i principi di trasparenza e tracciabilità dell'operazione, la quale può essere oggetto di uno specifico controllo da parte dell'Organismo di Vigilanza.

Infine, lo stesso provvederà, nell'ambito delle proprie relazioni all'Amministratore Unico, a rendere note le operazioni compiute nell'Area a rischio.

7.2 CONTROLLI SPECIFICI

• LIVELLI AUTORIZZATIVI DEFINITI. IN PARTICOLARE:

o i soggetti che esercitano poteri autorizzativi e/o negoziali nei confronti della Pubblica Amministrazione:

▪ sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal responsabile all'uopo delegato o autorizzato;

▪ operano esclusivamente nell'ambito del perimetro di clientela loro assegnato;

o gli atti che impegnano contrattualmente GETOPEN devono essere sottoscritti soltanto da soggetti appositamente incaricati;

o il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale per natura di spesa ed impegno, ivi incluse quelle nei confronti della Pubblica Amministrazione; la normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri.

• SEGREGAZIONE DEI COMPITI TRA I SOGGETTI COINVOLTI NEL PROCESSO DI DEFINIZIONE DELL'ACCORDO CONTRATTUALE CON GLI ENTI PUBBLICI. IN PARTICOLARE:

o le attività di sviluppo commerciale sono svolte principalmente dal RCOM e APVG;

o la definizione dell'accordo è affidata al responsabile all'AU in virtù dell'oggetto del contratto; l'atto formale della stipula del contratto avviene in base al vigente sistema dei poteri e delle deleghe e/o di apposite autorizzazioni scritte;

o i soggetti deputati alla predisposizione della documentazione per la presentazione dell'offerta tecnica ed economica, ovvero per la partecipazione a bandi di gara pubblica, possono essere differenti da coloro che sottoscrivono la stessa.

• ATTIVITÀ DI CONTROLLO:

o la documentazione relativa alla stipula dei rapporti contrattuali è sottoposta per il controllo all'AU che la sottoscrive;

o tutta la documentazione predisposta da GETOPEN per l'accesso a bandi di gara pubblici deve essere verificata, in termini di veridicità e congruità sostanziale e formale, dal responsabile aziendale competente in virtù dell'oggetto del contratto o da soggetti a ciò facoltizzati.

• TRACCIABILITÀ DEL PROCESSO SIA A LIVELLO DI SISTEMA INFORMATIVO SIA IN TERMINI DOCUMENTALI:

o ciascuna fase rilevante degli accordi con la Pubblica Amministrazione deve risultare da apposita documentazione scritta;

o ogni accordo/convenzione/contratto con enti pubblici è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe e/o apposite autorizzazioni scritte in essere;

o al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, il preposto aziendale è responsabile dell'archiviazione e della conservazione della documentazione di competenza, relativa anche alle singole operazioni, prodotta anche in via telematica o elettronica, nonché degli accordi/convenzioni/contratti definitivi, nell'ambito delle attività proprie del processo della stipula di rapporti con la Pubblica Amministrazione.

• in ordine ai sistemi premianti o di incentivazione, pur se attualmente non previsti, qualora venissero effettuati devono essere in grado: di assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente protocollo, nonché con

le previsioni del Codice Etico, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

8 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO

I *Destinatari* devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposto su apposita piattaforma informatica – tutta la documentazione necessaria.

Conclusa l'ispezione, l'AU, o il responsabile della Funzione aziendale interessata, all'uopo incaricata, dovrà inviare una relazione riepilogativa all'OdV.

In ogni caso, il Responsabile della procedura informa, tempestivamente, l'Organismo di Vigilanza sulle ispezioni della Pubblica Amministrazione e sugli adempimenti richiesti alla Società.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse ai Processi Sensibili, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute; infatti, è obbligo per chiunque entri in contatto con la Pubblica Amministrazione in occasione d'ispezioni, accertamenti e verifiche di segnalare, tempestivamente, all'OdV anomalie o fatti straordinari nei rapporti con la Pubblica Amministrazione commessi (o tentati) in violazione nella presente procedura, nonché di eventuali violazioni del Modello e del Codice Etico.

L'ODV DOVRÀ:

▪ controllare i flussi finanziari e la documentazione di GETOPEN, in particolare ponendo attenzione alla fatturazione passiva e alla congruità dei compensi dei collaboratori esterni;

▪ verificare la coerenza delle deleghe verso l'esterno con l'eventuale sistema di deleghe interno;

▪ proporre aggiornamenti o istruzioni scritte relative alla condotta da tenere nelle Aree a rischio come sopra identificate;

▪ svolgere verifiche periodiche in ordine al rispetto delle procedure interne e valutare la loro efficienza nel prevenire i reati;

▪ esaminare le segnalazioni di violazione

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina Amministratore Unico del 20.03.2024	ADOZIONE
Rev. 1	Determina Amministratore Unico del 05.08.2024	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231)

PARTE SPECIALE -2-

SOMMARIO

1 PREMESSA E OBIETTIVI DEL MODELLO

La presente procedura ha l'obiettivo di disciplinare alcune attività di gestione della tesoreria e delle casse a rischio di commissione d'illecito.

In particolare, la presente procedura disciplina tutte quelle attività collegate all'incasso, al pagamento ed alla gestione delle disponibilità liquide presenti presso i conti correnti bancari della società, ai fidi ed ai finanziamenti concessi dal sistema creditizio, nonché la gestione di titoli finanziari e di qualsiasi forma di investimento.

La presente procedura definisce, altresì, l'adeguamento alla riforma delle norme penali in materia di contrasto alle frodi e alle falsificazioni di mezzi di pagamento diversi dai contanti, attuata con il D.Lgs. 8 novembre 2021 n. 184, il D.Lgs. n. 195 dell'8 Novembre 2021 e la Legge n. 238 del 23.12.2021.

Infatti, la citata riforma ha definito i ruoli, le responsabilità operative, le attività di controllo ed i principi di comportamento adottati da GETOPEN S.r.l. nell'ambito del processo di gestione ed utilizzo di sistemi informatici, per le attività a rischio, connesse con la fattispecie di reato prevista dall'art. 25-octies, rubricato "*Delitti in materia di strumenti di pagamento diversi dai contanti*", che ha, dunque, ampliato il catalogo dei reati presupposto 231(ovvero dei reati relativi alla responsabilità amministrativa degli enti in materia di strumenti di pagamento diversi dai contanti, quali l'art. 493-ter e l'art. 493-quater).

In particolare, è stato modificato il reato presupposto 231 di cui all'art. 24 bis D.lgs. n. 231/2001, prevedendo che, con riferimento all'art. 640-ter cod. pen., per l'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale, la sanzione pecuniaria arrivi sino a 500 quote.

Inoltre, è stato previsto un generale inasprimento delle sanzioni qualora si verifichino trasferimenti illeciti di mezzi di pagamento diversi dal contante. Dunque, tali prescrizioni integrano, altresì, i principi di comportamento di cui al Modello e al Codice Etico.

2 ACRONIMI AZIENDALI

AU Amministratore Unico

RAM/RRU Responsabile Amministrazione - Risorse Umane

RCOM/APVG Responsabile Commerciale

RATTR Responsabile Attrezzature e Mezzi

CDL Consulente del Lavoro

REC Responsabile Esterno Contabilità

PER L'IDENTIFICAZIONE DEI SOGGETTI CHE CORRISPONDONO AGLI ACRONIMI AZIENDALI SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI GETOPEN S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di GETOPEN S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di GETOPEN S.r.l..

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

La responsabilità della gestione della presente procedura e della sua applicazione è in particolare del Responsabile Amministrativo.

La presente procedura è applicata dalla Società nei confronti dell'Amministratore Unico, dei Dipendenti, dei Fornitori, del Responsabile Esterno della Contabilità e di tutti Professionisti che, per la natura delle attività svolte, possono incorrere nella commissione di reati ex D.Lgs. 231/01 nel corso dello svolgimento di attività in nome e per conto della Società o da questa promossa nell'ambito della missione assegnata.

In generale, la presente procedura si applica a tutti i *Destinatari* che hanno il potere di ricevere denaro o di eseguire pagamenti in nome e per conto di GETOPEN, nonché di gestire per conto della stessa gli adempimenti di natura fiscale-amministrativo-contabile.

Dunque, il principale responsabile della presente procedura è l'Amministratore Unico.

5 PRINCIPI GENERALI DI COMPORTAMENTO

La presente procedura disciplina l'attività di controllo e di monitoraggio delle risorse economiche e finanziarie, nonché degli incassi e dei pagamenti che vengono gestiti dalle diverse Funzioni Aziendali, nei limiti degli importi che vengono autorizzati e nel rispetto della presente procedura.

I flussi finanziari, ovvero le procedure relative agli incassi ed ai pagamenti sono regolati dalle disposizioni di legge, in modo tale da garantire la tracciabilità di tutte le operazioni di tesoreria, riscontrabili anche presso i principali Istituti di Credito nazionali.

I *Destinatari* della presente procedura:

- ✓ Non dovranno porre in essere comportamenti che possano configurare le fattispecie delittuose di cui all'art. 25 quinquiesdecies del Decreto e, più in generale, di tutte le ipotesi criminali ivi previste;
- ✓ Non dovranno intrattenere rapporti commerciali con soggetti fisici o giuridici dei quali sia conosciuta o anche solo sospettata l'appartenenza ad organizzazioni criminali di qualsiasi tipo;
- ✓ Non dovranno accettare denaro e titoli per importi superiori a quelli previsti dal D.lgs.25 maggio 2017 n. 90 ss.mm.ii., se non tramite intermediari a ciò abilitati, quali Istituti Bancari, gli Istituti di moneta elettronica e Poste Italiane S.p.A;
- ✓ non dovranno accettare denaro e titoli trasferiti attraverso l'utilizzo di dispositivi, materiali o immateriali, o una loro combinazione, diversa dalla moneta a corso legale;
- ✓ Non dovranno porre in essere le condotte aventi ad oggetto mezzi di pagamento digitali attraverso ai quali viene scambiata moneta elettronica

avente corso legale, ma anche le c.d. criptovalute, prive di valore legale, ma sempre più accettate come mezzi di pagamento;

- ✓ Non dovranno adottare comportamenti finalizzati a trarre profitto per sé e per gli altri acquistando, ricevendo od occultando danaro o cose provenienti da un qualsiasi delitto, o comunque intromettendosi nel farli acquistare, ricevere od occultare;
- ✓ Non dovranno sostituire o trasferire denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compiere operazioni tese ad ostacolare l'identificazione della loro provenienza delittuosa;
- ✓ Non dovranno impiegare in attività economiche o finanziarie di denaro, beni o altre utilità provenienti dai casi di cui agli artt. 648 e 648 bis c.p;
- ✓ Non dovranno impiegare, sostituire, trasferire in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di un delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa;
- ✓ Non dovranno porre in essere una condotta che abbia, anche solo, creato intralcio non definitivo, ma concreto, rispetto all'identificazione della provenienza delittuosa del bene;
- ✓ Non dovranno commettere negozi simulati riguardanti non solo denaro contante su un conto corrente o beni immobili, ma beni della più diversa natura, quali a titolo esemplificativo la cessione di quote o azioni eseguita al fine di estraniarsi dalla compagine della società solo apparentemente, poiché chi si è spogliato formalmente della titolarità delle quote o azioni continua di fatto a determinarne l'attività come amministratore o socio occulto ed a partecipare alla gestione e agli utili derivanti dall'attività imprenditoriale;
- ✓ Non dovranno attribuire, fittiziamente, ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la

commissione di uno dei delitti di ricettazione, riciclaggio e impiego di denaro o beni di provenienza illecita (di cui agli artt. 648, 648-bis e 648-ter c.p.).

5.1 LA GESTIONE DEI PAGAMENTI

La Funzione Aziendale autorizzata ad effettuare il pagamento è tenuta al rispetto delle fasi qui di seguito riportate:

1. Il RAM deve predisporre un piano di pagamenti mensile, che verrà condiviso in una piattaforma digitale (ad es. TEAMS o simili) e che dovrà essere validato, con firma digitale o con firma olografa, dall'A.U.;
2. per il pagamento dei dipendenti, è necessario acquisire, prima di eseguire il pagamento, il documento giustificativo della spesa (come ad esempio le buste paga, i giustificativi per rimborso spese, *etc.*), validato da una diversa Funzione Aziendale;
3. il pagamento delle prestazioni di consulenza e della fornitura richiede l'attuazione dei seguenti presidi:
   - il pregresso inserimento nella anagrafica del gestionale;
   - la regolare emissione della fattura;
   - l'effettiva esecuzione della prestazione per la quale si richiede o si effettua il pagamento, mentre nel caso di forniture di merci, di materiale, di beni strumentali, la funzione incaricata dovrà verificare e confermare l'avvenuta consegna dei beni);
   - la corrispondenza tra il pagamento effettuato ed il corrispettivo indicato nel contratto o in eventuali preventivi.
4. I pagamenti superiori ad € 15.000,00 giornalieri, dovranno essere, previamente autorizzati, per iscritto, dall'A.U. e dovranno essere indicati nello specifico *report* semestrale che dovrà essere trasmesso all'OdV.

   Infatti, in ordine alla predetta autorizzazione, si precisa che il RAM inserirà, nel piano di pagamenti mensile, un'apposita voce e, precisamente "*pagamenti superiori ad € 15.000,00*", in modo tale che l'Amministratore Unico possa

autorizzare, con firma digitale o con firma olografa, i pagamenti effettuati oltre la soglia "*ordinaria*";

5. non sono ammessi pagamenti in contanti, oltre a quanto previsto dalla normativa vigente ed, in ogni caso, non sono ammessi pagamenti in contanti per importi superiori ad euro 500,00 giornalieri;
6. in caso di tenuta di contabilità esterna, il professionista terzo è tenuto a segnalare all'OdV i pagamenti effettuati in carenza di documentazione giustificativa.

5.2. REATI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E GESTIONE DEI PAGAMENTI

Il Decreto legislativo 184/2021 ha introdotto nel catalogo dei reati presupposto della responsabilità dell'ente i delitti in materia di strumenti di pagamento diversi dai contanti inserendo: **1)** l'aggravante di cui all'art. 640 ter, comma 2, c.p., le modifiche all'art. 493 ter c.p. e, ex novo, l'art. 493 quater c.p. Caratteristiche e contesto di detti reati fanno sì che gli stessi possano essere ricondotti nell'Area sensibile dei reati informatici fermo che, anche in questo caso, le attività sensibili previste in quest'area, ricomprendente reati che possono generare proventi illeciti, si devono intendere predisposte anche al fine della prevenzione dei reati di riciclaggio in senso lato.

SI ILLUSTRANO DI SEGUITO I REATI INTRODOTTI DALL'ART. 25.OCTIES.1:

FRODE INFORMATICA CHE PRODUCE TRASFERIMENTO DI DENARO, DI VALORE MONETARIO O DI VALUTA VIRTUALE (ART. 640 TER, COMMA 2).

La fattispecie consiste nell'alterare il funzionamento di un sistema informatico o telematico o nell'intervenire senza diritto sui dati, informazioni o programmi in essi contenuti, ottenendo un ingiusto profitto. La circostanza aggravante che il fatto produca un trasferimento di denaro, di valore monetario o di valuta virtuale determina anche la responsabilità dell'Ente senza bisogno che il soggetto passivo sia lo Stato, la Pubblica Amministrazione o l'UE.

INDEBITO UTILIZZO E FALSIFICAZIONE DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (493 TER C.P.)

La fattispecie punisce la condotta di chi, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti. Viene punita anche la condotta di chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. Il rischio di commissione di tale reato può in teoria configurarsi in tutte le realtà aziendali ed in particolare in tutti i processi aziendali interessati dalla movimentazione di flussi finanziari, in relazione alle differenti tipologie di strumenti di pagamento diverse dai contanti. In particolare, sono sensibili tutte le attività che rendono possibile l'accesso a dati identificativi, credenziali, etc., funzionali all'eventuale utilizzo indebito di strumenti di pagamento (diversi dai contanti) di titolarità di terzi, quali ad esempio le carte di credito.

DETENZIONE E DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A COMMETTERE REATI RIGUARDANTI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART. 493 QUATER C.P.)

Salvo che il fatto costituisca più grave reato, la fattispecie punisce chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a se' o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo. La condotta descritta potrebbe riscontrarsi nell'ambito di quelle attività che comportano la gestione e/o la diffusione di strumenti di pagamento diversi dai

contanti e negli ambienti tecnologici a supporto di dette attività. L'articolo 25 octies.1 del D. Lgs. 231/2001, ha inoltre esteso il catalogo dei reati presupposto a "*ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal Codice penale*" a condizione che ne siano oggetto materiale "strumenti di pagamento diversi dai contanti".

TRASFERIMENTO FRAUDOLENTO DI VALORI (ART. 512 BIS C.P.) - MODIFICATO DA D.L. N.19 DEL 2 MARZO 2024 COORDINATO CON LA LEGGE DI CONVERSIONE N.56 DEL 29 APRILE 2024)

Tale reato punisce chi, salvo che il fatto costituisca più grave reato, attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di prevenzione patrimoniale o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di ricettazione, riciclaggio e impiego di denaro o beni di provenienza illecita.

In generale può osservarsi che alcune fattispecie di reati informatici in concreto potrebbero non presentare il requisito della commissione nell'interesse o a vantaggio di GETOPEN, indispensabile affinché possa conseguire la responsabilità amministrativa della stessa. Per altro verso si ricorda che qualora fossero integrati tutti gli elementi previsti dal D. Lgs. 231/2001 la responsabilità di GETOPEN potrebbe sorgere, secondo la previsione contenuta nell'art. 8 del Decreto, anche quando l'autore del reato non sia identificabile (dovrebbe quantomeno essere provata la provenienza della condotta da un soggetto apicale o da un dipendente, anche se non identificato), evenienza tutt'altro che improbabile nel campo della criminalità informatica, in ragione della complessità dei mezzi impiegati e dell'evanescenza del cyberspazio, che rendono assai difficile anche l'individuazione del luogo ove il reato stesso possa ritenersi consumato. Va infine ricordato che l'art. 640 ter c.p., che punisce il delitto di frode informatica, costituiva già reato presupposto della responsabilità amministrativa degli Enti ex art. 24 D. Lgs. 231/2001 se perpetrato ai danni dello Stato o di altro Ente pubblico.

Orbene, alla luce delle superiori disposizioni, l'Amministratore Unico verifica che vengano osservati tutti gli obblighi di legge in materia di limitazione all'uso del contante e dei titoli al portatore.

Il presente protocollo si applica a tutte le Funzioni aziendali coinvolte nella gestione e nell'utilizzo degli strumenti di pagamento diversi dai contanti.

GETOPEN è costantemente impegnata nella ricerca e nell'attuazione di soluzioni operative il più possibile aggiornate, finalizzate a prevenire e ad ostacolare gli utilizzi fraudolenti degli strumenti di pagamento e quindi l'esecuzione di operazioni di pagamento non autorizzate.

Ai sensi del D. Lgs 231/2001, il processo potrebbe presentare occasioni per la commissione del reato di "*Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti*" e ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal Codice penale a condizione che ne siano oggetto materiale strumenti di pagamento diversi dai contanti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte di GETOPEN, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

La Legge n. 56/2024 - rubricata "Conversione in legge, con modificazioni, del D.L. 2 marzo 2024, n. 19, recante ulteriori disposizioni urgenti per l'attuazione del Piano Nazionale di Ripresa e Resilienza (PNRR) - ha modificato, ampliando il campo di applicazione, il testo di cui all'art. 512 – bis c.p., rubricato "Trasferimento fraudolento di valori", peraltro inserito di recente all'interno del catalogo dei reati presupposto di cui al d.lgs. 231/2001, all'art. 25 – octies.1.

E' stato quindi aggiunto il nuovo secondo comma, secondo cui: "*La stessa pena di cui al primo comma [reclusione da due a sei anni] si applica a chi, al fine di eludere le disposizioni in materia di documentazione antimafia, attribuisce fittiziamente ad altri la titolarità di imprese, quote societarie o azioni ovvero di cariche sociali, qualora l'imprenditore o la società partecipi a procedure di aggiudicazione o di esecuzione di appalti o di concessioni*".

Tale ultima modifica assume particolare rilevanza per le Società, specie per quelle che partecipano a bandi pubblici, in ragione della documentazione richiesta e da produrre in fase di gara, ma anche per ciò che concerne le procedure di qualificazione dei fornitori, e più in generale per tutte quelle che hanno particolari obblighi di segnalazione e vigilanza sulla clientela e che effettuano operazioni di trasferimento di beni, denaro o partecipazioni societarie.

È necessario pertanto, in logica preventiva, procedere ad un aggiornamento ed implementazione dei Protocolli e delle Istruzioni Operative aziendali, prevendendo specifici presidi per questa nuova fattispecie criminosa.

DESCRIZIONE DEL PROCESSO

Il processo di gestione e utilizzo degli strumenti di pagamento diversi dai contanti si articola nei seguenti processi:

• Carte di pagamento (carte di debito e di servizio, carte di credito, carte prepagate);

• Incassi e pagamenti (es. assegni, bonifici, addebiti diretti, RIBA – MAV – effetti);

• Servizi di Accesso ai Canali Digitali (accesso ed identificazione a distanza destinati a persone fisiche e persone giuridiche, altri servizi);

• Gestione risorse Umane con riferimento alle carte di credito aziendali e, laddove erogate dalla Società ai Dipendenti, ai buoni pasto, alle carte di servizio per le autovetture (carta carburante, telepass).

5.3 GESTIONE INCASSI

Relativamente al processo di gestione degli incassi, il RAM/RRU, o altra Funzione Aziendale eventualmente incaricata per iscritto, deve:

- ✓ Verificare l'identità della persona fisica o giuridica che esegue il pagamento;
- ✓ verificare che per ciascun incasso corrisponda un documento giustificativo.

Il RAM deve predisporre un "*piano degli incassi mensile*", che verrà condiviso, unitamente ad un "*piano pagamenti mensile*", su una piattaforma digitale (come ad es. TEAMS o simili) e verrà validato, con firma digitale o con firma olografa, apposta dall'Amministratore Unico.

L'A.U. verifica che le movimentazioni di somme di denaro avvengano sempre attraverso intermediari finanziari, come Banche, Istituti di moneta elettronica od altri soggetti tenuti all'osservanza della Direttiva 2005/60/CE (III Direttiva antiriciclaggio) e che vengano osservati tutti gli obblighi di legge in materia di limitazione all'uso del contante e dei titoli al portatore.

Per ciò che concerne gli incassi in contante, è preferibile evitare qualsiasi forma di cosiddetto "*pagamento facilitato*", salvo che si tratti di piccole somme. Tuttavia, in tal caso, prima di accettare i suddetti pagamenti, occorre consultare l'Amministratore Unico della Società.

5.4 GESTIONE RAPPORTI CON ISTITUTI DI CREDITO

La gestione dei rapporti con gli Istituti di Credito (come l'apertura di c/c bancari, la costituzione di depositi e di libretti di risparmio anche al portatore, la costituzione e la stipulazione di finanziamenti e di fidi, *etc.*) è di esclusiva competenza dell'Amministratore Unico.

L'Amministratore Unico ha il potere di firmare contratti con gli Istituti di Credito (come l'apertura di c/c bancari, la costituzione di depositi e di libretti di risparmio anche al portatore, di costituzione e di stipulazione di finanziamenti e di fidi, *etc.*).

Il REC esegue, con cadenza trimestrale, il controllo della riconciliazione dei saldi bancari con le risultanze contabili, verificando, dunque, la quadratura dei saldi bancari. La Società, con cadenza trimestrale, comunica l'avvenuta verifica della predetta quadratura dei saldi bancari all'OdV con specifici *report*.

5.5 GESTIONE CASSA CONTANTE

La Società effettua piccoli pagamenti per cassa, sempre con giustificativo di spesa (ad es. scontrino) ed in misura non superiore ad € 300,00 mensili.

Detti prelevamenti vengono effettuati, esclusivamente, dall'Amministratore Unico o dai soggetti muniti di bancomat e all'uopo espressamente autorizzati dallo stesso.

Il soggetto che ha eseguito la predetta operazione dovrà darne comunicazione al RAM o all'A.U., precisando, altresì, la causale.

La documentazione cartacea attestante la gestione della cassa (ricevute, scontrini, prelievo) viene archiviata secondo regole interne che ne assicurino la rintracciabilità.

L'Amministratore Unico, con cadenza trimestrale, effettua la quadratura di cassa, dandone comunicazione all'ODV.

5.6 FATTURAZIONE ATTIVA E PASSIVA E TRASMISSIONE PERIODICA LIQUIDAZIONE IVA

Le Funzioni Aziendali all'uopo preposte - come il REC e il RAM/RRU – devono garantire una corretta gestione dei processi di fatturazione attiva e passiva, ovvero delle diverse fasi di emissione e/o ricezione, nonché della fase di registrazione del pagamento.

In particolare, le predette Funzioni Aziendali devono: **1)** controllare le fatture emesse e/o ricevute, nonchè i controlli di registrazione delle medesime; **2)** accertare la coerenza delle informazioni contenute nei documenti giustificativi delle operazioni e la conformità dei dati inseriti nei medesimi documenti.

Le Funzioni Aziendali all'uopo preposte, dovranno dare immediata comunicazione all'OdV di eventuali anomalie che venissero riscontrate a seguito dei predetti controlli.

Gli adempimenti relativi alla trasmissione periodica dell'IVA dovranno essere tempestivamente messi a conoscenza dell'OdV mediante apposito report.

GETOPEN adotta un sistema gestionale relativo a tutte le attività fiscali-amministrativo-contabili, ed in particolare per le attività di fatturazione attiva e passiva, nonché dei relativi incassi ed acquisti, dovrà assicurare che:

1) i soggetti incaricati di porre in essere le citate attività, e con particolare riferimento alle attività di formazione, trasmissione, archiviazione ed eventuale aggiornamento della documentazione rilevante;

2) la registrazione di tutte le fasi del procedimento, ivi compresa, ove prevista, l'eventuale fase autorizzativa;

3) l'esistenza di appositi supporti, analogici e/o digitali, finalizzati ad assicurare la tracciabilità delle fatture emesse e/o ricevute dalla Società;

4) la tracciabilità dei pagamenti e/o degli incassi ricevuti, al fine di consentire la corretta emissione/registrazione della fattura (attiva/passiva) e del perfezionamento della fase di pagamento/incasso;

5) l'applicazione di procedure specifiche per la gestione degli accessi, tali da consentire la tracciabilità dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e di quelli autorizzati ad apportare modifiche, nonché la rilevazione degli accessi non autorizzati.

7 TRASFERIMENTO FRAUDOLENTO DI VALORI (EX ART. 512 BIS C.P.)

L'art. 6-ter della Legge 137/2023 ha introdotto all'interno dell'art. 25-octies.1, concernente i delitti in materia di strumenti di pagamento diversi dai contanti, la fattispecie di trasferimento fraudolento di valori (art. 512-bis c.p.), in relazione al quale è prevista per gli Enti la sanzione pecuniaria da 250 a 600 quote; alle citate sanzioni si aggiungono le sanzioni interdittive di cui ex art. 9, co. 2 del D.Lgs. n. 231/2001.

Pertanto, la suddetta Legge 137/2023 ha inserito tra i reati-presupposto il delitto di trasferimento fraudolento di valori di cui all'art. 512-bis c.p..

L'art. 512-bis c.p. prevede che "*Salvo che il fatto costituisca più grave reato, chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni*

o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648-bis e 648-ter, è punito con la reclusione da due a sei anni".

Dunque, il delitto di "trasferimento fraudolento di valori" si aggiunge all'indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.); alla detenzione e diffusione di dispositivi diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.) e alla frode informatica (art. 640-ter c.p.) aggravata dal trasferimento di denaro.

Dall'esame della citata disposizione emerge come si tratta di un reato che può essere commesso con una grande varietà di negozi simulati riguardanti non solo denaro contante su un conto corrente o beni immobili, ma beni della più diversa natura.

Invero, a titolo meramente esemplificativo, si può ritenere che l'ipotesi più ricorrente, nell'ambito della quale si può configurare il predetto reato, è quella della cessione di quote o azioni eseguita al fine di estraniarsi dalla compagine della società solo apparentemente, poiché chi si è spogliato formalmente della titolarità delle quote o delle azioni continua di fatto a determinarne l'attività come amministratore o socio occulto e a partecipare alla gestione e agli utili derivanti dall'attività imprenditoriale.

Il reato di cui all'art. 512-bis c.p., è un reato solo eventualmente plurisoggettivo, con la conseguenza che il terzo fittiziamente interposto (non punito direttamente dalla stessa disposizione) risponde a titolo di concorso con chi ha operato la fittizia attribuzione in quanto con la sua condotta cosciente e volontaria, contribuisce alla lesione dell'interesse protetto dalla norma (Corte di Cassazione sentenza n. 35826/2019).

È, quindi, sufficiente, ai fini della configurabilità del dolo del concorrente, che la particolare finalità tipizzata dalla disposizione incriminatrice sia perseguita almeno

da uno dei soggetti che concorrono alla realizzazione del fatto (Corte di Cassazione sentenza n. 38044/2021).

PERTANTO, I DESTINATARI DELLA PRESENTE PROCEDURA DOVRANNO ASTENERSI:

- Dall'eludere le disposizioni in materia di misure di prevenzione patrimoniali o di contrabbando o per agevolare la commissione dei delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, spogliandosi fittiziamente della titolarità di denaro, beni o altre utilità, attribuendola a terzi.

IL SISTEMA SANZIONATORIO:

Si rammenta che l'art. 25 octies.1 d.lgs. 231/2001 nel testo vigente annovera, al comma 1, quali reati presupposto, l'indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.), con sanzione amministrativa da 300 a 800 quote, la detenzione e diffusione di dispositivi diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.) e la frode informatica (art. 640-ter c.p.) aggravata dal trasferimento di denaro, con sanzione amministrativa fino a 500 quote. Il comma 2 contempla poi quale reato presupposto ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, salvo che il fatto costituisca più grave illecito amministrativo, con sanzioni amministrative graduate a seconda della pena edittale prevista dal codice penale.

La sanzione pecuniaria ora prevista per il trasferimento fraudolento di valori è invece da 250 a 600 quote.

Inoltre, il comma 3 prevede che, nei casi di condanna per uno dei delitti di cui al medesimo art. 25.octies.1, e quindi da adesso anche per il reato di cui all' art. 512-bis c.p., si applichino all'Ente le sanzioni interdittive dell'interdizione dall'esercizio dell'attività; della sospensione o della revoca delle autorizzazioni, licenze o concessioni; del divieto di contrattare con la pubblica amministrazione,

dell'esclusione da agevolazioni, finanziamenti, contributi o sussidi; del divieto di pubblicizzare beni o servizi (di cui al citato art. 9 comma 2, d.lgs. 231/2001).

DUNQUE, SI APPLICHERANNO LE SEGUENTI SANZIONI:

- Sanzioni pecuniarie da 250 a 600 quote.
- Sanzioni interdittive:
  - interdizione dall'esercizio dell'attività
  - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio.
  - Esclusione dalle agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi;
  - Divieto di pubblicizzare beni o servizi

8 ACQUISIZIONE DI NUOVI CESPITI E DISMISSIONE DEI CESPITI

In ordine ai cespiti, GETOPEN definisce le regole e le procedure aziendali per l'approvazione dell'acquisizione o della cessione o dismissione dei cespiti, con la previsione di un processo approvativo che consiste:

▪ Il RATTR, o altra Funzione Aziendale all'uopo autorizzata, deve comunicare all'Amministratore Unico e al RAM/RRU la possibilità di acquisire un nuovo cespite o l'esigenza di dismettere un cespite, caricando, nell'apposito archivio informatico della piattaforma digitale, una scheda del bene in questione e la relativa richiesta di autorizzazione, al fine di consentire la necessaria autorizzazione da parte dell'Amministratore Unico che può sottoscrivere, con firma digitale o con firma olografa, la suddetta scheda. Ottenuta l'autorizzazione, il RATTR o la Funzione responsabile all'uopo autorizzata, procede con la dismissione del bene.

▪ la Funzione Aziendale competente prima di porre in essere l'atto di acquisizione o di dismissione del cespite, dovrà essere, previamente, autorizzata dall'Amministratore Unico, il quale apporrà la propria firma olografa o digitale nella citata autorizzazione;

▪ deve essere attuata la gestione contabile e fiscale della registrazione associata all'acquisizione e alla cessione o dismissione dei cespiti.

9 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO

Tutti i *Destinatari* coinvolti nella puntuale applicazione della presente procedura, dovranno segnare all'ODV:

- ogni situazione anomala;
- ogni situazione in contrasto con la presente procedura;
- ogni condotta posta in essere in violazione delle disposizioni del Modello e del Codice Etico.

LE FUNZIONI AZIENDALI ALL'UOPO PREPOSTE DOVRANNO COMUNICARE ALL'ODV:

- Mediante un report semestrale i pagamenti superiori ad euro 15.000,00;
- Mediante un report annuale, l'elenco dei conti correnti "*temporanei*" o inattivi da almeno 6 mesi, o comunque poco movimentati (ad es. ≤ 2 operazioni in un anno);
- tempestivamente, le operazioni effettuate per mezzo di strumenti di pagamento anomali e operazioni condotte in un Paese estero cosiddetto "*non collaborativo*", con espressa indicazione della motivazione economica per la quale è stata eseguita la predetta operazione;
- tempestivamente, qualsiasi condotta che possa integrare le fattispecie di cui al D.lgs.231/2001 e qualsivoglia condotta rilevante ai fini della presente procedura.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di corporate governance per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 20.03.2024	ADOZIONE
Rev. 1	Determina dell'Amministratore Unico del 05.08.2024	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231)

PARTE SPECIALE -3-

SOMMARIO

1 OBIETTIVI E FUNZIONI DEL MODELLO

Il presente protocollo ha lo scopo di definire le condotte che ciascuna Funzione Aziendale coinvolta deve osservare al fine di prevenire la commissione dei reati societari, nonché al fine di garantire la corretta gestione delle attività inerenti la redazione ed approvazione del bilancio.

La procedura relativa alla predisposizione ed approvazione del bilancio viene posta in essere nel rispetto di quanto previsto nel Codice Etico e nel Modello adottati dalla Società ed in particolar modo nel rispetto delle procedure speciali disciplinate dal Modello 231 e relative ai "Reati societari e corruzione tra privati" ed ai "Reati tributari".

TUTTI I DESTINATARI DELLA PRESENTE PROCEDURA DEVONO:

a) tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;

b) attivarsi affinché i fatti di gestione siano rappresentati correttamente e tempestivamente nella contabilità;

c) garantire la tempestività, l'accuratezza e il rispetto del principio di competenza nell'effettuazione;

d) delle registrazioni contabili;

e) assicurarsi che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima e coerente con la documentazione di supporto in modo da consentire la ricostruzione accurata dell'operazione;

f) assicurare il rispetto dei principi contabili adottati e la tracciabilità nelle scritture di chiusura, assestamento e rettifica e le poste estimative/valutative;

g) assicurare la corretta contabilizzazione delle operazioni di acquisto, cessione / dismissione di immobilizzazioni immateriali, materiali e finanziarie e relative plusvalenze o svalutazioni;

h) applicare adeguate procedure di controllo in caso di sopravvenienze attive apparentemente non giustificate o in caso di registrazioni di incassi (e pagamenti) di cui non si riscontri una contropartita di credito (o debito) corrispondente;

i) osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;

l) assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;

m) assicurare che i rapporti con i funzionari delle Autorità di Vigilanza siano gestiti esclusivamente dai soggetti dotati di idonei poteri;

n) effettuare con tempestività, correttezza e buona fede tutte le comunicazioni nei confronti di Autorità di Vigilanza – siano esse previste dalla legge o richieste dall'Autorità stessa - evitando ogni comportamento che possa risultare di ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate;

o) assicurare che ogni tipo di operazione straordinaria sia condotta dalla Società nel pieno rispetto delle norme di legge o dei regolamenti applicabili;

p) mantenere riservati i documenti e le informazioni acquisiti nello svolgimento dei propri compiti e, in particolare, assicurare che la circolazione interna e verso Terzi di documenti contenenti informazioni potenzialmente privilegiate sia soggetta ad ogni necessaria attenzione e cautela, onde evitare pregiudizi a GETOPEN e indebite divulgazioni;

q) non comunicare ad altri, se non per motivi d'ufficio, le informazioni potenzialmente privilegiate di cui si viene a conoscenza;

r) far sottoscrivere, ai Terzi cui si comunicano informazioni potenzialmente privilegiate, in occasione del conferimento dell'incarico, un impegno di riservatezza.

2 ACRONIMI AZIENDALI

AU	Amministratore Unico
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale – Approvvigionamento
REC	Responsabile Esterno Contabilità
SOC	Soci

PER L'IDENTIFICAZIONE DEI SOGGETTI CHE CORRISPONDONO AGLI ACRONIMI AZIENDALI SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI GETOPEN S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di GETOPEN S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di GETOPEN S.r.l..

4 I REATI SOCIETARI - LE FATTISPECIE DI REATO DI CUI ALL'ART. 25-TER D.LGS. 231/2001

La presente Parte Speciale ha lo scopo di definire le procedure necessarie ad assicurare la prevenzione della commissione dei reati societari contemplati nell'art. 25 ter del D.Lgs. 231/2001, alla luce della modifica normativa di cui all'art. 4 del D.Lgs. 38/2017 che ha introdotto una nuova fattispecie di reato ("istigazione alla corruzione tra privati") e previsto la possibilità di comminare per alcune fattispecie

illecite anche sanzioni interdittive, oltre a quelle pecuniarie già contemplate. Si descrivono brevemente, di seguito, le singole fattispecie previste e ritenute concretamente applicabili al caso di specie.

ART. 2621. FALSE COMUNICAZIONI SOCIALI.

"*Fuori dai casi previsti dall'articolo 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da uno a cinque anni. La stessa pena si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi*".

Il reato di false comunicazioni sociali si configura allorquando si procede alla esposizione, all'interno dei bilanci, delle relazioni o delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero (ancorché oggetto di valutazione), ovvero alla mancata indicazione, nei medesimi documenti, di informazioni, la cui comunicazione è prescritta dalla legge, riguardanti la situazione economica, patrimoniale o finanziaria della società o del gruppo a cui appartiene, con modalità idonee ad indurre in errore i destinatari. Il reato si perfeziona nel momento in cui "consapevolmente" (così come recita la nuova formulazione dell'art. 2621 c.c.) siano esposti fatti non rispondenti al vero, oppure vengono omesse informazioni dovute per legge nell'ambito delle comunicazioni sociali. Soggetti attivi sono *"… gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori …"*. La fattispecie di cui all'art. 2621 c.c. sanziona la condotta ivi indicata a prescindere dal verificarsi del danno.

L'ART. 25-TER INCLUDE TRA I REATI IDONEI A CONFIGURARE LA RESPONSABILITÀ DELL'ENTE ANCHE IL NUOVO ART. 2621-BIS (FATTI DI LIEVE ENTITÀ):

"*Salvo che costituiscano più grave reato, si applica la pena da sei mesi a tre anni di reclusione se i fatti di cui all'articolo 2621 sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta. Salvo che costituiscano più grave reato, si applica la stessa pena di cui al comma precedente quando i fatti di cui all'articolo 2621 riguardano società che non superano i limiti indicati dal secondo comma dell'articolo 1 del regio decreto 16 marzo 1942, n. 267. In tale caso, il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale.*"

Le sanzioni previste dall'art. 2621 c.c. sono ridotte se i fatti sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta (art. 2621-bis c.c.). È, altresì, prevista l'ipotesi della non punibilità dei fatti di cui agli articoli sopra citati, rimessa all'apprezzamento del giudice che valuta, a tal fine, l'entità dell'eventuale danno cagionato alla società, ai soci o ai creditori (art. 2621-ter c.c.).

ART. 2625. IMPEDITO CONTROLLO.

"*Gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali sono puniti con la sanzione amministrativa pecuniaria fino a 10.329 euro. Se la condotta ha cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa. La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.*"

Il reato si configura allorquando si ostacoli o si impedisca lo svolgimento delle attività di controllo e/o di revisione, legalmente attribuite ai soci e agli organi sociali. La condotta può essere integrata mediante l'occultamento di documenti o l'utilizzo di altri idonei artifici. La pena è aumentata qualora sia cagionato un danno ai soci. Soggetti attivi del reato sono gli amministratori. Il reato può essere

commesso mediante qualsiasi condotta idonea ad ostacolare lo svolgimento delle attività di controllo riconosciute ai soci.

Ferma restando la rilevanza di qualsiasi condotta idonea a determinare l'evento sopra indicato, assumono particolare rilevanza:

- l'occultamento di documenti (ad es., dei libri sociali);
- l'adozione di altri artifici.

ART. 2626. INDEBITA RESTITUZIONE DEI CONFERIMENTI

"*Gli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli, sono puniti con la reclusione fino ad un anno*".

Il reato si configura allorquando si proceda, fuori dei casi di legittima riduzione del capitale sociale, alla restituzione, anche simulata, dei conferimenti ai soci o alla liberazione degli stessi dall'obbligo di eseguirli. Soggetto attivo del reato è l'Amministratore Unico.

Il reato può essere commesso mediante:

- restituzione, anche simulata, dei conferimenti effettuati dai soci;
- liberazione dei soci dall'obbligo di eseguire i conferimenti.

Il reato si perfeziona con l'esecuzione di una delle condotte tipiche previste dalla norma.

ART. 2627. ILLEGALE RIPARTIZIONE DEGLI UTILI E DELLE RISERVE.

"*Salvo che il fatto non costituisca più grave reato, gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite, sono puniti con l'arresto fino ad un anno. La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato*".

Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite. In ogni

caso, la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Soggetto attivo del reato è l'Amministratore Unico.

Il reato può essere commesso mediante:

- ripartizione di utili, o di acconti su utili, non effettivamente conseguiti o destinati per legge a riserva;
- ripartizione di riserve che per legge non possono essere distribuite.

ART. 2628. ILLECITE OPERAZIONI SULLE AZIONI O QUOTE SOCIALI O DELLA SOCIETÀ CONTROLLANTE

"Gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge, sono puniti con la reclusione fino ad un anno. La stessa pena si applica agli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto".

Il reato si configura allorquando si proceda, fuori dei casi previsti dalla legge, all'acquisto o alla sottoscrizione di azioni o quote emesse dalla società o della controllante, così da cagionare una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge. Si precisa che, se il capitale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio riferito all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

Il reato potrebbe essere commesso mediante acquisto o sottoscrizione di azioni o quote emesse dalla società, fuori dai casi previsti dalla legge, così da cagionare una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

Soggetto attivo del reato è l'Amministratore Unico.

ART. 2629. OPERAZIONI IN PREGIUDIZIO DEI CREDITORI.

"Gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Il risarcimento del danno ai creditori prima del giudizio estingue il reato."

La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori.

In ogni caso, il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Soggetto attivo del reato è l'Amministratore Unico.

La fattispecie potrebbe essere commessa qualora, in violazione delle disposizioni di legge a tutela dei creditori, sia cagionato un danno a questi ultimi mediante:

- riduzione del capitale sociale;
- realizzazione di operazioni di fusione o scissione.

ARTICOLO 2629-BIS. OMESSA COMUNICAZIONE DEL CONFLITTO D'INTERESSI

"L'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1 settembre 1993, n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998, del decreto legislativo 7 settembre 2005, n. 209, del decreto legislativo 21 aprile 1993, n. 124, che viola gli obblighi previsti dall'articolo 2391, primo comma, è punito con la reclusione da uno a tre anni, se dalla violazione siano derivati danni alla società o a terzi."

Il reato si configura allorquando l'amministratore ometta di comunicare la titolarità di un proprio interesse, personale o per conto di terzi, in una determinata operazione della società. La fattispecie sanziona, inoltre, la condotta

dell'Amministratore Delegato/Direttore Generale che, essendo portatore di analogo interesse, ometta di astenersi dal compiere l'operazione. Soggetto attivo del reato è l'Amministratore Unico.

ART. 2632. FORMAZIONE FITTIZIA DEL CAPITALE.

"Gli amministratori e i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione, sono puniti con la reclusione fino ad un anno."

Il reato si configura allorquando si proceda alla formazione o all'aumento in modo fittizio del capitale sociale mediante:

• attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale;

• sottoscrizione reciproca di azioni o quote;

• sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono l'Amministratore Unico e i soci conferenti.

Tale ipotesi di reato è integrata dalla condotta di formazione o aumento, in modo fittizio, del capitale sociale, effettuata mediante:

- attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale;
- sottoscrizione reciproca di azioni o quote;
- sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

ART. 2633. INDEBITA RIPARTIZIONE DEI BENI SOCIALI DA PARTE DEI LIQUIDATORI

"I liquidatori che, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionano danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Il risarcimento del danno ai creditori prima del giudizio estingue il reato".

Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Soggetti attivi del reato sono i liquidatori.

La fattispecie è integrata nel caso in cui, durante la fase della liquidazione, i liquidatori cagionano un danno ai creditori sociali mediante la ripartizione dei beni sociali tra i soci:

- prima del pagamento dei creditori sociali;
- prima dell'accantonamento delle somme necessarie a soddisfarli.

ART. 2635. CORRUZIONE TRA PRIVATI.

Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, che, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società, sono puniti con la reclusione da uno a tre anni.

Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.

Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste.

Le pene stabilite nei commi precedenti sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'art. 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.

Si procede a querela della persona offesa, salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi".

La condotta consiste, dal lato passivo, nell'accettare denaro o altra utilità per sé o altri (o la relativa promessa) per compiere od omettere atti in violazione degli obblighi inerenti l'ufficio o degli obblighi di fedeltà, che comportino un nocumento per la società.

Quanto agli obblighi violati questi possono avere fonte legislativa (codice civile artt. 2390-2392 c.c. per gli amministratori), o anche extra-codicistica (i.e. ambiente, sicurezza sul lavoro, etc.), o non legislativa (i.e. provvedimenti di autorità di vigilanza, etc.).

Quanto agli obblighi di fedeltà si fa riferimento agli obblighi collegati ai principi di correttezza e buona fede di cui agli artt. 1175, 1375 e 2105 del codice civile.

Dal lato attivo ("corruttore") la condotta consiste nell'offrire o promettere danaro o qualsiasi altra utilità (favori, assunzione di personale, offerta di contratti di consulenza ecc..).

I soggetti attivi del reato, dal lato passivo, possono essere gli "apicali" (amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori), ma anche i sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati (quindi i dipendenti ma anche i collaboratori esterni come agenti, concessionari, etc.). Il corruttore può essere chiunque.

È importante sottolineare che il bene giuridico che la fattispecie mira a tutelare è il patrimonio sociale. In particolare, si rileva che l'estraneità dell'atto ai doveri sociali oggetto di scambio non rileva di per sé, ma in quanto comporti un nocumento alla società, che conserva nella maggior parte dei casi il potere di decidere se i comportamenti corruttivi debbano o meno essere puniti.

Si segnala che, ai fini della responsabilità amministrativa, può essere sanzionato solo l'ente cui appartiene il "corruttore" (l'unico che può essere avvantaggiato dalla condotta corruttiva), mentre la società di riferimento del corrotto, essendo danneggiata dalla condotta delittuosa, non sarà punibile ex Decreto.

A titolo di esempio il reato potrebbe realizzarsi qualora il dipendente di una società offra omaggi o danaro all'amministratore di un'altra società che ha indetto una gara

o sta svolgendo una trattativa privata per una fornitura, al fine di indurre l'amministratore della società che ha indetto la gara/trattativa a violare le procedure dell'azienda che regolano lo svolgimento o l'aggiudicazione per avvantaggiare la società del corruttore, concludendo un contratto svantaggioso per la società.

ART. 2635 BIS. ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI.

"Chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo.

La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per sé o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata.

Si procede a querela della persona offesa".

La norma, inserita dall'art. 4 del D.Lgs. 15.03.2017, n. 38 (in vigore dal 14.04.2017), introduce la fattispecie dell'istigazione alla corruzione tra privati.

In particolare, sotto il profilo attivo, la condotta sanzionabile penalmente in capo a chiunque consiste nell'offrire o promettere denaro o altre utilità non dovuti ad uno dei soggetti interni elencati al fine del compimento o dell'omissione di atti in violazione degli obblighi inerenti il proprio ufficio o degli obblighi di fedeltà, qualora l'offerta o la promessa non sia accettata (art. 2635-bis, comma 1, c.c.). Sotto il profilo passivo, di contro, è prevista la punibilità del soggetto interno che solleciti una promessa o dazione di denaro o altra utilità, al fine del compimento o

dell'omissione di atti in violazione dei medesimi obblighi, qualora tale proposta non sia accettata (art. 2635-bis, comma 2, c.c.). Tale norma incriminatrice ha essenzialmente la finalità di evitare che rimangano impuniti i comportamenti di offerta non accettata (dal lato attivo) e di sollecitazione non accolta (dal lato passivo), che erano privi in precedenza di sanzione penale. Il momento consumativo, essendo la condotta di natura istantanea, coincide, in entrambe le fattispecie, con la formulazione dell'offerta, da un lato, o con la formulazione della sollecitazione, dall'altro.

ART. 2636. ILLECITA INFLUENZA SULL'ASSEMBLEA.

"Chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto, è punito con la reclusione da sei mesi a tre anni".

L'ipotesi di reato in esame tende a garantire che la volontà dell'organo deliberativo della società sia espressa attraverso l'esercizio di voti validi e nel rispetto della regola di maggioranza (o principio maggioritario). Soggetto attivo può essere «chiunque» e, quindi, anche un soggetto non socio ed estraneo alla società. Il reato si perfeziona nel momento in cui, a seguito di atti simulati o fraudolenti, si determina fittiziamente la maggioranza assembleare idonea ad adottare una o più delibere. Vale precisare, peraltro, che il reato non si configura se la delibera sarebbe stata comunque adottata dall'assemblea anche in mancanza della maggioranza "fraudolentemente orientata" (al fine di accertare tale ultima circostanza è necessario procedere alla c.d. "prova di resistenza" che consiste nel verificare se, sottraendo i voti espressi in virtù degli atti simulati o fraudolenti, la delibera raggiunge comunque le maggioranze prescritte per la sua regolare adozione).

ART. 2637. AGGIOTAGGIO.

"Chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale

di banche o di gruppi bancari, è punito con la pena della reclusione da uno a cinque anni".

Il reato si configura allorquando si proceda alla diffusione di notizie false ovvero alla realizzazione di operazioni simulate o ad altri artifici, idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari ovvero a incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

La condotta deve avere ad oggetto strumenti finanziari non quotati o per i quali non è stata presentata domanda di ammissione alla negoziazione in un mercato regolamentato.

Soggetto attivo del reato può essere chiunque.

LA CONDOTTA PENALMENTE SANZIONATA PUÒ ESSERE INTEGRATA MEDIANTE:

- diffusione di notizie false;
- realizzazione di operazioni simulate (ad es., compravendita di azioni o altri strumenti con mutamento soltanto apparente della proprietà degli stessi);
- compimento di altri artifici (ad es., diffusione di una serie di comunicazioni idonee ad ingenerare il convincimento circa la realizzazione di operazioni straordinarie).

LE ATTIVITÀ INDICATE DEVONO ESSERE CONCRETAMENTE IDONEE:

- a determinare una sensibile alterazione del prezzo di strumenti finanziari non quotati (o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato);
- ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.

ART. 2638. OSTACOLO ALL'ESERCIZIO DELLE FUNZIONI DELLE AUTORITÀ PUBBLICHE DI VIGILANZA.

"Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali

non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, sono puniti con la reclusione da uno a quattro anni. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Sono puniti con la stessa pena gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società, o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni. La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58".

La condotta tipica è quella dell'impedito e/o ostacolato controllo cd. "esterno" (ossia il controllo svolto dalle autorità pubbliche di vigilanza), non anche il controllo cd. "interno" (ossia quello esercitato da organi interni alla compagine sociale). La condotta criminosa si realizza 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 economica, 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.

Soggetti attivi del reato in parola possono essere l'Amministratore Unico e coloro che sono preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società sottoposte per legge alle autorità pubbliche di vigilanza.

Il reato in questione può essere realizzato attraverso due distinte modalità, entrambe finalizzate ad ostacolare l'attività di vigilanza delle Autorità Pubbliche preposte:

- la comunicazione alle Autorità Pubbliche di Vigilanza di fatti non rispondenti al vero, sulla situazione economica, patrimoniale o finanziaria, ovvero con l'occultamento di fatti che avrebbero dovuto essere comunicati;
- l'ostacolo all'esercizio delle funzioni di vigilanza svolte da Pubbliche Autorità, attuato consapevolmente ed in qualsiasi modo, anche omettendo le comunicazioni dovute alle medesime Autorità.

5 PREVENZIONE COMMISSIONE REATI SOCIETARI - PRINCIPI GENERALI DI CONTROLLO E DI COMPORTAMENTO

Nell'espletamento della propria attività per conto della Società, i destinatari che operano direttamente o indirettamente nelle aree "a rischio reato" sono tenuti al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal Modello e, in particolare, i principi e le regole etiche adottate dalla Società.

A tutti i soggetti destinatari del Modello è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, considerati singolarmente o complessivamente, siano idonei ad integrare i reati sopra descritti o possano in astratto diventarlo. In particolare, per ogni operazione contabile deve essere conservata agli atti sociali una adeguata documentazione di supporto dell'attività svolta, in modo da consentire:

a) l'agevole registrazione contabile;

b) l'individuazione dei diversi livelli di responsabilità;

c) la ricostruzione accurata della operazione, anche al fine di ridurre la probabilità di errori.

Alla luce dei principi di controllo prima evidenziati, è necessario che tutte le operazioni svolte nell'ambito delle attività "sensibili" ricevano debita evidenza.

Nell'esecuzione di tali operazioni, occorre che sia garantito il rispetto dei principi di comportamento di seguito indicati:

➢ astenersi dal porre in essere condotte tali da integrare le fattispecie di reato illustrate nella presente Parte Speciale;

➢ garantire il rispetto delle regole comportamentali previste nel Codice Etico, con particolare riguardo all'esigenza di assicurare che ogni operazione e transazione sia correttamente registrata, autorizzata, verificabile, legittima, coerente e congrua;

➢ tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e regolamentari vigenti, nell'esecuzione di tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci e ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;

➢ tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e regolamentari vigenti, nell'acquisizione, elaborazione e illustrazione dei dati e delle informazioni necessarie per consentire di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della Società;

➢ garantire il rispetto dei principi di integrità, correttezza e trasparenza così da consentire ai destinatari di pervenire ad un fondato ed informato giudizio sulla situazione patrimoniale, economica e finanziaria della Società e sull'evoluzione della sua attività, nonché sui prodotti finanziari e relativi;

➢ osservare le prescrizioni imposte dalla legge a tutela dell'integrità ed effettività del capitale sociale ed agire nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere al riguardo;

➢ astenersi dal compiere qualsivoglia operazione o iniziativa qualora vi sia una situazione di conflitto di interessi, ovvero qualora sussista, anche per conto di terzi, un interesse in conflitto con quello della Società;

➢ assicurare il regolare funzionamento della Società e degli organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale prevista dalla legge, nonché la libera formazione della volontà assembleare;

➢ astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false e/o non corrette e/o fuorvianti, idonee a provocare l'alterazione del prezzo di strumenti finanziari;

➢ gestire con la massima correttezza e trasparenza il rapporto con le Pubbliche Autorità, ivi incluse quelle di Vigilanza;

➢ effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche di Vigilanza, non ostacolando l'esercizio delle funzioni di vigilanza da queste intraprese;

➢ tenere un comportamento corretto e veritiero con gli organi di stampa e di informazione.

Su qualsiasi operazione realizzata dai soggetti sopra indicati e valutata potenzialmente a rischio di commissione di reati, l'OdV potrà predisporre controlli dei quali dovrà essere fornita evidenza scritta. In ogni caso, dovrà tenersi conto, in relazione alle specifiche fattispecie di reato di seguito indicate, delle seguenti previsioni.

LE FALSE COMUNICAZIONI SOCIALI

Per la prevenzione dei reati relativi alla predisposizione delle comunicazioni indirizzate ai soci e al pubblico in generale, nonché ai fini della formazione del bilancio, è necessario che la procedura aziendale contenga presidi di controllo al fine di consentire:

- il rispetto dei principi di compilazione dei documenti contabili di cui agli artt. 2423, 2423 *bis*, 2423 *ter* cod. civ.;
- il rispetto del principio di completezza del bilancio, mediante l'indicazione di tutti i dati prescritti dalla normativa vigente (cfr., artt. 2424 e ss. cod. civ.);
- l'elencazione dei dati e delle notizie che ciascuna funzione aziendale interessata deve fornire;
- l'indicazione delle altre funzioni aziendali a cui i dati devono essere trasmessi; i criteri per la loro elaborazione; la tempistica di consegna;
- la trasmissione dei dati alla funzione responsabile per via informatica, affinché resti traccia dei vari passaggi e siano identificabili i soggetti che hanno operato;

- la tempestiva trasmissione, all'Amministratore Unico, della bozza di bilancio, garantendo l'idonea registrazione di tale trasmissione;
- la giustificazione di ogni eventuale variazione dei criteri di valutazione adottati per la redazione dei documenti contabili sopra richiamati e delle relative modalità di applicazione. Tali situazioni devono, in ogni caso, essere tempestivamente comunicate all'OdV unitamente a:
- la preventiva approvazione, da parte degli organi aziendali competenti, delle operazioni societarie potenzialmente rilevanti ai fini del Decreto, qualora siano caratterizzate da una discrezionalità di valutazione che possa comportare significativi impatti sotto il profilo patrimoniale o fiscale;
- la tracciabilità delle operazioni che comportino il trasferimento e/o il deferimento di posizioni creditorie.

LA TUTELA DEL CAPITALE SOCIALE

Per la prevenzione dei reati relativi alla gestione delle operazioni concernenti conferimenti, distribuzione di utili o riserve, sottoscrizione ed acquisto di azioni o quote sociali, operazioni sul capitale, fusioni e scissioni, la procedura seguita in azienda dovrà prevedere:
- l'esplicita approvazione, da parte dell'Amministratore Unico, di ogni attività relativa alla costituzione di nuove società, all'acquisizione o alienazione di partecipazioni societarie, nonché in merito alla effettuazione di conferimenti, alla distribuzione di utili o riserve, a operazioni sul capitale sociale, a fusioni e scissioni.

CONFLITTI DI INTERESSE

In materia di conflitti di interesse, è necessario che i protocolli aziendali garantiscano la definizione dei casi in cui si potrebbero verificare i conflitti di interesse, prescrivendo e/o indicando:
- la raccolta di una dichiarazione periodica in merito ai potenziali conflitti di interesse e del rispetto del Codice Etico dal management della Società;
- l'individuazione puntuale dei soggetti che devono presentare tali dichiarazioni;
- le tempistiche e le responsabilità per il monitoraggio delle medesime dichiarazioni;
- i criteri per l'identificazione delle situazioni di potenziale conflitto di interesse;

- le regole comportamentali da seguire in occasione della effettuazione di operazioni straordinarie, ovvero della elaborazione di situazioni economiche, patrimoniali e finanziarie di carattere straordinario.

La Società, in ottemperanza ai principi sopra esposti, ha adottato una specifica procedura in materia di conflitto di interesse ed ha inserito specifiche previsioni nel Codice Etico.

6 FALSE O OMESSE DICHIARAZIONI PER IL RILASCIO DEL CERTIFICATO PRELIMINARE (ART. 54 D.LGS. N. 19/2023)

La condotta criminosa prende corpo quando si costruiscono documenti falsi o si alterano i veri, oppure tramite dichiarazioni non veraci o omissioni di informazioni si vuole dimostrare di aver adempiute a tutte le richieste per l'ottenimento del certificato preliminare nelle trasformazioni, fusioni e scissioni transfrontaliere

In caso di condanna ad una pena non inferiore a mesi otto di reclusione per questa fattispecie di reato è prevista l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

A tal fine, è espressamente vietato che il personale apicale addetto alla Predisposizione di bilanci, alla documentazione di natura contabile e alla predisposizione di documenti veritieri, falsifichi la documentazione per dimostrare di aver adempiuto a tutte le richieste per l'ottenimento del certificato preliminare.

7 CAMPO DI APPLICAZIONE NELL'ATTIVITA' DI PREDISPOSIZIONE DEL BILANCIO E RESPONSABILE DELLA PROCEDURA

La presente procedura si applica a tutti i soggetti coinvolti nelle attività di contabilità generale e predisposizione del bilancio della Società ed in particolare nei confronti dell'AU, del RAM e del REC

Il responsabile principale dell'attività di predisposizione del bilancio è l'Amministratore Unico. In via sussidiaria ne rispondono il RAM/RRU e il REC, nonché tutti i soggetti esterni (ovvero i consulenti) che operano per conto della Società.

8 PRINCIPI GENERALI DI COMPORTAMENTO

L'Amministratore Unico è responsabile della predisposizione del Bilancio e della pubblicazione di dati non veritieri e corretti, salvo il caso in cui il fatto sia imputabile al comportamento colposo o doloso del professionista incaricato della medesima predisposizione.

Tutte le Funzioni Aziendali, interne ed esterne, a qualsiasi titolo coinvolte nelle attività di tenuta della contabilità e della successiva predisposizione/deposito delle comunicazioni sociali in merito alla situazione economico e patrimoniale di GETOPEN, sono tenute ad osservare le modalità esposte nella presente procedure, nelle previsioni di legge esistenti in materia, nonché nelle procedure che disciplinano le attività in questione, norme tutte improntate a principi di trasparenza, accuratezza e completezza delle informazioni contabili al fine di produrre situazioni economiche, patrimoniali e finanziarie veritiere e tempestive anche ai sensi ed ai fini di cui agli artt. 2621 e 2622 del Codice Civile.

IN PARTICOLARE, LE FUNZIONI AZIENDALI SONO TENUTE A:

• rispettare i principi contabili di riferimento;

• osservare, nello svolgimento delle attività di contabilizzazione dei fatti relativi alla gestione della Società e di formazione del bilancio, un comportamento corretto, trasparente e collaborativo;

• procedere alla valutazione e registrazione di elementi economico patrimoniali nel rispetto dei criteri di ragionevolezza e prudenza, illustrando con chiarezza, nella relativa documentazione, i criteri che hanno guidato la determinazione del valore del bene;

• fornire ai soci e terzi (Banche, Enti pubblici, ecc.) in generale informazioni veritiere e complete sulla situazione economica, patrimoniale e finanziaria della Società e sull'evoluzione delle relative attività;

• assicurare che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima, coerente e congrua;

• garantire la completa tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte, archiviando in maniera corretta e dettagliata i documenti di supporto.

I Destinatari che, per ragione del proprio incarico o della propria funzione o mandato, siano coinvolti nella gestione degli adempimenti degli organi sociali, devono:

• rispettare le regole e i principi contenuti nel Codice Civile o altre normative e regolamenti vigenti;

• osservare scrupolosamente tutte le norme di legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;

• assicurare il regolare funzionamento della società e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare nel rispetto delle leggi vigenti;

• non ostacolare l'esercizio delle funzioni di vigilanza svolte da parte di pubbliche autorità, attuato consapevolmente ed in qualsiasi forma, anche omettendo le comunicazioni dovute alla autorità medesime;

AI DESTINATARI È FATTO ESPRESSO OBBLIGO DI:

• rispettare le previsioni contenute nel Codice Etico e nel Modello;

• rispettare le procedure ed i protocolli interni che disciplinano specificamente i comportamenti che i medesimi devono tenere per evitare la commissione delle fattispecie criminose di cui al precedente paragrafo;

• tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio, delle situazioni patrimoniali e contabili di periodo e delle comunicazioni sociali in genere, al fine di fornire ai destinatari di tali comunicazioni (soci, creditori e terzi in genere) un'informazione rispondente al vero e corretta sullo stato economico, patrimoniale e finanziario in cui versa la Società. Più precisamente, in questo contesto, è assolutamente vietato predisporre, redigere,

trasmettere e/o comunicare, in qualsivoglia modo e forma, dati e informazioni inesatti, errati, incompleti, lacunosi e/o falsi aventi ad oggetto lo stato patrimoniale economico e finanziario della Società, ovvero compiere qualsivoglia omissione nella predisposizione, redazione, trasmissione e/o comunicazione di tali dati e/o informazioni;

• osservare con la massima diligenza e rigore tutte le disposizioni legislativamente previste a tutela dell'integrità e conservazione del capitale sociale; tutto ciò allo scopo precipuo di non ledere in alcun modo il legittimo affidamento riposto dai creditori e dai terzi in genere. In questo ambito, è assolutamente vietato: **(a)** al di fuori dei casi legislativamente previsti di riduzione del capitale sociale, restituire i conferimenti effettuati a qualsivoglia titolo dai soci o rilasciare agli stessi soci liberatorie, espresse o tacite, dall'obbligo di eseguire i conferimenti in questione; **(b)** eseguire ripartizioni degli utili o di acconti di utili inesistenti o effettuare ripartizioni di somme destinate per legge a riserve indistribuibili secondo le vigenti disposizioni; **(c)** effettuare riduzioni del capitale sociale, fusioni con altra società o scissioni al fine di cagionare un danno ai creditori sociali; **(d)** aumentare fittiziamente in ogni modo o forma il capitale sociale;

• garantire il corretto funzionamento degli organi sociali e più in generale della Società;

• assicurare per ogni operazione contabile la corretta conservazione agli atti sociali di adeguata documentazione a supporto dell'attività svolta, in modo da consentire: **(a)** la corretta registrazione contabile; **(b)** l'individuazione dei diversi livelli di responsabilità; **(c)** la ricostruzione accurata dell'operazione, anche al fine di ridurre la probabilità di errori interpretativi.

I Responsabili sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

8.1 CONTROLLI SPECIFICI

CON RIFERIMENTO ALL'ATTIVITÀ DI "FORMAZIONE DEL BILANCIO E PROCESSO FISCALE", LA SOCIETÀ HA IMPLEMENTATO I SEGUENTI CONTROLLI:

• sono presenti specifici principi e regole di condotta nel Codice Etico aventi ad oggetto la trasparenza delle operazioni contabili.

• la gestione degli aspetti fiscali ordinari (es. dichiarazione IVA annuale, dichiarazione dei redditi ai fini IRES e IRAP, dichiarazione dei sostituti d'imposta e certificazioni uniche etc.) è demandata ad uno Consulente esterno;

• La redazione e compilazione delle dichiarazioni viene predisposta dal consulente esterno attraverso l'estrazione dei dati dal sistema gestionale amministrativo contabile.

• LA SOCIETÀ HA FORMALIZZATO APPOSITO CONTRATTO CON LO STUDIO ESTERNO AVENTE AD OGGETTO:

▪ Gestione degli adempimenti fiscali;

▪ Tenuta della contabilità;

▪ Predisposizione bilancio annuale.

• lo Studio esterno si occupa della predisposizione dei seguenti documenti: lo stato patrimoniale, il conto economico e la nota integrativa in conformità alle leggi vigenti in Italia.

La bozza del bilancio, dopo essere stata predisposta, viene sottoposta all'Amministratore Unico della società per l'approvazione.

• LA CONTABILITÀ VIENE GESTITA DALLO STUDIO ESTERNO, SULLA BASE DEI DOCUMENTI CONTABILI ACQUISITI. IN PARTICOLARE, L'ATTIVITÀ COMPRENDE:

▪ il controllo formale dei documenti ricevuti;

▪ la registrazione dei documenti.

8.2 LA TENUTA DELLA CONTABILITÀ PRESSO UN CONSULENTE ESTERNO

GETOPEN conferisce - con apposito mandato o lettera di incarico professionale, contenenti specifiche clausole relative all'osservanza dei principi e delle norme di condotta previste dal Codice Etico e dal Modello 231 – l'affidamento per la tenuta della contabilità a professionisti esterni, coadiuvati da un responsabile interno ad GETOPEN e preposto alla raccolta, tenuta e trasmissione di tutta la contabilità della Società al REC.

L'attività di registrazione dei dati contabili deve essere svolta in osservanza agli obblighi di legge ed ai principi contabili nazionali e deve essere finalizzata ad assicurare la correttezza e l'affidabilità delle medesime registrazioni e dei *report* gestionali, nonché il tempestivo adempimento di tutti gli obblighi previsti dalle vigenti disposizioni di legge.

8.3 PREVENZIONE DEI RISCHI E PROCEDURE DI CONTROLLO

Le norme penali a cui il Decreto 231 fa riferimento in tema di reati societari, richiedono l'intenzionalità della condotta, ossia la volontarietà della falsa comunicazione. Pertanto, se non vi è una forma di partecipazione cosciente e volontaria il reato non sarà configurabile.

GETOPEN garantisce la sussistenza delle necessarie competenze specialistiche dei professionisti esterni incaricati della tenuta della contabilità e, dunque, in ordine alla corretta applicazione delle norme tecniche in materia di formazione e valutazioni di bilancio (i c.d. principi contabili). La procedura di contabilizzazione e rilevazione dei dati, a sua volta, garantirà la correttezza delle informazioni sottostanti. Tutto ciò, complessivamente, si ritiene idoneo ad impedire la formulazione di una errata indicazione di importi nel bilancio o una errata esposizione di fatti nella nota integrativa.

Va peraltro evidenziato che, in generale, la definizione delle procedure aziendali in ambito amministrativo e dei connessi sistemi di controllo interno, acquisisce ulteriore valenza in termini di prevenzione dai rischi di commissione dei reati, se viene supportata dal monitoraggio dei relativi comportamenti e adempimenti; tale monitoraggio costituisce un valido strumento d'individuazione delle "*aree a rischio*" nel sistema gestionale di settore e d'impresa.

L'AMMINISTRATORE UNICO HA IL DOVERE DI VIGILARE SULL'INTERO PROCEDIMENTO CHE PORTA ALLA FORMAZIONE DEL BILANCIO ED, IN PARTICOLARE DOVRÀ:

1. monitorare l'identificazione dei dati e le notizie ricevute dal RAM/RRU e dal REC ai fini della predisposizione del bilancio;

2. assicurare che i documenti analizzati dovranno essere caricati e tenuti in apposito archivio informatico all'uopo predisposto nella piattaforma digitale di condivisione;

3. effettuare, a campione, un controllo sulla correttezza delle registrazioni contabili, eseguite dalle funzioni preposte;

4. garantire la formazione dei dipendenti coinvolti nella redazione del bilancio. All'uopo verranno organizzati dall'AU e/o RAM/RRU dei corsi di formazione sulle principali nozioni e problematiche giuridiche e contabili relative alla predisposizione del bilancio;

5. assicurare l'applicazione dei principi di trasparenza e veridicità nei controlli effettuati dall'Amministratore Unico;

6. prima di procedere all'approvazione del bilancio, riunirsi con l'Organismo di Vigilanza, l'AU (o, se delegato, il RAM/RRU) e il REC, al fine di analizzare eventuali criticità nell'attività di revisione.

Il rispetto dei principi fissati dal presente protocollo per le procedure aziendali di redazione ed approvazione del bilancio, unitamente al rispetto della legislazione vigente ed all'applicazione dei principi contabili nazionali e internazionali, consentiranno l'adozione di decisioni sui valori delle poste valutative del conto economico e dello stato patrimoniale, improntate sulla base di riscontri oggettivi e documentati, nel rispetto dei criteri di prudenza, veridicità e trasparenza, con riscontro esaustivo nella nota integrativa.

Inoltre, in occasione dell'approvazione del bilancio, il RAM/RRU, o la funzione eventualmente preposta a coadiuvare il REC nella redazione del bilancio, dovrà rilasciare un'apposita attestazione convalidata dal medesimo REC, attestante:

a. la veridicità e correttezza, la precisione e completezza dei dati e delle informazioni contenute nel bilancio, ovvero di tutti i documenti connessi, nonché degli elementi informativi messi a disposizione dalla società;

b. l'insussistenza di elementi da cui poter desumere che le dichiarazioni e i dati raccolti contengano elementi incompleti o inesatti;

c. l'insussistenza di elementi di non conformità riscontrati nell'attività prestata e l'indicazione della competenza dimostrata da parte del professionista incaricato della consulenza per la redazione del bilancio;

d. il rispetto delle procedure tese a fornire una ragionevole certezza sulla completezza delle informazioni e dei dati contenuti nei documenti utilizzati.

La suddetta attestazione deve essere trasmessa, prima dell'approvazione del bilancio, all'OdV, il quale potrà chiedere di esaminare la bozza di bilancio prima della data fissata per la sua adozione.

8.4 CONTROLLO DEI BILANCI INFRANNUALI

Il REC, trimestralmente e previo confronto con il RAM/RRU, dovrà caricare nell'apposito archivio informatico all'uopo predisposto nella piattaforma digitale di condivisione, le liquidazioni periodiche IVA, così da sottoporle all'attenzione dell'AU, il quale dovrà controllarle e vistarle, con firma digitale o con firma olografa.

Il REC dovrà segnalare eventuali difformità rilevate nella disamina di documenti contabili per la redazione del bilancio all'OdV.

In particolare, dovranno essere attenzionate, a titolo meramente esemplificativo e non esaustivo, le seguenti voci: operazioni esenti IVA, gestione degli omaggi, capitalizzazione di cespiti e diritti pluriennali e relativi ammortamenti, dismissione di cespiti e diritti pluriennali, valorizzazione del magazzino, gestione dei fondi svalutazione e rischi, *etc.*

Di tali attività, l'OdV dovrà avere puntuale evidenza attraverso la trasmissione, con cadenza trimestrale, dei suddetti documenti.

8.5 DISTRIBUZIONE DI DIVIDENDI E GESTIONE DELLE OPERAZIONI STRAORDINARIE

Ogni operazione idonea a incidere nel patrimonio indisponibile della Società, non può essere effettuata se non previa e puntuale verifica della consistenza dello stato patrimoniale.

L'Amministratore Unico dovrà, previamente, informare l'OdV delle adunanze dell'assemblea dei soci aventi all'ordine del giorno la distribuzione dei dividendi,

l'approvazione del bilancio e l'autorizzazione a potere eseguire operazioni straordinarie di impresa (come fusione, scissione *etc.*).

In particolare, nella gestione delle operazioni straordinarie (es. fusioni, acquisizioni e dismissioni, ecc.) è richiesto che:

• ogni operazione sia sottoposta ed approvata dall'Amministratore Unico e/o dal Consiglio di amministrazione delle società interessate all'operazione straordinaria;

• sia sempre predisposta idonea documentazione a supporto dell'operazione, da parte della funzione aziendale proponente o competente all'istruzione della pratica con particolare attenzione ad operazioni di acquisizione e/o cessione con controparti che hanno la propria sede in stati esteri che non garantiscono la trasparenza societaria o abbiano una fiscalità privilegiata;

• prima di effettuare qualsiasi operazione di costituzione e/o acquisizione del controllo, anche in via indiretta, di società o enti assimilabili aventi sede legale in uno Stato estero, deve essere preventivamente verificato che lo Stato in cui la società ha sede: **(a)** garantisca un regime di trasparenza dell'informazione societaria compatibile con il regime di trasparenza in materia garantito dagli Stati dell'Unione Europea; **(b)** non sia presente nell'elenco dei Paesi a regime fiscale privilegiato (c.d. "black list");

• nelle ipotesi di costituzione e/o acquisizione del controllo, anche in via indiretta, di società o enti assimilabili che abbiano la propria sede in Stati esteri che non garantiscano la trasparenza societaria devono essere espresse le ragioni di natura imprenditoriale che giustificano l'operazione;

• sia verificata preliminarmente da parte della funzione aziendale competente, la completezza, inerenza e correttezza della documentazione di supporto dell'operazione, ai fini della registrazione contabile;

• in caso di operazioni straordinarie, sia previsto, anche attraverso il supporto di eventuali Advisor specialistici, l'avvio di attività di Due Diligence sull'oggetto della compravendita.

IL RAPPORTO DI DUE DILIGENCE DEVE CONTENERE:

▪ nominativi delle persone che hanno condotto le attività di Due Diligence;

▪ esami effettuati e i relativi esiti;

▪ deduzioni e raccomandazioni fatte;

▪ eventuali modifiche agli accordi da proporre alla controparte.

9 AREA SENSIBILE CONCERNENTE I REATI TRIBUTARI - MANCATO PAGAMENTO DI IMPOSTE

La disciplina dei reati tributari, che la puntuale ed attenta osservanza della presente procedura mira a prevenire, è stata riformata dal D. L. 124/2019, il cui articolo 39 ha introdotto nel D. Lgs. 231/2001 i reati tributari con effetto dal 24 dicembre 2019. L'articolo 5 del D. Lgs. 75/2020 vi ha poi aggiunto i reati di omessa o infedele dichiarazione e di indebita compensazione, ed ha reso punibili - modificando l'articolo 6 del D. Lgs.74/2000 - anche i reati dichiarativi di cui agli articoli 2, 3 e 4 solo tentati, con effetto dal 30 luglio 2020.

Si ricorda che ai sensi dell'art. 26 del D. Lgs. 231/2001 la responsabilità degli enti per i delitti tentati non sussiste se l'ente volontariamente impedisce la finalizzazione dell'azione o il verificarsi dell'evento.

Recentemente la normativa in materia è stata modificata dal D. Lgs. N. 87 del 14.06.2024, "revisione del sistema sanzionatorio tributario", con la modifica del testo art. 10 quater D. Lgs 74/2000 (indebita compensazione) che ha interessato la fattispecie dei reati previsti dall'art. 25- quinquesdecies (reati tributari) D. Lgs. 231/2001.

INDEBITA COMPENSAZIONE (ART. 10-QUATER D. LGS. 74/2000) INSERITO DA D.LGS.N.75 DEL 14 LUGLIO 2020 E MODIFICATO DA D.LGS N. 87 DEL 14 GIUGNO 2024)

TALI REATI PUNISCONO RISPETTIVAMENTE CHI:

• nelle dichiarazioni annuali dei redditi o IVA indica elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi inesistenti, e siano superate determinate soglie di rilevanza penale;

• non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte (o la dichiarazione di sostituto di imposta) quando è superata una determinata soglia di imposta evasa;

• non versa le imposte dovute utilizzando in compensazione crediti non spettanti, per un importo annuo superiore a una determinata soglia.

Dette condotte comportano anche la responsabilità amministrativa ai sensi del D. Lgs. 231/2001 solo se hanno ad oggetto l'evasione dell'IVA per un importo non inferiore a € 10 milioni e se sono commesse nell'ambito di sistemi fraudolenti transfrontalieri.

In presenza di entrambe le circostanze il reato di dichiarazione infedele è punito, ai sensi dell'art. 6 del D. Lgs. 74/2000, anche se è solo tentato, quando cioè sussistano atti preparatori, quali ad esempio l'omissione di obblighi di fatturazione, che potranno quindi aver effetto sulla successiva dichiarazione, se tali fatti siano compiuti anche nel territorio di un altro Stato membro dell'UE.

Nel caso di mancato pagamento di imposte, l'AU deve verificare, annualmente, l'eventuale superamento delle soglie penali integranti reati perseguibili a carico del rappresentante legale. L'esito di tale verifica dovrà essere trasmesso all'OdV.

AL FINE DI PREVENIRE LA COMMISSIONE DI REATI FISCALI E LA SOTTRAZIONE FRAUDOLENTA, È FATTO ESPRESSO DIVIETO DI:

1) eludere o tentare di eludere, la procedura di riscossione coattiva, attraverso l'alienazione simulata di beni e/o la realizzazione di atti fraudolenti su beni propri o altrui;

2) indicare, nella documentazione presentata nell'ambito di contenziosi fiscali, elementi attivi o passivi diversi da quelli reali.

3) indicare, nella documentazione presentata nell'ambito di contenziosi fiscali, elementi attivi o passivi diversi da quelli reali.

Tutti i Destinatari dei superiori obblighi dovranno informare, tempestivamente, l'ODV di tutti i contenziosi della Società con l'Erario.

Tra i reati che la presente procedura mira a prevenire, si indicano qui di seguito:

DICHIARAZIONE FRAUDOLENTA MEDIANTE USO DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 2 D.LGS. 74/2000)

L'ipotesi di reato di cui all'art. 2 D.Lgs. 74/2000 mira a colpire l'utilizzo di fatture o di altra documentazione fiscale (ricevute, bolle, etc.) mendace, formata cioè al

solo scopo di fornire una rappresentazione contabilmente “spendibile” di operazioni economiche inesistenti, e ciò con la finalità di abbattere l’imponibile fiscale, ovvero di falsare i meccanismi di liquidazione e versamento dell’imposta sul valore aggiunto. La fattispecie penale non richiede il superamento di alcuna soglia di punibilità e, dunque, trova applicazione qualunque sia l'ammontare di imposta evaso. La norma, inoltre, nel riferirsi all'uso di fatture o altri documenti concernenti operazioni inesistenti, non distingue tra quelle che sono tali dal punto dì vista oggettivo o soggettivo. Ai fini della configurabilità del reato, inoltre, è necessario il dolo specifico, rappresentato dal perseguimento della finalità evasiva, che deve aggiungersi alla volontà di realizzare l'evento tipico (la presentazione della dichiarazione). Tale elemento soggettivo, secondo un indirizzo giurisprudenziale, è compatibile con il dolo eventuale, ravvisabile nell'accettazione del rischio che l'azione di presentazione della dichiarazione, comprensiva anche di fatture o altri documenti per operazioni inesistenti, possa comportare l'evasione delle imposte dirette o dell'IVA. L'art. 2, comma 2, della stessa disposizione precisa che, affinché sia configurabile la fattispecie penale, tali fatture o tali documenti devono essere registrati nelle scritture contabili obbligatorie ovvero detenuti a fine di prova nei confronti dell'amministrazione finanziaria. L'utilizzazione delle fatture per operazioni inesistenti, infatti, costituisce un ante factum meramente strumentale alla realizzazione dell'illecito. Dal momento che l’impresa non è solo un soggetto produttivo di ricchezza bensì anche, e conseguentemente, una parte del rapporto impositivo (in veste di soggetto passivo, talvolta anche di sostituto o responsabile di imposta, etc.), evidente la possibile inerenza di tali condotte delittuose all’attività degli enti collettivi e delle persone giuridiche. Per effetto dell’art. 39 del DL 26 ottobre 2019, n. 124, convertito, con modificazioni, dalla Legge 19 dicembre 2019, n. 157, il reato di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti è ora sanzionato con la pena della reclusione da 4 a 8 anni (la pena della reclusione andava originariamente da 1 anno e 6 mesi a sei anni). È prevista una circostanza attenuante con il nuovo comma 2-bis, stabilendo che se l'ammontare degli elementi passivi fittizi è inferiore a 100.000,00

euro la cornice edittale è ridotta da un anno e sei mesi a sei anni (secondo alcuni commentatori la fattispecie attenuata costituirebbe un reato autonomo).
È previsto altresì il ricorrere di una causa di non punibilità se il debito tributario, compresi sanzioni e interessi, viene estinto mediante integrale pagamento degli importi dovuti, a seguito del ravvedimento operoso (e sempreché tale ravvedimento sia intervenuto prima che l'autore del reato abbia avuto formale conoscenza di accessi, ispezioni, verifiche o dell'inizio di qualunque attività di accertamento amministrativo o di procedimenti penali).
Si applica anche il comma 3 dell'art. 13 D.Lgs. n. 74/2000 secondo il quale, qualora, prima della dichiarazione di apertura del dibattimento di primo grado, il debito tributario sia in fase di estinzione mediante rateizzazione, anche ai fini dell'applicabilità dell'articolo 13-bis, è dato un termine di tre mesi per il pagamento del debito residuo.
Appare opportuno aggiungere che l'art. 39, comma 1, lett. q), sempre nel caso in cui sia integrato il reato suddetto, prevede l'applicazione della confisca "in casi particolari" di cui all'art. 240-bis cod. pen. (rendendo possibile, di conseguenza, il ricorso al sequestro cautelare prodromico a detta confisca), ma soltanto quando "l'ammontare degli elementi passivi fittizi è superiore a euro duecentomila".
La fattispecie penale in commento nella nuova versione si applica dal 24.12.2019 e dunque, considerato che il reato di perfeziona con la presentazione della dichiarazione fraudolenta, essa NON opera per la dichiarazione annuale relativa all'anno 2018 ma solo per le dichiarazioni IVA da presentarsi nell'aprile 2020 e per tutte le prossime dichiarazioni infrannuali ed annuali.

DICHIARAZIONE FRAUDOLENTA MEDIANTE ALTRI ARTIFICI (ART. 3 D.LGS. 74/2000)

L'ipotesi di reato di cui all'art. 3 D.Lgs. 74/2000 ha un campo di applicazione residuale rispetto a quella di cui all'art. 2: essa mira a dilatare la tutela penale dell'interesse erariale ricomprendendo nel concetto di frode anche l'utilizzo di documentazione mendace ulteriore e diversa rispetto a quella prevista dall'art. 2 e, con formula di chiusura, di altri "mezzi fraudolenti". La condotta incriminata consiste nel fatto di chi, fuori dei casi previsti dall'art. 2, al fine di evadere le imposte

sui redditi o l'IVA, indichi in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, avvalendosi di documenti falsi (vale a dire registrandoli nelle scritture contabili obbligatorie o detenendoli a fini di prova nei confronti dell'amministrazione finanziaria) o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria ovvero compiendo operazioni simulate oggettivamente o soggettivamente, quando, congiuntamente:

• l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a 30.000 euro;

• l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al 5% dell'ammontare dell'imposta medesima o comunque a euro trentamila. La giurisprudenza ha chiarito che il reato in esame, come modificato dall'art. 3 d.lgs. 24 settembre 2015, n. 158, è caratterizzato da struttura bifasica, nel senso che la condotta è articolata in due segmenti, presupponendo la compilazione e la presentazione di una dichiarazione mendace nonché la realizzazione di una attività ingannatoria prodromica. Nel caso in cui quest'ultima sia posta in essere da altri, il soggetto agente ne deve avere consapevolezza al momento della presentazione della dichiarazione (Corte di Cassazione Penale, Sez. 3, sentenza n. 15500 del 15/02/2019). Di recente, è stato ritenuto che il rilascio, da parte di professionista abilitato, di un mendace visto di conformità o di un'infedele certificazione tributaria, di cui rispettivamente agli artt. 35 e 36 d.lgs. 9 luglio 1997 n. 241, ai fini degli studi di settore, costituisce un mezzo fraudolento, idoneo ad ostacolare l'accertamento e ad indurre l'amministrazione finanziaria in errore, tale da integrare il concorso del professionista nel reato di dichiarazione fraudolenta mediante altri artifici (Corte di Cassazione Penale, Sez. 3, sentenza n. 19672 del

13/03/2019). Per effetto dell'art. 39 del DL 26 ottobre 2019, n. 124, convertito, con modificazioni, dalla legge 19 dicembre 2019, n. 157, il reato è ora punito con la reclusione da tre a otto anni (la cornice editatle sostituita era da un anno e sei mesi a sei anni). L'art. 39 cit., comma 1, lett. q), ha previsto anche per questo reato la confisca allargata, ma solo quando l'imposta evasa è superiore a euro 100.000. Anche qui trova applicazione la causa di non punibilità di cui all'art. 13, comma 2, D.Lgs. n. 74/2000 ed anche qui valgono le considerazioni svolte nel commento all'art. 2 del D.Lgs 74/2000 quanto alla operatività sotto il profilo temporale della norma.

EMISSIONE DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 8 D.LGS. 74/2000)

L'ipotesi di reato di cui all'art. 8 D.Lgs. 74/2000 è, di fatto, speculare rispetto a quella dell'art. 2 (che punisce l'utilizzazione della falsa documentazione). La disposizione in parola mira a reprimere la formazione e l'emissione della documentazione o di altri documenti per operazioni inesistenti. Nella prassi, la disposizione in commento è lo strumento normativo privilegiato di contrasto alla operatività delle cd. "cartiere", vale a dire di società e/o di strutture economiche che non svolgono alcuna reale attività produttiva ma che esauriscono la propria funzione nel produrre costi fittizi che altre società portano poi in contabilità, allo scopo di abbattere le poste attive e quindi la base imponibile del tributo. Con riferimento alla configurabilità di questo illecito, di recente, è stato ribadito che non è necessario, sotto il profilo soggettivo, che il fine di favorire l'evasione fiscale di terzi attraverso l'utilizzo delle fatture emesse sia esclusivo, essendo integrato anche quando la condotta sia commessa per conseguire anche un concorrente profitto personale (Corte di Cassazione Penale, Sez. 3, sentenza n. 39316 del 24/05/2019), così come è stato ribadito che la disposizione prevista dall'art. 9 d.lgs. 10 marzo 2000, n. 74, che, al fine di evitare che la medesima condotta sostanziale sia punita due volte, esclude la configurabilità del concorso di chi emette la fattura per operazioni inesistenti nel reato di chi se ne avvale e viceversa, non impedisce il concorso nell'emissione della fattura, secondo le regole ordinarie dell'art. 110 cod.

pen., di soggetti diversi dall'utilizzatore (Corte di Cassazione Penale, Sez. 3, sentenza n. 51468 del 18/06/2018). Il delitto in esame, inoltre, è reato istantaneo che si consuma nel momento di emissione della fattura ovvero, ove si abbiano plurimi episodi nel medesimo periodo di imposta, nel momento di emissione dell'ultima di esse, non essendo richiesto che il documento pervenga al destinatario, né che quest'ultimo lo utilizzi (Corte di Cassazione Penale, Sez. 3, sentenza n. 47459 del 05/07/2018).

Anche in questo caso la nuova normativa ha aumentato la pena, analogamente a quanto fatto per il parallelo delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti. La cornice edittale è adesso fissata da 4 a 8 anni di reclusione.

L'art. 39, comma 1, lett. m), del DL 26 ottobre 2019, n. 124, convertito con modificazioni dalla Legge 19 dicembre 2019, n. 157 ha introdotto nell'art. 8 una circostanza attenuante con il nuovo comma 2-bis: stabilendo che, se l'importo non rispondente al vero indicato nelle fatture o nei documenti - per periodo d'imposta - è inferiore a centomila euro, si applica la reclusione da un anno e sei mesi a sei anni. L'art. 39, comma 1, lett. q), poi, ha esteso l'istituto della confisca allargata anche a questo reato, ma solo quando l'importo non rispondente al vero indicato nelle fatture o nei documenti è superiore a euro 200.000. Dunque, mentre per l'applicazione della pena più grave è sufficiente che gli elementi passivi fittizi ammontino a 100 mila euro, per l'applicazione della confisca allargata tale importo deve essere raddoppiato.

OCCULTAMENTO O DISTRUZIONE DI DOCUMENTI CONTABILI (ART. 10 D.LGS. 74/2000)

L'ipotesi di reato di cui all'art. 10 D.Lgs. 74/2000 è finalizzata a fornire un presidio penalistico rispetto all'obbligo di tenuta delle scritture fiscali previsto dalla normativa di settore.

La finalità è quella di anticipare la tutela dell'interesse pubblico ad un effettivo concorso al prelievo fiscale degli operatori economici ad un momento precedente rispetto a quello della presentazione delle previste dichiarazioni fiscali (che vengono

naturalmente elaborate sulla base delle risultanze delle scritture contabili). Il reato è caratterizzato dalla presenza del dolo specifico di evasione.

La condotta incriminata consiste nel fatto di chi, salvo che il fatto costituisca più grave reato, al fine di evadere le imposte sui redditi o l'IVA, ovvero di consentire l'evasione a terzi, occulti o distrugga in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

La pena irrogabile è ora da tre a sette anni di reclusione; prima era da un anno e sei mesi a 6 anni. Questa fattispecie si applica in via residuale, ove non ricorra un più grave reato, e punisce chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

Non è stata prevista l'applicazione, nel caso in cui sia compiuto questo delitto, dell'istituto della confisca allargata.

SOTTRAZIONE FRAUDOLENTA AL PAGAMENTO DI IMPOSTE (ART. 11 D.LGS. 74/2000)

La disposizione in commento mira, da un lato (ipotesi del primo comma), ad una tutela rafforzata della garanzia patrimoniale generica dell'obbligazione tributaria: sono così sanzionate, con l'arma della pena detentiva, condotte simulatorie e fraudolente (del debitore di imposta o di terzi soggetti) miranti a vanificare gli effetti della riscossione coattiva. Dall'altro lato, il comma secondo della medesima disposizione intende garantire che eventuali accordi stragiudiziali con il fisco siano raggiunti dal contribuente su di un piano di leale collaborazione, sanzionando condotte dirette a falsare la base negoziale sulla quale l'amministrazione finanziaria e il debitore d'imposta concordano le rispettive partite
di dare/avere.

DICHIARAZIONE INFEDELE (ART. 4, D. LGS. N. 74/2000)

Il delitto di dichiarazione infedele punisce chi evidenzia nelle dichiarazioni tributarie ai fini delle impostedirette e dell'IVA "elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti". Il reato si considera

commesso nel caso di presentazione di una dichiarazione relativa a dette imposte ideologicamente falsa, perché rappresenta una situazione economico-patrimoniale difforme dal vero, in virtù dell'utilizzo di dati falsi, in modo da indurre in errore l'amministrazione finanziaria.

Per elementi attivi si intendono:

• i redditi fondiari;

• i redditi da capitale;

• i redditi diversi da plusvalenza;

• i redditi di impresa, costituiti dai ricavi, dalle plusvalenze patrimoniali, dalle sopravvenienze attive, dai dividendi, dagli interessi e dai proventi immobiliari;

• i redditi di lavoro autonomo, costituiti dai ricavi derivanti dall'esercizio di arti e professioni.

Gli elementi passivi rilevanti, invece, sono esclusivamente quelli inesistenti, come sopra definiti.

Il reato non si configura nel caso di non corretta classificazione, di valutazione di elementi attivi o passivi oggettivamente esistenti, rispetto ai quali i criteri concretamente applicati sono stati comunque indicati nel bilancio ovvero in altra documentazione rilevante ai fini fiscali, di violazione dei criteri di determinazione dell'esercizio di competenza, di non inerenza e di non deducibilità di elementi passivi reali.

Il reato rileva ai fini della responsabilità amministrativa da reato degli enti esclusivamente nel caso in cui sia commesso nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.

OMESSA DICHIARAZIONE (ART. 5, D. LGS. N. 74/2000)

Il reato punisce chi:

• al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte;

• non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta.

Il reato si consuma nel momento della mancata presentazione della dichiarazione.

Il reato rileva ai fini della responsabilità amministrativa da reato degli enti esclusivamente nel caso in cui sia commesso nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.

INDEBITA COMPENSAZIONE (ART. 10 QUATER, D. LGS. N. 74/2000) - INSERITO DAL D.LGS.N.75 DEL 14 LUGLIO 2020 E MODIFICATO DA D.LGS N. 87 DEL 14 GIUGNO 2024)

La condotta incriminata consiste nella redazione e successivo invio di un Modello F24 ideologicamente falso in quanto rappresentativo di crediti non spettanti o inesistenti che – imputati in compensazione – determinano, come effetto negativo dell'azione, il mancato versamento, totale o parziale, delle somme dovute.

I crediti non spettanti o inesistenti rilevanti ai fini della commissione del reato in esame sono quelli per i quali è consentita la compensazione in sede di versamento unitario e, in particolare:

- imposte dei redditi, relative addizionali e ritenute alla fonte;
- IVA;
- imposte sostitutive delle imposte sui redditi e dell'IVA;
- IRAP;
- contributi previdenziali dovuti da titolari di posizione assicurativa;
- contributi previdenziali ed assistenziali dovuti da imprenditori e committenti di prestazioni di collaborazione coordinata e continuativa;
- premi per l'assicurazione contro gli infortuni sul lavoro e le malattie professionali;
- interessi previsti in caso di pagamento rateale;
- altre entrate individuate con decreto del Ministero delle finanze.

Il reato rileva ai fini della responsabilità amministrativa da reato degli enti esclusivamente nel caso in cui sia commesso nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.

L'art. 39, comma 1, lett. m), del DL 26 ottobre 2019, n. 124, convertito con modificazioni dalla Legge 19 dicembre 2019, n. 157 ha introdotto nell'art. 8 una

circostanza attenuante con il nuovo comma 2-bis: stabilendo che, se l'importo non rispondente al vero indicato nelle fatture o nei documenti - per periodo d'imposta - è inferiore a centomila euro, si applica la reclusione da un anno e sei mesi a sei anni.

L'art. 39, comma 1, lett. q), poi, ha esteso l'istituto della confisca allargata anche a questo reato, ma solo quando l'importo non rispondente al vero indicato nelle fatture o nei documenti è superiore a euro 200.000. Dunque, mentre per l'applicazione della pena più grave è sufficiente che gli elementi passivi fittizi ammontino a 100 mila euro, per l'applicazione della confisca allargata tale importo deve essere raddoppiato.

Ancora, si precisa che con il D.Lgs. n.87 del 14 Giugno 2024 sono state apportate modifiche all'interno dell'Art.25-quinquiesdecies del D.Lgs 231/01 (Reati tributari), ed in particolare, all'art.10-quater "Indebita compensazione" è stato aggiunto il comma 2-bis che tratta della eventuale esclusione della punibilità dell'agente in merito a spettanze del credito.

In particolare, il testo del comma 2 bis prevede testualmente: "*La punibilità dell'agente per il reato di cui al comma 1 è esclusa quando, anche per la natura tecnica delle valutazioni, sussistono condizioni di obiettiva incertezza in ordine agli specifici elementi o alle particolari qualità che fondano la spettanza del credito*".

9.1 PRINCIPI ORGANIZZATIVI E DI CONTROLLO

Il presente paragrafo è inerente alle condotte poste in essere da Soggetti Apicali o Soggetti Sottoposti, nonché da Soggetti Terzi che svolgono le Attività sensibili, nell'ambito dei reati descritti nel presente capitolo.

I DESTINATARI, PERTANTO, DEVONO CONFORMARE LE PROPRIE ATTIVITÀ AI SEGUENTI PRINCIPI:

• rispettare le previsioni contenute nel Modello e nel Codice Etico;

• rispettare le procedure interne che disciplinano specificamente i comportamenti che i medesimi devono tenere per evitare la commissione delle fattispecie criminose di cui al presente capitolo.

9.2 REGOLE GENERALI DI COMPORTAMENTO

È FATTO ESPRESSO OBBLIGO AI DESTINATARI DI:

• svolgere le attività sensibili conformemente alle leggi vigenti, alle norme generali del Codice Etico, nonché alle disposizioni aziendali, ai protocolli di comportamento ed alle specifiche procedure previste dalla Società a presidio dei rischi di commissione del reato di cui alla presente parte speciale.

È FATTO ESPRESSO DIVIETO AI DESTINATARI DI:

• porre in essere, dare collaborazione o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;

• porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di resto rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

• porre in essere qualsiasi situazione di conflitto di interessi in relazione a quanto previsto dalle suddette ipotesi di reato;

• tenere un comportamento corretto e trasparente, assicurando pieno rispetto delle norme di legge, dei regolamenti, delle procedure interne, nelle attività finalizzate alla formazione del bilancio e di tutte le attività connesse, anche nelle fasi di acquisizione, elaborazione, comunicazione di dati aziendali, nonché di fatturazione e contabilizzazione;

• astenersi dal porre in essere operazioni fraudolente, simulate, diffondere notizie false, non corrette;

• garantire il regolare svolgimento delle assemblee, evitando condizionamenti;

• effettuare/ricevere elargizioni o promesse di danaro o altra utilità a/da pubblici funzionari, incaricati di pubblico servizio, soggetti privati, italiani o stranieri;

• distribuire/ricevere omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata

qualsiasi forma di regalo a/da funzionari pubblici ed a/da privati italiani ed esteri (anche in quei Paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o a/da loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere benefico o culturale. I regali offerti – salvo quelli di modico valore – devono essere documentati in modo adeguato per consentire le verifiche da parte dell'OdV;

• accordare vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti e/o appartenenti alla Pubblica Amministrazione Italiana o straniera, ovvero a privati, che possano determinare le stesse conseguenze previste al punto b);

• effettuare prestazioni in favore dell'Amministratore Unico, Dipendenti, Collaboratori, Consulenti e Partners a qualsiasi titolo della Società che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;

• riconoscere compensi in favore dell'Amministratore Unico, di Dipendenti, Collaboratori, Consulenti e Partners a qualsiasi titolo della Società che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;

• effettuare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari;

• intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo: soggetti legati all'ambiente del riciclaggio e/o della ricettazione e/o della evasione ed elusione fiscale, all'usura;

• utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;

• assumere, impiegare e/o gestire personale in violazione delle previsioni di legge e/o dei contratti
collettivi e comunque della dignità e libera determinazione individuale.

10 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

Tutti i *Destinatari* coinvolti nella predisposizione del bilancio e della relativa documentazione, devono comunicare, tempestivamente, all'Organismo di Vigilanza:

- eventuali situazioni anomale;
- eventuali violazioni della presente procedura;
- eventuali comportamenti non conformi a quanto previsto dal Modello e dal Codice Etico.

INOLTRE, L'AMMINISTRATORE UNICO È TENUTO A TRASMETTERE ALL'ORGANISMO DI VIGILANZA, CON PERIODICITÀ ALMENO SEMESTRALE, ULTERIORI INFORMAZIONI SPECIFICAMENTE RICHIESTE OVVERO:

- rilievi eventualmente segnalati dal RAMM e/o dal REC;
- rilevante modifica dell'assetto sociale ed eventuali casi di esclusione del diritto di voto per determinate categorie di soci.

I *Destinatari*, qualora dal processo di tenuta della contabilità e dalla redazione del Bilancio risultino voci e/o movimenti non giustificati – come ad es. "*sopravvenienze attive apparentemente non giustificate*" o casi "*di registrazioni di incassi e/o pagamenti*" di cui non si riscontri una contropartita di credito (o debito) corrispondente, sarà necessario comunicare, tempestivamente, le predette anomalie all'OdV.

I *Destinatari* devono, altresì, garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposto nell'apposita piattaforma di condivisione - tutta la documentazione necessaria.

Tutta la documentazione relativa alla tenuta della contabilità, alla predisposizione del bilancio e della documentazione connessa, è archiviata a cura del RAM/RRU, o della funzione eventualmente incaricata dall'AU, ed è tenuta a disposizione dell'OdV.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di *corporate governance* per la prevenzione dei reati di false comunicazioni sociali;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 20.03.2024	ADOZIONE
Rev. 1	Determina dell'Amministratore Unico del 05.08.2024	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231)

PARTE SPECIALE -4-

SOMMARIO

1 OBIETTIVI E FUNZIONE DEL MODELLO

Il presente protocollo si applica a tutte le Funzioni Aziendali di GETOPEN coinvolte nella gestione del processo di selezione e assunzione del personale.

Il processo potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di "Corruzione contro la Pubblica Amministrazione" nelle loro varie tipologie, "Induzione indebita a dare o promettere utilità", "Traffico di influenze illecite", nonché dei reati di "Corruzione tra privati" e "Istigazione alla corruzione tra privati".

Una gestione non trasparente del processo di selezione ed assunzione del personale, potrebbe, infatti, consentire la commissione di tali reati attraverso la promessa di assunzione verso rappresentanti della Pubblica Amministrazione, e/o esponenti apicali, e/o persone loro subordinate di società o enti controparti o in relazione con la Società, o soggetti da questi indicati, concessa al fine di influenzarne l'indipendenza di giudizio o di assicurare un qualsivoglia vantaggio per GETOPEN.

Nell'ipotesi di assunzione di soggetti facenti parti di Paesi Terzi, GETOPEN con la presente procedura ha fissato i principi finalizzati a prevenire il rischio della commissione del reato di "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

2 ACRONIMI AZIENDALI

AU	Amministratore Unico
RSGQ	Responsabile Sistema di Gestione Qualità
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RTEC/RPROG	Responsabile Tecnico/Responsabile Progettazione
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RSCM	Responsabile singola commessa
RATTR	Responsabile Attrezzature e Mezzi

PROG Programmatori

CDL Consulente del lavoro

REC Responsabile Esterno Contabilità

PER L'IDENTIFICAZIONE DEI SOGGETTI CHE CORRISPONDONO AGLI ACRONIMI AZIENDALI SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI GETOPEN S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di GETOPEN S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di GETOPEN S.r.l..

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

Come su esposto, il presente protocollo si applica a tutte le Funzioni Aziendali coinvolte nella gestione del processo di selezione e assunzione del personale.

Rientrano, dunque, nel campo di applicazione della procedura di selezione del personale dipendente il RAM/RRU e l'AU.

5 DESCRIZIONE DEL PROCESSO

Il processo di selezione e assunzione si articola nelle seguenti fasi:

- **SELEZIONE DEL PERSONALE:**

o analisi e richiesta di nuove assunzioni;

o definizione del profilo del candidato;

o reclutamento dei candidati;

o effettuazione del processo selettivo;

o individuazione dei candidati.

- **FORMALIZZAZIONE DELL'ASSUNZIONE.**

Resta nelle competenze delle Funzioni Aziendali specificatamente facoltizzate l'istruttoria relativa alla selezione ed assunzione di personale specialistico altamente qualificato ovvero di figure destinate a posizioni di vertice.

6 PRINCIPI DI CONTROLLO

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

• **LIVELLI AUTORIZZATIVI DEFINITI:**

- accentramento del processo di selezione e assunzione del personale in capo alla Funzione Aziendale competente che valuta la possibilità di assumere nuovo personale in coerenza con il budget ed i piani interni di sviluppo;
- autorizzazione all'assunzione concessa soltanto dal personale espressamente autorizzato dall'AU;

• **SEGREGAZIONE DEI COMPITI TRA I DIVERSI SOGGETTI COINVOLTI NEL PROCESSO.**

In particolare, l'approvazione finale dell'assunzione è demandata all'Amministratore Unico.

• **ATTIVITÀ DI CONTROLLO:**

- compilazione da parte del candidato, al momento dello svolgimento della selezione, di un'apposita modulistica per garantire la raccolta omogenea delle informazioni sui candidati;

• **TRACCIABILITÀ DEL PROCESSO SIA A LIVELLO DI SISTEMA INFORMATIVO SIA IN TERMINI DOCUMENTALI:**

- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Funzione Aziendale incaricata di procedere alla selezione e alla successiva assunzione del personale, è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta, anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo di selezione e assunzione del personale.

7 PRINCIPI DI COMPORTAMENTO

La selezione del Personale è effettuata in base alle esigenze aziendali e alla corrispondenza con i profili professionali ricercati, riconoscendo pari opportunità per i candidati.

Le informazioni richieste in sede di selezione sono strettamente collegate alla verifica del profilo professionale e psico-attitudinale ricercato, nel rispetto della sfera privata del candidato e delle sue opinioni personali. Non può costituire oggetto del colloquio l'analisi delle condizioni economiche personali del lavoratore o la valutazione del suo stato di bisogno.

La Società si avvale esclusivamente di Personale assunto in conformità alle tipologie contrattuali previste dalla normativa e dai contratti collettivi nazionali o territoriali di lavoro applicabili stipulati dalle associazioni sindacali più rappresentative a livello nazionale.

L'accesso ai ruoli e/o agli incarichi è definito in considerazione dell'affidabilità (in termini di diligenza e fedeltà), delle competenze e delle capacità dei singoli, sulla base delle specifiche esigenze della Società e senza discriminazione alcuna, compatibilmente con i criteri di efficienza generale del lavoro.

Salvo espressa e motivata deroga dell'Amministratore Unico, previo parere non vincolante dell'Organismo di Vigilanza, non possono essere assunti presso la Società:

- ✓ pubblici dipendenti con i quali negli ultimi due anni la Società abbia intrattenuto rapporti commerciali o comunque inerenti l'attività degli stessi pubblici dipendenti, loro parenti o affini o persone ad esse legate anche da un rapporto di amicizia o di interesse;
- ✓ soggetti che ricoprono cariche pubbliche o che svolgono incarichi pubblici tali da poterli porre in una situazione di conflitto di interessi, loro parenti o affini o persone ad esse legate anche da un rapporto di amicizia o di interesse;
- ✓ soggetti che abbiano subito sentenze di condanna passata in giudicato per reati dai quali possa derivare la responsabilità amministrativa ex d.lgs. 231/2001, o che per reati dello stesso tipo abbiano procedimenti penali in corso.

È, in ogni caso, fatto tassativo divieto a chiunque di promettere o concedere promesse d'assunzione, in favore di:

- rappresentanti della Pubblica Amministrazione;
- loro parenti o affini;
- persone segnalate dai soggetti di cui ai punti precedenti;

al fine di influenzare l'indipendenza di giudizio dei rappresentanti della Pubblica Amministrazione o di indurli ad assicurare un qualsiasi vantaggio per la Società.

I benefit sono gestiti nel rispetto della normativa previdenziale, contributiva e fiscale in materia.
Qualora la Società si avvalga di società esterne per l'espletamento di attività legate alla gestione del Personale, i contratti con tali società devono contenere un'apposita dichiarazione di conoscenza della normativa di cui al D.lgs. 231/2001 e di impegno al suo rispetto.

Le Funzioni Aziendali che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella selezione, assunzione e gestione del personale (anche in somministrazione ed anche straniero non comunitario) devono:
- operare nel rispetto del criterio di meritocrazia in relazione alle reali esigenze della società;
- garantire l'esistenza della documentazione attestante il corretto svolgimento delle procedure di selezione e assunzione;
- assicurare che la definizione delle condizioni economiche sia coerente con la posizione ricoperta dal candidato e le responsabilità/compiti assegnati;
- garantire che l'assunzione del personale avvenga sulla base di regolari contratti di lavoro, non essendo ammessa alcuna forma di rapporto lavorativo non conforme o comunque elusiva delle disposizioni normative vigenti;
- dimostrare l'impiego di lavoratori stranieri con valido permesso di soggiorno e monitorarne l'effettivo rinnovo, secondo i termini di legge;
- curare l'archiviazione di tutta la documentazione prodotta/ricevuta con riferimento alle attività propedeutiche e conseguenti alla presentazione della domanda di nulla osta, all'assunzione di lavoratori stranieri residenti all'estero;
- richiedere a ciascun dipendente, prima dell'assunzione, di produrre il casellario giudiziario ed il certificato dei carichi pendenti in corso di validità.

Le Funzioni Aziendali che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella selezione, assunzione e gestione del personale (anche straniero non comunitario) non possono:
- operare secondo logiche di favoritismo e/o pratiche discriminatorie;

- rendere promesse di assunzione e/o di avanzamento di carriera a risorse vicine a funzionari pubblici e a soggetti privati, qualora non venga rispettato il principio della meritocrazia;
- assumere personale, anche per contratti temporanei, senza il rispetto delle normative vigenti (ad esempio in termini di contributi previdenziali ed assistenziali, permessi di soggiorno, etc.);
- assumere o promettere l'assunzione nella società di impiegati della Pubblica Amministrazione (o loro parenti, affini, amici, etc.) o soggetti privati, che abbiano partecipato personalmente e attivamente ad una trattativa d'affari pubblica o privata, ovvero che abbiano partecipato, anche individualmente, a processi autorizzativi della Pubblica Amministrazione o ad atti ispettivi, nei confronti della Società, qualora non venga rispettato il principio della meritocrazia;
- impiegare lavoratori stranieri del tutto privi di permesso di soggiorno o con un permesso annullato, revocato o scaduto, per il quale non sia stata presentata domanda di rinnovo, documentata dalla relativa ricevuta postale;
- assumere un cittadino straniero non comunitario in Italia per motivi di turismo, anche se regolarmente munito della prescritta dichiarazione di presenza;
- fare ricorso, in qualsiasi forma, al lavoro minorile;
- assumere o promettere l'assunzione di soggetti, al fine di favorire o recare vantaggio ad organizzazioni criminali, ed in particolare ad associazioni di tipo mafioso e/o ad associazioni con finalità di terrorismo.

Le Funzioni Aziendali interessate sono tenute a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.1 L'ASSUNZIONE

Se le valutazioni sui candidati avranno esito positivo, sarà possibile procedere all'assunzione.

L'Amministratore Unico sottoscrive il contratto di assunzione.

7.2 IL PAGAMENTO DEL SALARIO MENSILE E LA GESTIONE DI RIMBORSI SPESE

Il CDL, elabora, mensilmente, un elenco con i pagamenti da effettuare in favore dei dipendenti che viene sottoposto al controllo dell'Amministratore Unico.

I rimborsi spese a ciascun dipendente devono essere eseguiti sulla base di evidenze documentali, di cui dovrà predisporsi apposito report.

In caso di concessione di *"fringe benefits"*, essi devono risultare dalla busta paga.

Gli avanzamenti di carriera sono stabiliti sulla base di valutazioni oggettive, in relazione alle competenze possedute ed a quelle potenzialmente esprimibili, in ragione della funzione da ricoprire.

Le retribuzioni eccedenti le misure fissate dai contratti collettivi, sulla base delle responsabilità e dei compiti della mansione attribuita al dipendente e, comunque, in riferimento ai valori medi di mercato, dovranno essere motivate dal CDL e, all'uopo, autorizzate per iscritto o digitalmente dall'Amministratore Unico.

INOLTRE, PER L'UTILIZZO DI RISORSE FINANZIARIE COLLEGATE AL PAGAMENTO DEGLI STIPENDI:

1. il pagamento deve essere effettuato, esclusivamente, sul conto corrente comunicato dal dipendente;
2. il pagamento deve corrispondere a quanto risultante dalla busta paga mensile; si precisa che, i rimborsi spese devono anch'essi risultare dalla busta paga, supportati dalle evidenze di spesa.

   E', tuttavia, possibile, laddove richiesto dal dipendente interessato, eseguire il pagamento di un anticipo sullo stipendio, purchè lo stesso venga annotato sull'apposito archivio informatico – all'uopo predisposto nella piattaforma digitale di condivisione – e successivamente, procedere al pagamento del saldo dovuto, dopo l'emissione della relativa busta paga;
3. vige il divieto di effettuare pagamenti su conti cifrati e di pagamento in favore di un soggetto diverso dalla controparte contrattuale;
4. il pagamento non può essere effettuato in un Paese terzo rispetto a quello delle parti contraenti o di esecuzione del contratto;
5. il pagamento effettuato su conti correnti di banche appartenenti od operanti in paesi elencati tra i c.d. "paradisi fiscali", o in favore di società "*off shore*", deve avvenire nel rispetto delle leggi in materia;
6. al momento dell'addebito del bonifico e al fine di garantire la tracciabilità del pagamento, conservare, nell'apposito archivio informatico - all'uopo

predisposto nella piattaforma digitale di condivisione -, la contabile di pagamento.

7.3 L'ADOZIONE DEL MODELLO E IL SISTEMA SANZIONATORIO

Ai nuovi assunti verrà consegnata copia cartacea (o digitale) del Modello 231 e del Codice Etico, a seguito della quale la risorsa, con la sottoscrizione del contratto di assunzione, si impegna: ***i)*** al rispetto dei principi e delle regole negli stessi contenuti; ***ii)*** a prendere, periodicamente, visione del Modello sul sito aziendale, al fine di verificare possibili revisioni che verranno apportate al medesimo in ragione di possibili aggiornamenti normativi.

La risorsa dovrà, inoltre, essere informata del fatto che la società ha adottato un sistema sanzionatorio, in aderenza a quanto previsto dal CCNL di riferimento, per cui eventuali violazioni del Modello e del Codice Etico potranno essere sanzionate e, i comportamenti più gravi, potranno sfociare nel licenziamento per giusta causa.

7.4 L'ASSUNZIONE DI PERSONALE STRANIERO

Il RAM/RRU, in collaborazione con l'eventuale Funzione richiedente e/o eventuali soggetti terzi, si impegna a rispettare i seguenti ulteriori presidi di controllo nella selezione ed impiego di cittadini stranieri non comunitari, garantendo la tracciabilità della documentazione prodotta in ogni fase del processo.

In caso di assenza del permesso di soggiorno, il RAM/RRU e/o eventuali soggetti terzi all'uopo incaricati:

- richiedono alle Autorità competenti il nulla osta e verificano l'effettivo ricevimento dello stesso da parte dello Sportello Unico Immigrazione;
- raccolgono copia del visto d'ingresso, rilasciato dall'ambasciata e/o consolato italiano presso lo stato straniero, per motivi di lavoro subordinato del lavoratore;
- mantengono copia del permesso di soggiorno o della ricevuta rilasciata dall'ufficio postale.

La documentazione di cui ai punti precedenti deve pervenire alla Società e/o ad eventuali soggetti terzi all'uopo incaricati, in data antecedente l'entrata in Italia del cittadino straniero non comunitario.

In caso di possesso di un valido documento di soggiorno, il RAM/RRU e/o eventuali soggetti terzi all'uopo incaricati:

- verificano che il cittadino straniero non comunitario, già soggiornante in Italia, sia munito di regolare documento in corso di validità che abiliti a prestare lavoro (permesso di soggiorno europeo per soggiornanti di lungo periodo; permesso per lavoro subordinato o autonomo, per attesa di occupazione, per famiglia, per assistenza ai minori, per asilo politico, per protezione sociale, per motivi umanitari);
- se pendente domanda di rinnovo del permesso di soggiorno, controllano la relativa ricevuta postale rilasciata dall'autorità preposta;
- comunicano l'assunzione al Centro per l'impiego, competente per la sede di lavoro, il giorno precedente all'inizio dell'attività, inviando lo specifico modello.

I cittadini stranieri assunti presso la Società devono essere specificamente evidenziati all'interno dell'anagrafica dipendenti; tali posizioni vengono monitorate e, per quelle prossime alla scadenza, il RAM/RRU provvede a richiedere la documentazione necessaria entro la data di scadenza.

Resta, comunque, inteso che la responsabilità di rinnovo del permesso di soggiorno è in capo ai singoli dipendenti; il RAM/RRU ne monitora esclusivamente le scadenze. Tale onere di monitoraggio può essere espressamente affidato, tramite apposita delega, al responsabile di Funzione eventualmente incaricato.

In ogni caso, GETOPEN e/o eventuali soggetti terzi all'uopo incaricati, ognuno per le parti di rispettiva competenza, si impegnano a garantire al lavoratore straniero non comunitario il trattamento retributivo ed assicurativo previsto dalle leggi vigenti e dai contratti collettivi nazionali di lavoro applicabili e ad effettuare, entro i termini di legge, le comunicazioni obbligatorie relative al rapporto di lavoro.

Nel caso in cui il lavoratore non adempia alle richieste di cui sopra o, comunque, non fornisca la relativa documentazione, il datore di lavoro – qualora il lavoratore fosse già stato assunto – potrà sospendere il rapporto di lavoro, in attesa dell'esito della procedura di rinnovo. In caso di esito negativo, il datore di lavoro potrà procedere con il licenziamento legittimo del lavoratore. Il RAM/RRU comunicherà

all'Amministratore Unico di procedere al licenziamento dei soggetti che non hanno ottenuto o richiesto il rinnovo.

7.5 LA TRACCIABILITÀ DELLE PRESENZE

Il RAM/RRU, consegna il *file* presenze dipendenti al Consulente del lavoro per l'elaborazione delle buste paga, e dovrà conservarlo nell'apposito archivio informatico – all'uopo predisposto nella piattaforma digitale di condivisione - per eventuali verifiche.

7.6 FORMAZIONE

Obiettivo principale di GETOPEN è garantire la corretta conoscenza da parte del personale del contenuto del Decreto e degli obblighi dal medesimo derivanti. La formazione e l'informazione del personale, in merito alla previsione normativa ed all'attuazione del Modello, è operata dall'Amministratore e dalle principali funzioni aziendali, di concerto con l'Organismo di Vigilanza. Le principali modalità di svolgimento delle attività di formazione/informazione necessarie, anche ai fini del rispetto delle disposizioni contenute nel Decreto, attengono la specifica informativa all'atto dell'assunzione e le ulteriori attività ritenute necessarie al fine di garantire la corretta applicazione delle disposizioni previste nel Decreto.

LA FORMAZIONE E L'INFORMAZIONE DEL PERSONALE RISULTERÀ COSÌ ARTICOLATA:

- istituzione di un vademecum iniziale di formazione, previsione di note informative interne, inserimento di una nota informativa nel corpo della lettera di assunzione, inerente all'adozione del presente Modello e del Codice Etico, nonché un invito a prendere visione dei relativi contenuti e a uniformarsi ai principi in esso descritti.

La formazione aziendale, nei confronti dei soggetti interessati, prevede pure la programmazione di corsi di aggiornamento e formazione periodica a seconda della necessità, col fine di assicurare che tutto il personale, ad ogni livello, sia consapevole della importanza della conformità delle proprie azioni rispetto al Modello organizzativo e delle possibili conseguenze dovute a comportamenti che si discostino dalle regole dettate dal Modello. L'impresa organizzerà la formazione e l'addestramento secondo le esigenze rilevate periodicamente, tenendo in considerazione le peculiarità delle diverse aree di rischio e delle professionalità del personale che vi opera. Al fine di garantire l'effettiva diffusione del Modello e

l'informazione del personale, con riferimento ai contenuti del Decreto e agli obblighi derivanti dall'attuazione del medesimo, sul sito aziendale è istituita una specifica sezione dedicata all'argomento, con rappresentazione di tutti i documenti che compongono il Modello, aggiornata su indicazione dell'Organismo di Vigilanza, compreso il Codice Etico.

Invero, l'attività di formazione, promossa dallo stesso ODV, è finalizzata a promuovere la conoscenza della normativa di cui al decreto legislativo 231/2001 e a fornire un quadro esaustivo della stessa, dei risvolti pratici che da essa discendono, nonché dei contenuti e principi su cui si basa il Modello Organizzativo e il relativo Codice Etico fra tutti i dipendenti che, pertanto, sono tenuti a conoscerli, osservarli e rispettarli, contribuendo alla loro attuazione.

La partecipazione ai corsi di formazione ha carattere obbligatorio.

8 GESTIONE DEI TRATTAMENTI PREVIDENZIALI E ASSISTENZIALI DEL PERSONALE

Qualsiasi contatto con esponenti della Pubblica Amministrazione per questioni inerenti il personale, deve essere annotato su apposito registro.

Qualsiasi documento diretto alla P.A. relativo alla gestione del personale, deve essere sottoposto al CDL.

9 LA GESTIONE DEGLI OMAGGI

Il Codice Etico stabilisce la politica di GETOPEN in merito alla ricezione e all'offerta di omaggi, ospitalità ed intrattenimenti (ossia erogazioni gratuite di beni e servizi, a fini promozionali o di pubbliche relazioni), delineando le relative responsabilità dei soggetti coinvolti nel processo.

Nell'ambito dei suddetti comportamenti e come disciplinato dal protocollo relativo alla gestione degli omaggi, è fatto divieto alla Società, ai suoi dipendenti e/o ai soggetti terzi in particolare, di concedere altri vantaggi di qualsiasi natura (es.: promesse di assunzione, *etc.*) in favore dei rappresentanti della Pubblica Amministrazione e/o soggetti privati, ovvero farsi concedere altri vantaggi.

10 SCELTA DEI CONSULENTI ESTERNI

La scelta e la gestione dei Consulenti deve rispondere esclusivamente a criteri di ragionevolezza, professionalità, integrità, correttezza e trasparenza nel rispetto delle modalità e dei poteri di spesa di tempo in tempo disciplinati dalla regolamentazione interna in materia.

IN PARTICOLARE:

- ✓ negli accordi o nei contratti che vengono stipulati con Consulenti devono essere inserite opportune clausole che consentano all'azienda di risolvere il rapporto qualora emergano comportamenti da parte degli stessi non in linea con le norme del Modello adottato da GETOPEN;
- ✓ le Funzioni Aziendali che si avvalgono del Consulente, o che sono designate responsabili del processo nel quale ricade l'attività dello stesso, devono conoscerne e valutarne il comportamento, informando l'Organismo di Vigilanza qualora emergano comportamenti contrari al rispetto dei principi contenuti nel presente Modello.

11 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

Tutte le Funzioni Aziendali coinvolte nella selezione e assunzione del personale informano, tempestivamente, l'Organismo di Vigilanza delle situazioni anomale e/o in contrasto con la presente procedura, nonchè di qualsivoglia comportamento non conforme alle disposizioni previste dal Codice Etico.

Inoltre, i soggetti a vario titolo coinvolti, sono tenuti a trasmettere all'Organismo di Vigilanza, con periodicità annuale:

- ➢ le assunzioni / avanzamenti di carriera e variazioni remunerative, relative a personale che abbia ricoperto cariche pubbliche e/o che abbia avuto esperienze lavorative in un ente pubblico;
- ➢ copia dei procedimenti disciplinari svolti e le eventuali sanzioni comminate, i provvedimenti assunti ovvero i provvedimenti motivati di archiviazione di procedimenti disciplinari a carico del personale aziendale.

I destinatari devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio ordinato – tutta la documentazione all'uopo necessaria.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di *corporate governance* per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari;

• con periodicità annuale, effettua dei controlli, anche documentali, tramite interviste al personale o al RAM/RRU, al fine di verificare gli orari dei lavoratori, controllare l'adeguatezza dei turni e del termine dell'orario di lavoro, del riposo settimanale, delle ferie, dell'aspettativa obbligatoria, delle agevolazioni previste dalla legge in materia di disabilità, maternità, paternità, malattia.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 20.03.2024	ADOZIONE
Rev. 1	Determina dell'Amministratore Unico del 20.03.2024	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231)

PARTE SPECIALE -5-

Sommario

1 OBIETTIVI E FUNZIONE DEL MODELLO

La Legge 48/2008 recante la "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*" ha introdotto nel Decreto l'art. 24 bis che ha inserito i reati informatici fra i reati presupposto del Decreto stesso.

La tematica è rilevante, considerata l'ormai enorme diffusione degli strumenti informatici e la circostanza che le aziende siano spesso esposte ad attacchi/violazioni dei propri sistemi informativi. Peraltro, con il recente aumento dell'utilizzo dello smart working, le aziende sono ancora più esposte al rischio di violazione delle misure tecniche adottate: l'uso di dispositivi e/o di connessioni di rete personali può, infatti, creare l'occasione per la commissione dei reati c.d. di criminalità informatica, che, come noto, ai sensi Decreto, possono comportare la responsabilità della Società ove gli stessi siano commessi nell'interesse o a vantaggio dell'ente.

2 ACRONIMI AZIENDALI

AU	Amministratore Unico
RSPP	Responsabile Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC/RPROG	Responsabile Tecnico/Responsabile Progettazione
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RATTR	Responsabile Attrezzature e Mezzi
RAM/RRU	Responsabile Amministrazione - Risorse Umane
PROG	Programmatori
RSCM	Responsabile singola commessa
CDL	Consulente del Lavoro
REC	Responsabile Esterno Contabilità

PER L'IDENTIFICAZIONE DEI SOGGETTI CHE CORRISPONDONO AGLI ACRONIMI AZIENDALI SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI GETOPEN S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di GETOPEN S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di GETOPEN S.r.l..

4 CAMPO DI APPLICAZIONE E RESPONSABILI DELLA PROCEDURA

Il presente protocollo deve essere osservato da tutte le Funzioni Aziendali coinvolte nella gestione e nell'utilizzo dei sistemi informatici della società.

Sono responsabili della procedura le funzioni aziendali coinvolte per ragioni del proprio incarico nella gestione e nell'utilizzo delle reti informatiche e, dunque, l'AU, il RSPP, il RSGQ, il RTEC, il RPROG, ed il RAM/RUU e tutti i dipendenti che utilizzano ed hanno accesso ai sistemi informatici della Società

5 AREE A RISCHIO

Nella presente Parte Speciale, si provvede dunque a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 24-bis del Decreto, e suddivisi tra:

 reati potenzialmente realizzabili;

 reati la cui commissione, per quanto non si possa escludere del tutto, è stata ritenuta remota/non ipotizzabile in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente gestita in considerazione del rispetto dei principi e delle regole comportamentali enunciate nel Codice Etico adottato dalla Società;

 reati non applicabili alla Società.

NELLO SPECIFICO:

REATO	RIFERIMENTO	REALIZZABILITA'
Falsità in un documento informatico pubblico	ART. 491 BIS C.P.	-
Accesso abusivo ad un sistema informatico o telematico	ART. 615-TER C.P.	POSSIBILE
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	ART.615-QUATER C.P.	POSSIBILE

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico o telematico	ART. 615-QUINQUIES C.P.	POSSIBILE
Intercettazione, impedimento o Interruzione illecita di comunicazioni informatiche o telematiche	ART. 617-QUATER C.P.	POSSIBILE
Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche	ART. 617-QUINQUIES C.P.	POSSIBILE
Danneggiamento di informazioni, dati e programmi informatici	ART. 635-BIS C.P	POSSIBILE
Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	ART. 635-TER C.P.	POSSIBILE
Danneggiamento di sistemi	ART. 635-QUATER C.P.	POSSIBILE
Danneggiamento di sistemi informatici o telematici di pubblica utilità	ART. 635-QUINQUIES C.P.	POSSIBILE
Frode informatica del certificatore di firma elettronica	ART. 640-QUINQUIES C.P.	NON APPLICABILE
Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica	ART. 1, COMMA 11, D.L. 21 SETTEMBRE 2019, N. 105	NON APPLICABILE

6 I REATI INFORMATICI E DI INDEBITO UTILIZZO DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

I REATI PRESUPPOSTO ELENCATI DALL'ART. 24 BIS DEL D. LGS. 231/2001 SONO:

IL PROCESSO DI GESTIONE E UTILIZZO DEGLI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI SI ARTICOLA NEI SEGUENTI PROCESSI:

• Carte di pagamento (carte di debito e di servizio, carte di credito, carte prepagate);

• Incassi e pagamenti (es. assegni, bonifici, addebiti diretti, RIBA – MAV – effetti);

• Servizi di Accesso ai Canali Digitali (accesso ed identificazione a distanza destinati a persone fisiche e persone giuridiche, altri servizi);

• Prevenzione delle frodi (Security Fraud Management);

• Gestione Reclami lamentele e disconoscimenti (Customer Relationship Management)

• Gestione risorse Umane con riferimento alle carte di credito aziendali e se rilasciate ai Dipendenti anche i buoni pasto e le carte di servizio per le autovetture (carta carburante, telepass).

ART. 615 TER C.P. - ACCESSO ABUSIVO AD UN SISTEMA TELEMATICO O INFORMATICO - MODIFICATO DALLA LEGGE N.90 DEL 28 GIUGNO 2024

La norma in esame punisce l'accesso non autorizzato ad un sistema informatico o telematico altrui, protetto da misure di sicurezza interne al medesimo, siano esse di tipo hardware o software.

La condotta illecita può concretizzarsi sia in un'attività di "introduzione" che di "permanenza" abusiva nel sistema informatico o telematico del proprietario del medesimo.

Il reato è aggravato, tra gli altri casi, se commesso da un soggetto che abusa della sua qualità di operatore del sistema informatico o telematico.

Il reato in questione, ad esempio, contrasta il fenomeno dei c.d. "hackers", e cioè di quei soggetti che si introducono nei sistemi informatici altrui, attraverso le reti telematiche, aggirando le protezioni elettroniche create dai proprietari di tali sistemi per tutelarsi dagli accessi indesiderati.

Tale reato si realizza quando un soggetto "abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto ad escluderlo". Tale delitto è punito con la reclusione fino a tre anni

La pena è della reclusione da uno a cinque anni, è stata con la Legge n.90 del 28 giugno 2024 aumentata da due a dieci anni:

- Se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la

professione di investigatore privato, o con abuso della qualità di operatore del sistema;

- Se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- Se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti

Qualora il delitto in oggetto riguardi sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni, da ultimo, ovvero con la Legge n.90 del 28 giugno 2024, la pena è stata aumentata da tre a dieci anni e da quattro a dodici anni.

Il delitto di accesso abusivo al sistema informatico rientra tra i delitti contro la libertà individuale. Il bene che viene protetto dalla norma è il domicilio informatico seppur vi sia chi sostiene che il bene tutelato è, invece, l'integrità dei dati e dei programmi contenuti nel sistema informatico. L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema.

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato

Il delitto di accesso abusivo a sistema informatico si integra, ad esempio, nel caso in cui un soggetto accede abusivamente ad un sistema informatico e procede alla stampa di un documento contenuto nell'archivio del PC altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso

abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura)

Il delitto potrebbe essere astrattamente commesso da parte di qualunque dipendente della società accedendo abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), ad esempio, per prendere cognizione di dati riservati di un'impresa concorrente, ovvero tramite la manipolazione di dati presenti sui propri sistemi come risultato dei processi di business allo scopo di produrre un bilancio falso o, infine, mediante l'accesso abusivo a sistemi aziendali protetti da misure di sicurezza, da parte di utenti dei sistemi stessi, per attivare servizi non richiesti dalla clientela

ART. 615 QUATER C.P. - DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI

La norma in esame, tutelando la riservatezza dei codici di accesso, punisce la condotta di chi si procura illecitamente codici, parole chiave o altri mezzi idonei per accedere ad un sistema informatico o telematico protetto da misure di sicurezza.

Tra le condotte illecite tipizzate dalla norma rientrano anche le attività di diffusione, comunicazione o consegna a terzi dei predetti codici idonei all'accesso, nonché di comunicazione di indicazioni o istruzioni idonee al predetto scopo.

La norma sanziona solo le condotte prodromiche e preparatorie all'accesso abusivo al sistema informatico o telematico.

Il reato, ad esempio, è integrato qualora un soggetto ceda illecitamente ad un terzo la propria password di accesso alle banche dati cui abitualmente si collega.

ART. 615-QUATER C.P. - DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE, CODICI E ALTRI MEZZI ATTI ALL'ACCESSO A SISTEMI INFORMATICI O TELEMATICI (MODIFICATO DA L.N.238 DEL 23 DICEMBRE 2021 E DALLA LEGGE N.90 DEL 28 GIUGNO 2024)

La Legge n.90 del 28 giugno 2024 ha inasprito le pene della reclusione previste dall'art 615 quater c.p., qualora ricorrano le circostanze di cui all'articolo 615-ter, comma 2 e 3 c.p.

"*Chiunque, al fine di procurare a sé' o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164. La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma*".

Il legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accessi abusivi a sistemi informatici. Per mezzo dell'Art. 615-quater, 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.

I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (ad esempio, badge, carte di credito, bancomat e smart card)

Questo delitto si integra sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi. La condotta è abusiva nel caso in cui i codici di accesso siano ottenuti a seguito della violazione di una norma, ovvero di una clausola contrattuale, che vieti detta condotta (ad esempio, policy Internet)

L'Art. 615-quater, inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza

Risponde, ad esempio, del delitto di diffusione abusiva di codici di accesso, il dipendente di un'azienda autorizzato ad un certo livello di accesso al sistema informatico che ottenga illecitamente il livello di accesso superiore, procurandosi codici o altri strumenti di accesso mediante lo sfruttamento della propria posizione all'interno dell'azienda oppure carpisca in altro modo fraudolento o ingannevole il codice di accesso.

ART. 617 QUATER C.P. - INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (MODIFICATO DA L.N.238 DEL 23 DICEMBRE 2021 E DALLA LEGGE N.90 DEL 28 GIUGNO 2024)

La norma in esame, tutelando la genuinità e la riservatezza delle comunicazioni, punisce le condotte di intercettazione, impedimento o interruzione delle comunicazioni telematiche, poste in essere all'insaputa del soggetto che trasmette la comunicazione. La formula normativa di "comunicazioni telematiche" si presta ad abbracciare qualunque forma e qualunque strumento di divulgazione, ivi compresa la stessa via telematica, e quindi anche la diffusione del testo della comunicazione via Internet o attraverso qualsiasi altra rete. Il reato è aggravato, tra gli altri casi, se commesso da un soggetto che abusa della sua qualità di operatore del sistema informatico o telematico.

La Legge n.90 del 28 giugno 2024 ha inasprito le pene della reclusione previste dall'art. 617 quater c.p., qualora ricorrano le circostanze di cui all'articolo 615-ter, terzo comma, disponendo che "*Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di al primo comma. I delitti di cui ai commi*

primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da quattro a dieci anni se il fatto è commesso: 1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-ter, terzo comma.

2) in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema."

La norma tutela la libertà e la riservatezza delle comunicazioni informatiche o telematiche durante la fase di trasmissione al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi.

La fraudolenza consiste nella modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione.

Perché possa realizzarsi questo delitto è necessario che la comunicazione sia attuale, vale a dire in corso, nonché personale ossia diretta ad un numero di soggetti determinati o determinabili (siano essi persone fisiche o giuridiche). Nel caso in cui la comunicazione sia rivolta ad un numero indeterminato di soggetti la stessa sarà considerata come rivolta al pubblico.

Attraverso tecniche di 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 si integra, ad esempio, con il vantaggio concreto dell'ente, nel caso in cui un dipendente esegua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di un concorrente.

ART. 617 QUINQUIES C.P. - INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE OD INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE (MODIFICATO DA L.N.238 DEL 23 DICEMBRE 2021 E DALLA LEGGE N.90 DEL 28 GIUGNO 2024)

La norma in esame punisce la condotta di installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche, posta in essere al di fuori dei casi espressamente consentiti dalla legge.

Si riporta l'articolo così come recentemente modificato dalla Legge n.90 del 28 giugno 2024 che ha inasprito le pene della reclusione, qualora ricorrano le circostanze di cui all'articolo 617-quater, quarto comma, numero 1) e 2).

"*Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.*

Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 2), la pena è della reclusione da due a sei anni- Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 1), la pena è della reclusione da tre a otto anni".

Il reato, si realizza quando qualcuno, "*fuori dai casi consentiti dalla legge, detiene, diffonde o installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi*".

La condotta vietata dall'Art. 617-quinquies è, pertanto, costituita non solo dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, ma anche se le si detiene solamente o vengono diffuse. Si tratta di un reato che mira a prevenire quello precedente di

intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche.

Anche la semplice installazione di apparecchiature idonee all'intercettazione viene punita dato che tale condotta rende probabile la commissione del reato di intercettazione.

Qualora all'installazione faccia seguito anche l'utilizzo delle apparecchiature per l'intercettazione, interruzione, impedimento o rivelazione delle comunicazioni, si applicheranno nei confronti del soggetto agente, qualora ricorrano i presupposti, più fattispecie criminose.

Il reato si integra, ad esempio, a vantaggio dell'ente, nel caso in cui un dipendente, direttamente o mediante conferimento di incarico ad un investigatore privato (se privo delle necessarie autorizzazioni) si introduca fraudolentemente presso la sede di un concorrente o di un cliente insolvente al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche.

ART. 635-BIS C.P. - DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (MODIFICATO DALLA LEGGE N.90 DEL 28 GIUGNO 2024)

L'art. 635 bis c.p. si configura quando un soggetto "*distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui*".

La Legge n.90 del 28 giugno 2024 ha modificato la citata disposizione prevedendo un inasprimento della pena quando:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato-

Pertanto, il reato si configura quando un soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

ART. 635 TER C.P. DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI PUBBLICI O DI INTERESSE PUBBLICO (ART. 635-TER C.P. MODIFICATO SIA NELLA RUBRICA CHE NEL TESTO DALLA LEGGE N.90 DEL 28 GIUGNO 2024)

Legge n.90 del 28 giugno 2024 ha modificato la disposizione di cui all'art. 635 ter c.p. disponendo che:

"*Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni.*

La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3)"

La norma in questione al primo comma punisce le condotte prodromiche e preparatorie al danneggiamento di informazioni, dati e programmi informatici di cui all'art. 635 bis c.p. riguardanti informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità.

La concreta realizzazione del danno, invece, integra un'autonoma ipotesi di reato, sanzionata più pesantemente nel comma 2 della norma in commento.

ART. 635-QUATER C.P. DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (MODIFICATO DALLA LEGGE N.90 DEL 28 GIUGNO 2024)

Si riporta integralmente il testo sostituito dalla Legge n.90 del 28 giugno 2024:
"*Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da due a sei anni.*
La pena è aumentata è della reclusione da tre a otto anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato".
Questo reato si realizza quando un soggetto "*mediante le condotte di cui all'Art. 635-bis (danneggiamento di dati, informazioni e programmi informatici), ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento*".
Il reato si configura quando qualcuno, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque,

mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici.

ART. 629, 3° COMMA, C.P. ESTORSIONE (INTRODOTTO DALLA LEGGE N.90 DEL 28 GIUGNO 2024)

"Chiunque, mediante le condotte di cui agli articoli 615 ter, 617 quater, 617 sexies, 635 bis, 635 quater e 635 quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità".

Il reato si configura quando qualcuno, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies, minaccia o costringe taluno a compierle o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

Il recente provvedimento, dunque, costruisce una nuova fattispecie criminosa, sanzionandola più aspramente dell'estorsione semplice (che è punita oggi con una pena massima di dieci anni di reclusione).

Una cornice edittale che si inasprisce in maniera significativa nel caso in cui sussistano talune circostanze aggravanti. Basti pensare che, sulla scorta delle nuove prescrizioni dettate dalla Legge, nell'ipotesi in cui la condotta penalmente rilevante venga posta in essere a danno di una persona incapace per età o per infermità, il reato è punito con la reclusione fino a ventidue anni di reclusione.

ART. 635 QUINQUIES C.P. DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICO INTERESSE (MODIFICATO SIA NELLA RUBRICA CHE NEL TESTO DALLA LEGGE N.90 DEL 28 GIUGNO 2024)

Si riporta integralmente il testo sostituito dalla Legge n.90 del 28 giugno 2024:
Salvo che il fatto costituisca piu' grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni.
La pena è della reclusione da tre a otto anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.
La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3).
Il reato si può configurare nel caso in cui un dipendente cancelli file o dati, relativi ad un'area per cui sia stato abilitato ad operare, per conseguire vantaggi interni (ad esempio, far venire meno la prova del credito da parte di un ente o di un fornitore) ovvero che l'amministratore di sistema, abusando della sua qualità, ponga in essere i comportamenti illeciti in oggetto per le medesime finalità già descritte.

ART.640-TER C.P. FRODE INFORMATICA (MODIFICATO DAL D.LGS N. 36 DEL 10 APRILE 2018, DAL D.LGS.N.184 DELL'8 NOVEMBRE 2021 E DAL D.LGS N. 150 DEL 10 OTTOBRE 2022)

Questo reato si configura quando chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno

La pena prevista è la reclusione da sei mesi a tre anni e la multa da € 51 a €1.032

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'art. 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.

La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza prevista dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età.

ART. 640 QUINQUIES C.P. FRODE INFORMATICA DEL SOGGETTO CHE PRESTA SERVIZI DI CERTIFICAZIONE DI FIRMA ELETTRONICA

La norma in esame punisce la frode informatica commessa esclusivamente dal soggetto che presta servizi di certificazione di firma elettronica ovvero fornisce altri servizi connessi con quest'ultimo, secondo quanto previsto dal Codice dell'Amministrazione Digitale ex D.Lgs. 82/2005.

La condotta punita penalmente consiste nella violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato: si tratta, in particolare, degli obblighi di controllo e garanzia previsti dal predetto D.Lgs. 82/2005.

ART. 491 BIS C.P. - FALSITÀ NEI DOCUMENTI INFORMATICI

L'art. 491 bis c.p. dispone che ai documenti informatici pubblici aventi efficacia probatoria si applichi la medesima disciplina penale prevista per le falsità commesse con riguardo ai tradizionali documenti cartacei, previste e punite dagli articoli da 476 a 493 del codice penale. Si citano in particolare i reati di falsità materiale o ideologica commessa da pubblico ufficiale o da privato, falsità in registri e notificazioni, falsità ideologica in certificati commessa da persone esercenti servizi di pubblica necessità, uso di atto falso.

Il concetto di documento informatico è nell'attuale legislazione svincolato dal relativo supporto materiale che lo contiene, in quanto l'elemento penalmente determinante ai fini dell'individuazione

7 REATI PRESUPPOSTO STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

Il Decreto legislativo 184/2021 ha introdotto nel catalogo dei reati presupposto della responsabilità dell'ente i delitti in materia di strumenti di pagamento diversi dai contanti inserendo: **1)** l'aggravante di cui all'art. 640 ter, comma 2, c.p.; **2)** le modifiche all'art. 493 ter c.p.; **3)** ed, ex novo, l'art. 493 quater c.p. Caratteristiche e contesto di detti reati fanno sì che gli stessi possano essere ricondotti nell'Area sensibile dei reati informatici fermo che, anche in questo caso, le attività sensibili previste in quest'area, ricomprendente reati che possono generare proventi illeciti, si devono intendere predisposte anche al fine della prevenzione dei reati di riciclaggio in senso lato.

SI ILLUSTRANO DI SEGUITO I REATI INTRODOTTI DALL'ART. 25.OCTIES.1:

FRODE INFORMATICA CHE PRODUCE TRASFERIMENTO DI DENARO, DI VALORE MONETARIO O DI VALUTA VIRTUALE (ART. 640 TER, COMMA 2).

La fattispecie consiste nell'alterare il funzionamento di un sistema informatico o telematico o nell'intervenire senza diritto sui dati, informazioni o programmi in essi contenuti, ottenendo un ingiusto profitto. La circostanza aggravante che il fatto produca un trasferimento di denaro, di valore monetario o di valuta virtuale determina anche la responsabilità dell'Ente senza bisogno che il soggetto passivo sia lo Stato, la Pubblica Amministrazione o l'UE

INDEBITO UTILIZZO E FALSIFICAZIONE DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (493 TER C.P.)

La fattispecie punisce la condotta di chi, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti.

Viene punita anche la condotta di chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

Il rischio di commissione di tale reato può in teoria configurarsi in tutte le realtà aziendali ed in particolare in tutti i processi aziendali interessati dalla movimentazione di flussi finanziari, in relazione alle differenti tipologie di strumenti di pagamento diverse dai contanti.

In particolare, sono sensibili tutte le attività che rendono possibile l'accesso a dati identificativi, credenziali, etc., funzionali all'eventuale utilizzo indebito di strumenti di pagamento (diversi dai contanti) di titolarità di terzi, quali ad esempio le carte di credito.

DETENZIONE E DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A COMMETTERE REATI RIGUARDANTI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART. 493 QUATER C.P.)

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

La condotta descritta potrebbe riscontrarsi nell'ambito di quelle attività che comportano la gestione e/o la diffusione di strumenti di pagamento diversi dai contanti e negli ambienti tecnologici a supporto di dette attività.

L'articolo 25 octies.1 del D.Lgs. 231/2001, ha inoltre esteso il catalogo dei reati presupposto a "*ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal Codice penale*" a condizione che ne siano oggetto materiale "*strumenti di pagamento diversi dai contanti*".

8 ATTIVITA AZIENDALI SENSIBILI E PRINCIPI GENERALI DI COMPORTAMENTO

PREVENZIONE REATI INFORMATICI RIGUARDANTI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI:

Le attività aziendali sensibili di GETOPEN, nelle quali possono essere commessi i reati informatici (ivi compresi i reati di "Frode informatica che produce trasferimento di denaro, di valore monetario o di valuta virtuale" e "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti") e trattati in modo illecito i dati aziendali informatici, sono proprie di ogni ambito aziendale che utilizza le tecnologie dell'informazione.

All'uopo, GETOPEN ha predisposto appositi presidi organizzativi e si è dotata di adeguate soluzioni di sicurezza, in conformità alla normativa europea e nazionale in materia di protezione dei dati personali, per prevenire e controllare i rischi in tema di tecnologia dell'informazione (IT) e di Cybersecurity, a tutela del proprio patrimonio informativo, della clientela e dei terzi.

Invero, per Patrimonio Informativo Aziendale s'intende un coacervo di categorie di informazioni assolutamente eterogenee, concernenti non solo i dati espliciti, ovvero le informazioni strutturate (ad esempio, in database) o quelle formalizzate (in documenti e nei sistemi informativi: procedure, policy, contratti, piani, progetti), ma anche le informazioni nella posta elettronica, nonché i software e tutte le

informazioni facilmente individuabili perché contenute in un supporto, fisico o digitale.

Ancora, per quanto attiene il reato di "Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti ed ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal Codice penale, a condizione che ne siano oggetto materiale strumenti di pagamento diversi dai contanti", le attività aziendali sensibili della Società nelle quali può essere commessa questa tipologia di reato, riguardano tutti i processi aziendali che comportano la movimentazione di flussi finanziari sia di GETOPEN, che per conto della propria clientela, attraverso le differenti tipologie di strumenti di pagamento diverse dai contanti e dei relativi applicativi.

Orbene, tutte le Funzioni Aziendali che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione e utilizzo dei sistemi informatici aziendali, devono rispettare le prescrizioni sopra individuate e, in particolare:

- ✓ intercettare, impedire e/o interrompere l'utilizzo di ogni dispositivo, oggetto o record protetto, materiale o immateriale, o una loro combinazione, diverso dalla moneta a corso legale, che da solo o unitamente a una procedura o ad una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario anche attraverso mezzi di scambio digitale;
- ✓ intercettare, impedire e/o interrompere l'utilizzo di apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere reati riguardanti gli strumenti di pagamento diversi dai contanti o sono specificamente adattati al medesimo scopo;
- ✓ intercettare, impedire e/o interrompere l'utilizzo dispositivi finalizzati al trasferimento di denaro, di valore monetario o di valuta virtuale;
- ✓ intercettare trasferimenti illeciti di mezzi di pagamento diversi dal contante;
- ✓ vietare ed ostacolare la diffusione e l'installazione abusiva di apparecchiature ed altri mezzi atti ad intercettare, impedire o interrompere comunicazioni

informatiche o telematiche, nonché le condotte atte a danneggiare o interrompere un sistema informatico o telematico.

9 I REATI INFORMATICI DI GESTIONE ED UTILIZZO DEI SISTEMI INFORMATICI DEL PATRIMONIO INFORMATIVO DI GETOPEN

L'utilizzo e la gestione di sistemi informatici e del Patrimonio Informativo sono attività imprescindibili per l'espletamento del business aziendale e contraddistinguono la maggior parte dei processi di GETOPEN.

Si rendono quindi necessarie una efficace e stringente definizione di norme e misure di sicurezza organizzative, comportamentali e tecnologiche e la realizzazione di attività di controllo, peculiari del presidio a tutela di una gestione e di un utilizzo dei sistemi informatici e del Patrimonio Informativo di GETOPEN in coerenza con la normativa vigente.

Alla luce delle considerazioni che precedono, di seguito si declinano i processi sui quali si basa il presidio posto in essere sulla gestione e sull'utilizzo dei sistemi informatici e del Patrimonio Informativo di GETOPEN.

IL PROCESSO DI GESTIONE DELLA SICUREZZA INFORMATICA SI ARTICOLA NELLE SEGUENTI FASI:

- analisi del rischio IT e definizione dei requisiti di sicurezza informatica;
- gestione Accessi Risorse Informatiche e Servizi di Sicurezza ICT;
- monitoraggio eventi sicurezza informatica e gestione eventi critici di sicurezza informatica;
- sicurezza delle terze parti;
- diffusione della cultura di sicurezza informatica;
- progettazione e realizzazione soluzioni di sicurezza informatica.

IL PROCESSO DI PREVENZIONE FRODI SI ARTICOLA NELLE SEGUENTI FASI:

- identificazione delle misure atte al rafforzamento della prevenzione;
- monitoraggio dell'evoluzione delle frodi informatiche;
- gestione delle comunicazioni con le Autorità Competenti.

IL PROCESSO DI GESTIONE DELLA SICUREZZA FISICA SI ARTICOLA NELLE SEGUENTI FASI:

- gestione protezione di aree e locali ove si svolge l'attività;

• gestione sicurezza fisica dei sistemi periferici.

IL PROCESSO DI GESTIONE E SUPPORTO ICT (*INFORMATION AND COMUNICATION TECHNOLOGIES*) SI ARTICOLA NELLE SEGUENTI FASI:

• erogazione dei servizi ICT;

• monitoraggio del funzionamento dei servizi ICT e gestione delle anomalie;

• assistenza agli utenti attraverso attività di Help desk e problem solving.

Il processo di gestione delle comunicazioni alle Autorità Preposte per la definizione, gestione e controllo del "Perimetro di sicurezza nazionale cibernetica" si articola, nel rispetto degli attesi provvedimenti attuativi del Governo nelle seguenti fasi:

• individuazione delle informazioni ed eventi che devono essere oggetto di comunicazione/segnalazione;

•trasmissione, a seconda delle Autorità Preposte, della comunicazione/segnalazione a cura delle funzioni compenti.

10 ATTIVITA AZIENDALI SENSIBILI E PRINCIPI GENERALI DI COMPORTAMENTO

PRESIDI DI CONTROLLO SPECIFICI

1) Ai Destinatari del Modello è fatto divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che – considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato tra quelle sopra considerate;
- violare i principi di comportamento previsti nella presente Parte Speciale, nonché le regole e prassi interne di interesse;

2) individuazione e adozione di misure adeguate di sicurezza di natura organizzativa, fisica e logistica, in modo da minimizzare il rischio di accessi non autorizzati, di alterazione, di divulgazione, di perdita o distruzione delle risorse informatiche e che si pongano quale obiettivo quello di:

- tutelare la sicurezza delle informazioni;
- prevedere eventuali controlli di sicurezza specifici per tipologia di asset;

- prevedere eventuali controlli di sicurezza destinati a indirizzare i comportamenti e le azioni operative del personale di GETOPEN;
- prevedere più livelli di sicurezza mediante l'utilizzo di password, firewall e simili;
- introdurre un sistema di filtro e di limitazione alla navigazione sui computer in dotazione ai dipendenti.

3) obbligo per tutti i Destinatari del presente Modello di rispettare i principi comportamentali posti a presidio del rischio di commissione dei delitti informatici, volti ad assicurare l'osservanza dei seguenti parametri di sicurezza del patrimonio informativo di GETOPEN previsti dai principali standard internazionali in tema di sicurezza delle informazioni:

- **RISERVATEZZA** intesa come garanzia che una informazione sia accessibile solo a chi è autorizzato;

- **INTEGRITÀ** intesa come salvaguardia dell'accuratezza e della completezza dell'informazione e dei metodi di elaborazione;

- **DISPONIBILITÀ** intesa come garanzia che gli utenti autorizzati abbiano accesso alle informazioni e alle risorse associate, quando richiesto.

IN PARTICOLARE, È VIETATO:

(a) connettere ai sistemi informatici di GETOPEN personal computer, periferiche, altre apparecchiature o installare software senza preventiva autorizzazione della Funzione Aziendale preposta;

(b) procedere a installazioni di prodotti software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi e i regolamenti che disciplinano e tutelano il diritto d'autore;

(c) modificare la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola interna ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;

(d) acquisire, possedere, o utilizzare strumenti software e/o hardware – se non per casi debitamente autorizzati, ovvero in ipotesi in cui tali software e/o hardware siano utilizzati per il monitoraggio della sicurezza dei sistemi informativi interni –

che potrebbero essere adoperati abusivamente per valutare o compromettere la sicurezza di sistemi informatici o telematici;

(e) ottenere credenziali di accesso a sistemi informatici o telematici aziendali dei clienti o di terze parti con metodi o procedure differenti da quelle per tali scopi autorizzate da GETOPEN;

(f) divulgare, cedere o condividere con personale interno o esterno a GETOPEN le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti, soci o terze parti;

(g) accedere abusivamente a un sistema informatico altrui – ovvero nella disponibilità di altri dipendenti o terzi – nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;

(h) manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti, soci o di terze parti, comprensivo di archivi, dati e programmi;

(i) sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;

(l) acquisire e/o utilizzare prodotti tutelati dal diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;

(m) comunicare a persone non autorizzate, interne o esterne a GETOPEN i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;

(n) mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti virus o altri programmi in grado di danneggiare o intercettare dati;

(o) lo spamming come pure ogni azione di risposta al medesimo;

(p) inviare attraverso un sistema informatico interno qualsiasi informazione o dato, previa alterazione o falsificazione dei medesimi;

(q) utilizzare per finalità diverse da quelle lavorative le risorse informatiche (es. personal computer fissi o portatili) assegnate da GETOPEN;

(r) alterare documenti elettronici, pubblici o privati, con finalità probatoria.

I DESTINATARI DEL MODELLO SONO TENUTI A RISPETTARE SCRUPOLOSAMENTE TUTTE LE NORME VIGENTI, E IN PARTICOLARE:

• utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;

• custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi di GETOPEN, evitando che terzi soggetti possano venirne a conoscenza;

• garantire la tracciabilità dei documenti prodotti;

• assicurare meccanismi di protezione dei file, quali, ad esempio, password da aggiornare periodicamente, secondo le prescrizioni comportamentali di GETOPEN;

• utilizzare beni protetti dalla normativa sul diritto d'autore nel rispetto delle regole ivi previste;

• utilizzare unicamente materiale pubblicitario (i.e. materiale fotografico) autorizzato.

4) informazione rivolta a tutti i destinatari eventualmente autorizzati all'utilizzo dei sistemi informativi in ordine alla importanza di:

- mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi;

- utilizzare correttamente i software e banche dati in dotazione;

- non inserire dati, immagini o altro materiale coperto dal diritto d'autore senza avere ottenuto le necessarie autorizzazioni;

5) formazione e addestramento periodico in favore dei dipendenti, diversificato in ragione delle rispettive mansioni, nonché, in misura ridotta, in favore dei destinatari eventualmente autorizzati all'utilizzo dei sistemi informativi, al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche.

6) informazione rivolta ai dipendenti e, in generale, a tutti i destinatari del Modello eventualmente autorizzati all'utilizzo dei sistemi informativi, della necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;

7) limitazione degli accessi alle stanze server unicamente al personale autorizzato;

8) protezione, per quanto possibile, di ogni sistema informatico di GETOPEN, al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative a un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;

9) dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venire disattivati;

10) impedire l'installazione e l'utilizzo di software non approvati da GETOPEN e non correlati con l'attività professionale espletata per la stessa;

11) informazione rivolta agli utilizzatori dei sistemi informatici che i software per l'esercizio delle attività di loro competenza sono protetti dalle leggi sul diritto d'autore e in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;

12) limitazione dell'accesso alle aree e ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di virus capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti e, in ogni caso, implementare – in presenza di specifici accordi – presidi volti a individuare eventuali accessi o sessioni anomale, previa individuazione degli "indici di anomalia" e predisposizione di flussi informativi tra le Funzioni competenti nel caso in cui vengano riscontrate le suddette anomalie;

14) qualora per la connessione alla rete Internet si utilizzino collegamenti wireless, protezione degli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni a GETOPEN, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti;

15) previsione di un procedimento di autenticazione mediante l'utilizzo di credenziali al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei dipendenti, degli stagisti e degli altri soggetti – come ad esempio i collaboratori esterni – eventualmente autorizzati all'utilizzo dei sistemi informativi.

IN PARTICOLARE:

• le Funzioni Aziendali coinvolte nei processi devono predisporre e mantenere il censimento degli applicativi che si interconnettono con la Pubblica Amministrazione o con le Autorità di Vigilanza e/o dei loro specifici software in uso;
• i soggetti coinvolti nel processo devono essere appositamente incaricati;
• ogni dipendente/amministratore del sistema è tenuto alla segnalazione al proprio preposto di eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di hacker esterni) mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente ed attivando l'eventuale escalation che può condurre anche all'apertura di uno stato di crisi ed alle comunicazioni alle Autorità Preposte;
• ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (es. personal computer fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività. Tali risorse devono essere conservate in modo appropriato e la Società dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;
• qualora sia previsto il coinvolgimento di soggetti terzi/outsourcer nella gestione dei sistemi informatici e del Patrimonio Informativo di GETOPEN, nonché nell'interconnessione/utilizzo dei software della Pubblica Amministrazione o delle Autorità di Vigilanza, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001 e di impegno al suo rispetto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001 e, più in particolare, a titolo meramente esemplificativo e non esaustivo:

• introdursi abusivamente, direttamente o per interposta persona, in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate o di utilizzare indebitamente, falsificare o alterare strumenti di pagamento diversi dai contanti;

• accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati di GETOPEN, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
• intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
• utilizzare dispositivi tecnici o strumenti software non autorizzati (virus, worm, troian, spyware, dialer, keylogger, rootkit, ecc.) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
• distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
• introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
• detenere, procurarsi, riprodurre o diffondere abusivamente codici d'accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
• produrre, importare, esportare, vendere, trasportare, distribuire, mettere a disposizione o in qualsiasi modo procurare a sé o ad altri apparecchiature, dispositivi o programmi informatici progettati principalmente per commettere reati riguardanti strumenti di pagamento diversi dai contanti o adattati a tale scopo;
• procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
• alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;
• produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;

• porre in essere mediante l'accesso alle reti informatiche condotte illecite costituenti violazioni di diritti sulle opere dell'ingegno protette, quali, a titolo esemplificativo:

o diffondere in qualsiasi forma opere dell'ingegno non destinate alla pubblicazione o usurparne la paternità;

o detenere qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di protezione dei programmi di elaborazione;

o rimuovere o alterare informazioni elettroniche inserite nelle opere protette o comparenti nelle loro comunicazioni al pubblico, circa il regime dei diritti sulle stesse gravanti;

• omettere di comunicare entro i termini prescritti dalla normativa vigente in materia di "sicurezza nazionale cibernetica" dati, informazioni o elementi di fatto rilevanti;

• esibire documenti e dati incompleti e/o comunicare dati falsi o alterati nell'ambito delle comunicazioni in materia di "sicurezza nazionale cibernetica".

I Responsabili sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

10.1 ATIVITÀ SVOLTE IN MODALITÀ SMART WORKING – PRINCIPI DI COMPORTAMENTO

Coloro che svolgono l'attività lavorativa in modalità smart working dovranno:

- verificare l'aggiornamento dell'antivirus e delle pach di sicurezza (sit web Microsoft, Apple o dei produttori di aggiornamenti automatici di sicurezza, ve ne sono molti free), limitare al massimo tale utilizzo e cancellare i dati aziendali sui device personali;

- proteggere WiFi domestica: password del router complessa (almeno otto caratteri di cui almeno due in cifre o caratteri speciali). Non utilizzare reti Wi-Fi pubbliche, hot spot pubblici o Internet café. Se necessario utilizzare hot spot del telefono aziendale. Usare canali di comunicazione approvati;

- se non strettamente indispensabile, non inoltrare e-mail a e-mail personali o salvare le informazioni aziendali su dispositivi personali, nel caso cancellare i dati dai device personali appena possibile;
- se si stampa materiale a casa ricordarsi di mantenere le stampe come da policy aziendali;
- verificare sempre l'indirizzo di provenienza delle mail prima di aprirle;
- se si nota qualcosa di sospetto sul proprio dispositivo, si ricevono chiamate o messaggi non richiesti o si desidera segnalare un incidente di sicurezza, contattare i colleghi dell'Area IT per i quali sono segnalate le fasce orarie di presenza ogni settimana. In caso adi dubbi contattate senza esitare in vostro responsabile.

10.2 L'ACCESSO AI SISTEMI INFORMATICI, ACQUISTO E CONTROLLO DI *SOFTWARE - HARDWARE*

L'eventuale acquisto da parte della Società di nuovi *software* deve essere debitamente approvato dall'Amministratore Unico, previa acquisizione della dichiarazione della casa madre di conformità del *software* al Regolamento Europeo n. 679/2016 (*privacy by design* e *by default*).

È obbligatorio l'utilizzo di *software antivirus* e *firewall* costantemente aggiornati automaticamente per protezione contro potenziali attacchi verso l'esterno originati da tutti i server o le *workstations* della Società (postazioni fisse e portatili).

10.3 L'ACCESSO A SITI DI ENTI PUBBLICI O PRIVATI

L'accesso a siti di enti pubblici o privati che richiede apposita autenticazione da parte della Società è consentito solo a personale specifico e all'uopo autorizzato (tramite *user-id* e *password*, *Token* di autenticazione).

I soggetti che in azienda – l'AU ed il soggetto all'uopo eventualmente incaricato – siano a conoscenza delle credenziali per l'accesso ai sistemi informatici della P.A. o di enti privati sono obbligati a tenere segrete le credenziali di accesso ai sistemi e a conservarle in modo adeguato.

10.4 I DISPOSITIVI ASSEGNATI A DIPENDENTI O FUNZIONI AZIENDALI

La Società può mettere a disposizione dei dipendenti e/o delle funzioni aziendali appositi dispositivi elettronici, da utilizzare unicamente ai fini dell'espletamento dell'attività aziendale, nel pieno rispetto delle normative in materia di utilizzo e gestione dei sistemi informatici e delle procedure aziendali definite.

In particolare, qualora siano assegnati ai dipendenti dispositivi informatici personali, deve essere redatto verbale di consegna e, all'atto dell'interruzione del rapporto lavorativo (eventuale licenziamento e/o dimissioni) ovvero in caso di guasti o sostituzioni dei predetti dispositivi, il relativo verbale di restituzione.

In caso di smarrimento o furto, dovrà essere data immediata informazione al superiore gerarchico e/o all'AU, che dovrà occuparsi di effettuare la relativa denunzia alle competenti autorità.

È vietato prestare o cedere a terzi qualsiasi apparecchiatura informatica messa a disposizione dalla Società.

I Dipendenti e le Funzioni Aziendali devono, una volta terminata la lavorazione assegnata, salvare i dati nell'archivio Cloud preposto per l'archiviazione e condivisione dei dati.

10.5 USO DELLA RETE INTERNET

La rete *internet* deve essere utilizzata solo per scopi prettamente attinenti all'attività lavorativa e devono essere implementati i meccanismi di protezione della rete. È espressamente vietato utilizzare la rete aziendale per navigare in siti illeciti, ed in particolare pornografici e pedopornografici, nonché dedicati al gioco d'azzardo o altri tipi di giochi *online*.

10.6 LE *PASSWORD* DI ACCESSO AI DISPOSITIVI

A ciascun dipendente o funzione aziendale, che utilizzi dispositivi aziendali, dovrà essere creata un'utenza personale o *account* corredato da apposita *password*. La *password* del dispositivo potrà essere modificata dal singolo utente, che dovrà avere cura di custodirla.

Le utenze che non verranno utilizzate per più di tre mesi devono essere disabilitate: l'AU o la Funzione eventualmente incaricata dal primo per iscritto, si occuperà della disabilitazione delle utenze.

Il dipendente che venga munito di un dispositivo elettronico mobile o fisso, dovrà accedervi tramite apposita *password* – composta da almeno 8 caratteri, contenente numeri e almeno una lettera composta da almeno da 8 caratteri, che non dovrà essere riportata su carta o cellulari e dispositivi elettronici in genere.

10.7 LA GESTIONE DELLA POSTA ELETTRONICA

La gestione della posta elettronica certificata e le *password* di accesso non possono essere diffuse ad altro soggetto diverso dall'Amministratore Unico.

Le P.E.C. in entrata devono essere regolarmente archiviate dall'AU ed inserite in un registro digitale e/o cartaceo.

L'invio di P.E.C. in uscita deve unicamente avvenire a cura dell'Amministratore Unico, nonché, previa autorizzazione, da parte del RPROG o di altra funzione aziendale all'uopo autorizzata.

Per quanto riguarda la posta elettronica ordinaria le caselle di posta assegnate ai dipendenti devono riportare il riferimento al nome della Società.

La gestione della posta elettronica aziendale e, pertanto, il trattamento dei dati connesso al suo utilizzo da parte dei soggetti autorizzati, dovrà essere svolta nel pieno rispetto della normativa *privacy* vigente (anche al livello comunitario), nonché di quelle all'uopo previste in relazione ai rapporti di lavoro.

10.8 L'UTILIZZO DI SUPPORTI MAGNETICI RIMOVIBILI

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, *etc.*), contenenti dati particolari/sensibili, nonché informazioni costituenti *know-how* aziendale, devono essere trattati con particolare cautela al fine di evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

10.9 IL LICENZIAMENTO O LE DIMISSIONI DI UN DIPENDENTE

Qualora un dipendente interrompa il rapporto di lavoro con l'azienda, per qualsivoglia ragione, è necessario modificare le *password* di cui lo stesso era a conoscenza e/o disabilitare le utenze.

GETOPEN S.r.l. si riserva, tuttavia, di valutare a proprio esclusivo ed insindacabile giudizio, la necessità di mantenere attiva in ricezione le utenze – es. la casella postale – per un congruo periodo di tempo, al fine di garantire la funzionalità aziendale.

10.10 LA VARIAZIONE DI DATI NEL SISTEMA INFORMATICO

Eventuali variazioni dei dati inseriti nel sistema informatico e concernenti l'anagrafica Clienti e/o Dipendenti (ad esempio l'IBAN fornitore e/o dipendente, *password, etc.)*, devono essere autorizzate dal Responsabile di funzione e, comunque, comunicate per iscritto all'AU.

10.11 INSTALLAZIONE DI *SOFTWARE* DI TERZE PARTI PER LA FATTURAZIONE

È FATTO DIVIETO AD OGNI FUNZIONE AZIENDALE AUTORIZZATA ALL'UTILIZZO DEI SISTEMI INFORMATICI DI:

- Modificare contenuti e settaggi dei programmi ivi installati;
- procurarsi, riprodurre, diffondere, comunicare e/o consegnare codici, parole chiave e/o altri mezzi idonei al superamento delle misure di sicurezza poste a protezione dei *software.*

Devono essere tempestivamente comunicati all'OdV eventuali aggiornamenti relativi al sistema informatico aziendale (*software*), ad esempio: modifiche e/o integrazioni dei profili autorizzativi, delle funzioni, delle modalità di inserimento dati, del rilevamento accessi, etc.

10.12 L'UTILIZZO DI SISTEMI *CLOUD COMPUTING*

L'utilizzo di sistemi di cd. *cloud computing* è ammesso solo se l'applicativo è conforme al GDPR *compliance*.

10.13 FALSITÀ DI UN DOCUMENTO INFORMATICO O TELEMATICO E UTILIZZO DI *SMARTCARD*

L'utilizzo di *smartcard* per la firma "digitale" di documenti, è consentito solo ed esclusivamente all'AU.

Le credenziali per la firma possono essere detenute anche da altre funzioni o dipendenti, in azienda, ad esempio dal RPROG; tuttavia, ai fini dell'utilizzo è necessario acquisire apposita autorizzazione scritta da parte dell'AU.

10.14 DATA BREACH

Ogni dipendente o collaboratore che nell'utilizzo dei dispositivi informatici aziendali in dotazione sospetti o constati l'avvenuta perdita, modifica, comunicazione non autorizzata, diffusione non autorizzata o accesso non autorizzato dei dati personali trattati dall'azienda (quali, a titolo di esempio: furto, smarrimento di supporti, *virus*, *e mail* sospette aperte per errore, *etc.*) è tenuto a informare immediatamente e, comunque, non oltre 24 ore dalla conoscenza di tale evento, il superiore gerarchico e/o l'AU..

L'Amministratore Unico, valutata l'entità e la gravità del *data breach*, effettuerà, entro le 72 ore seguenti, tutti gli adempimenti richiesti dalla legge, notificando la violazione al *Garante Privacy* e agli interessati, ove richiesto. L'Amministratore, inoltre, provvederà ad adottare, immediatamente, tutte le misure di sicurezza idonee ad evitare ulteriori conseguenze dannose, originate dal *data breach* all'Azienda e/o a terzi eventualmente interessati, nonché a prevenire ulteriori *data breach*.

DIVIETO DI PAGAMENTI IN CASO DI DATA BREACH PER RIAVERE I DATI

Nel caso di infezione del sistema informatico della Società causato da *crypto virus* o analoghi *virus* che bloccano, carpiscono, oscurano, sottraggono i dati, oltre ad attivare la procedura di *data breach* prescritta dalla legge, qualora esse siano corredate da richieste di riscatto di denaro o altra utilità per rientrare in possesso dei dati o per evitare altre conseguenze dannose derivanti dall'utilizzo o la perdita dei dati personali e non, della Società, l'AU dovrà denunciare il fatto alle competenti

autorità. È fatto divieto di corrispondere denaro, *bitcoin* o altre utilità a titolo di riscatto e, comunque, per rientrare in possesso dei dati o per evitare altre azioni dannose per la società.

10.15 PREVISIONE DI UNA PROCEDURA DI *DISASTER RECOVERY*

Al fine di evitare possibili violazioni dei dati personali e/o aziendali, è obbligatorio che, su tutti i pc aziendali fissi o mobili, venga effettuato settimanalmente un *backup* dei dati. Inoltre, verrà effettuato un *backup* delle macchine virtuali, contenti i *database* aziendali.

11 I DIVIETI

Le predette attività di controllo costituiscono valido presidio, anche a garanzia della tracciabilità delle modifiche apportate alle procedure informatiche, della rilevazione degli utenti che hanno effettuato tali modifiche e di coloro che hanno effettuato i controlli sulle modifiche apportate.

In ogni caso, le attività di gestione ed utilizzo dei sistemi informatici aziendali devono essere assoggettate ad una costante attività di controllo, attraverso l'utilizzo di adeguate misure per la protezione delle informazioni, salvaguardandone la riservatezza, l'integrità e la disponibilità, con particolare riferimento al trattamento dei dati personali.

IN OGNI CASO, È FATTO DIVIETO DI:

- Installare, nella rete aziendale di GETOPEN S.r.l., programmi/*software* privi di licenza che non rientrino nello scopo per cui il sistema informatico è stato assegnato all'utente;
- distruggere e/o alterare documenti informatici, aventi finalità probatoria in assenza di una specifica autorizzazione dell'amministratore;
- per ciascun dipendente, di rivelare le proprie credenziali di autenticazione (nome utente e *password*) alla rete aziendale o anche ad altri siti/sistemi;

- copiare documenti e materiali protetti da *copyright*, senza l'autorizzazione espressa del detentore, salvi i casi in cui tali attività rientrino nel normale svolgimento delle funzioni affidate;
- effettuare l'*upload* e il *download* di *software* gratuiti (*freeware* e *shareware*), nonché l'utilizzo di documenti provenienti da siti *web* o *http*, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione;
- installare autonomamente programmi provenienti dall'esterno sui *computer* di GETOPEN, tali da agevolare il rischio di introduzione di *virus* informatici e/o di alterazione della funzionalità delle applicazioni *software* esistenti;
- effettuare collegamenti alla rete con modalità difformi dall'architettura informatica prevista;
- utilizzare la casella di posta elettronica "personale" per trasmettere documenti e allegati vari al di fuori della rete informatica aziendale, ciò al fine di garantire la sicurezza e la *privacy* delle informazioni trattate;
- prendere parte a *blog*, dibattiti non attinenti al lavoro con la propria postazione aziendale di accesso alla rete;
- manomettere, in qualunque modo, il funzionamento di un sistema informatico; in particolare aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (*antivirus*, *firewall*, *proxy*, *server*);
- entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- modificare la configurazione aziendale del personal computer in dotazione ed utilizzare software diversi o aggiuntivi rispetto a quelli coperti da licenza d'uso o, comunque, installati dalla Società, salvo espressa autorizzazione del Responsabile della Funzione Aziendale all'uopo preposta e purchè si tratti di software necessari allo svolgimento dell'attività lavorativa;
- installare e/o utilizzare programmi, dispositivi, software o qualsiasi altro strumento informatico che permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali;

- detenere, diffondere ed installare abusivamente apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici;
- detenere, diffondere ed installare abusivamente apparecchiature ed altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- detenere, diffondere ed installare abusivamente apparecchiature, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema telematico protetto da misure di sicurezza, al fine di procurare a sé o ad altri un profitto o arrecare un danno ad altri;
- detenere, diffondere ed installare abusivamente apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- danneggiare un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, detenendo, producendo, riproducendo, importando, diffondendo, comunicando, consegnando o mettendo a disposizione di terzi o installando apparecchiature, dispositivi o programmi informatici;
- intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrente tra più sistemi, impedendole o interrompendole;
- detenere, diffondere ed installare abusivamente apparecchiature e altri mezzi atti ad intercettare, impedire ed interrompere comunicazioni informatiche o telematiche;
- detenere materiale pornografico realizzato utilizzando minori degli anni diciotto;
- utilizzare sistemi informatici o appositi siti internet per l'adescamento di minori;
- diffondere notizie false o porre in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione di strumenti finanziari (art. 185 TUF).

12 I CONTROLLI PER LA PREVENZIONE DEI REATI INFORMATICI

È fatto obbligo alla Società di attivarsi, con cadenza semestrale, per porre in essere le azioni necessarie all'adeguato e corretto funzionamento del sistema informatico aziendale. Tali adempimenti dovranno essere realizzati da un esperto informatico (anche interno alla Società) all'uopo autorizzato dall'AU.

IL TECNICO INCARICATO DOVRÀ, IN PARTICOLARE:

- verificare la sicurezza della rete e dei sistemi informativi aziendali ed identificare le potenziali vulnerabilità nel sistema dei controlli IT;
- effettuare le attività di verifica dell'esistenza dei *backup*. Di tale attività deve essere conservata un'evidenza documentale; in caso di intervento di soggetto interno alla Società, quest'ultimo dovrà redigere apposito verbale inerente l'attività svolta, sottoscritto anche dall'AU;
- verificare e vietare le condotte aventi ad oggetto mezzi di pagamento digitali attraverso cui viene scambiata moneta elettronica avente corso legale, ma anche le c.d. criptovalute, prive di valore legale ma socialmente sempre più accettate come mezzi di pagamento.

Nel caso in cui l'attività di gestione del sistema informatico dovesse essere svolta da un terzo esterno alla Società – fermo restando l'obbligo di regolamentare il trattamento dei dati ai sensi dell'art. 28 del Regolamento Europeo n. 679/2016 – il responsabile di Funzione coinvolto dovrà predisporre un *report* di intervento completo di data, ora, nominativo del soggetto che ha effettuato l'intervento, la tipologia delle operazioni effettuate e lo scopo. Il *report* sarà sottoscritto dal responsabile di Funzione e dal soggetto che ha effettuato l'intervento, e trasmesso all'AU, il quale provvederà ad apporre apposito visto.

I collegamenti da remoto per manutenzione e/o riparazioni al sistema informatico possono essere effettuati solo previa autorizzazione dell'utente utilizzatore del dispositivo informatico interessato.

Inoltre, GETOPEN al fine di prevenire la commissione dei reati informatici e del trattamento illecito dei dati si impegna a:

- promuovere l'adozione di un programma di sensibilizzazione sulla sicurezza delle informazioni con l'obiettivo di rendere i dipendenti – ed in particolare il responsabile della sicurezza informatica - consapevoli delle loro responsabilità per la sicurezza delle informazioni e dei mezzi con cui tali responsabilità vengono assolte. Invero, la società dovrà, con cadenza annuale, eseguire un apposito programma di formazione, in modo da rimanere in linea con le politiche e le procedure organizzative all'uopo previste;
- organizzare dei programmi di formazione per sensibilizzare i dipendenti in materia di responsabilità amministrativa degli enti con l'intento di evitare che l'azione illecita di un dipendente comporti l'apertura di un procedimento ex Decreto 231 a carico della società.
- promuovere ed assicurare il puntuale rispetto da parte di tutti i Destinatari della presente procedura del regolamento informatico adottato da BITCONTROL e delle relative procedure aventi ad oggetto il corretto utilizzo delle risorse informatiche aziendali, la sicurezza informatica/telematica, la protezione dei dati sensibili.

13 CYBERSICUREZZA

La Legge n. 90 del 2024, c.d. "legge sulla Cybersicurezza" interviene anche sul catalogo dei reati presupposto in materia di responsabilità amministrativa degli enti, contemplati nel decreto legislativo n. 231 del 2001. In particolare, il legislatore:

1. Ritocca il contenuto dell' articolo 24-bis, relativo ai reati informatici, aumentando le sanzioni previste all'interno del suo comma 1, le quali passano da una cornice edittale ricompresa tra cento e cinquecento quote, ad una ricompresa tra duecento e settecento quote.

2. Aggiunge all'articolo 24-bis il nuovo comma 1-bis, ai sensi del quale si applica all'ente la sanzione pecuniaria da trecento a ottocento quote a seguito della commissione della nuova fattispecie di reato –introdotta sempre dalla Legge sulla

Cybersicurezza – legata all'estorsione informatica di cui all' articolo 629, comma 3, del codice penale. Nei casi di condanna, inoltre, è prevista anche l'applicazione delle sanzioni interdittive previste dall' articolo 9, comma 2, del decreto legislativo n. 231/2001, per una durata non inferiore a due anni.

Invero, è evidente come il legislatore, attraverso il combinato disposto del comma 3 dell' articolo 629 del codice penale e del comma 1-bis dell' articolo 24-bis del decreto legislativo n. 231/2001, tenti di limitare la piaga estorsiva discendente, anzitutto, dagli attacchi informatici di tipo ransomware, provando a creare anche un argine al dilagare dei pagamenti dei riscatti richiesti dalle organizzazioni criminali.

Tuttavia, l'introduzione nel nostro ordinamento del reato di estorsione informatica, teso a punire con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000 "chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno", difficilmente potrà modificare da sola lo scenario criminale legato agli attacchi ransomware nei confronti dell'Italia, che vede agire – nella quasi totalità dei casi – soprattutto soggetti al di fuori dei nostri confini nazionali.

Il medesimo ragionamento vale anche per quanto previsto al comma 1-bis dell' articolo 24-bis del decreto legislativo n. 231/2001, il quale, nei fatti, introduce correttamente la responsabilità amministrativa dell'ente, unitamente alle discendenti sanzioni interdittive personali, ma solo nel caso in cui, semplificando, il reato di estorsione informatica sia commesso da un soggetto appartenente all'ente stesso. Un'ipotesi, questa, certamente possibile e, quindi, senz'altro da regolamentare, ma che nella quotidianità dei reati informatici appare forse come un "caso limite" e che, purtroppo, potrebbe avere poco impatto sul dilagare – soprattutto nel mondo privato – dei pagamenti di riscatti a seguito di attività estorsive condotte, ad esempio, attraverso attacchi ransomware.

3. Modifica il comma 2 dell'articolo 24-bis, relativo alla commissione dei delitti di cui agli articoli 615-quater ("Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici e telematici") e 615-quinquies ("Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico") del codice penale, innalzando la sanzione pecuniaria ivi prevista sino a quattrocento quote.

4. Sostituisce tra i reati presupposto per i quali è prevista l'applicazione all'ente della sanzione pecuniaria di cui al precede al punto 3., il riferimento all'articolo 615-quinquies c.p., abrogato proprio dalla Legge sulla Cybersicurezza, con il richiamo al nuovo delitto di detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico di cui all'articolo 635-quater.1.

14 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

Tutti i Destinatari coinvolti nelle attività di gestione ed utilizzo dei Sistemi Informatici aziendali sono tenuti a comunicare tempestivamente all'Organismo di Vigilanza:

- ✓ qualsiasi violazione ai principi di comportamento;
- ✓ qualsiasi violazione del Modello di Organizzazione e del Codice Etico, con l'indicazione delle ragioni delle difformità e dando atto del processo autorizzativo seguito.

I Destinatari devono, ognuno per le parti di rispettiva competenza, verificare la tracciabilità del processo eseguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposta su apposita piattaforma informatica -tutta la documentazione necessaria.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di corporate governance per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 20.03.2024	ADOZIONE
Rev. 1	Determina dell'Amministratore Unico del 05.08.2024	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231)

PARTE SPECIALE -6-

SOMMARIO

1 OBIETTIVI E FUNZIONI DEL MODELLO

In relazione alla gestione della c.d. omaggistica e delle spese di rappresentanza, sono state analizzate in relazione ai reati di cui agli artt. 25, 24ter, 25ter, 25octies, L.190/12 del D. Lgs. 231/2001, che disciplinato quali principali fattispecie di illecito presupposto:

- ✓ i reati commessi nei rapporti con la Pubblica Amministrazione – artt. 317, 318, 319, 314, 316, 322-bis c.p. (Concussione, Corruzione per l'esercizio della funzione, Corruzione per atto contrario ai doveri d'ufficio, Peculato);
- ✓ i reati di criminalità organizzata – artt. 416, 416bis c.p. – (Associazione per delinquere, Associazione di tipo mafioso);
- ✓ i reati societari – artt. 2635, 2635bis, 2638 c.c. – (Corruzione tra privati, Istigazione alla corruzione tra privati, Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza);
- ✓ i reati di Riciclaggio, Corruzione, Concussione e Induzione indebita, Peculato - 648, 648bis, 648ter, 648ter-1 c.p. – (Ricettazione, Riciclaggio, Impiego di denaro, beni o utilità di provenienza illecita, Autoriciclaggio).

Orbene, dall'analisi delle superiori fattispecie di reato e dall'esame dell'attività espletata da GETOPEN, si ritiene che la puntuale osservanza dei principi e delle disposizioni adottate dal Codice Etico e dalla presente procedura si può prevenire la commissione dei citati reati.

2 ACRONIMI AZIENDALI

AU	Amministratore Unico
RSPP	Responsabile del Servizio Prevenzione e Protezione

RSGQ	Responsabile Sistema di Gestione Qualità
RTEC/RPROG	Responsabile Tecnico/Responsabile Progettazione
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RPROG	Responsabile Progettazione
RGAD	Responsabile Gestione Archivi e Documenti
REC	Responsabile Esterno Contabilità

PER L'IDENTIFICAZIONE DEI SOGGETTI CHE CORRISPONDONO AGLI ACRONIMI AZIENDALI SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI GETOPEN S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di GETOPEN S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di GETOPEN S.r.l.

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

Il presente protocollo, le disposizioni del Codice Etico e del Modello, dovranno essere osservati da tutte le Funzioni Aziendali che si occupano del processo di scelta e gestione dei partner commerciali, sia essi fornitori di prodotti - come attrezzature elettroniche, prodotti di cancelleria, *software*, *etc.* -, sia essi fornitori di servizi – come società e/o professionisti che svolgono attività di consulenza, studi di commercialisti/avvocati, *etc.* –, nonché a tutti coloro che, a diverso titolo, sono coinvolti nella gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni.

La gestione degli omaggi viene affidata dall'Amministratore Unico ad un Responsabile all'uopo preposto il quale dovrà:

- monitorare e accertare la corretta esecuzione del processo di distribuzione degli Omaggi;

- monitorare la conservazione dei beni destinati a omaggi.

5 GESTIONE DEGLI OMAGGI, SPESE DI RAPPRESENTANZA E SPONSORIZZAZIONE

GETOPEN assicura che le attività inerenti alla gestione degli omaggi, delle liberalità e delle spese di rappresentanza siano condotte in maniera trasparente e documentabile, nel rispetto delle regole di condotta definite nel Codice Etico.

Gli omaggi devono rientrare nell'ambito del budget di funzione, previsto in fase di pianificazione, e il relativo processo di acquisto deve avvenire nel rispetto dei principi espressi dal Codice Etico e degli elementi di controllo previsti dal processo di acquisto di beni e servizi di GETOPEN, declinati nel presente documento.

È previsto il divieto di qualsiasi forma di regalo a funzionari pubblici italiani ed esteri, o a loro familiari, nonché ai fornitori/partner della Società che possa influenzare la discrezionalità ovvero l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per GETOPEN.

Le donazioni e le spese di rappresentanza devono essere autorizzate dall'Amministratore Unico.

Tutte le spese di rappresentanza devono essere inerenti alle attività aziendali e rendicontate attraverso la predisposizione di un'opportuna nota spese a cui si allegano i relativi giustificativi fiscalmente validi, fornendo l'indicazione della data, della tipologia di spesa, dell'importo e dei soggetti terzi beneficiari.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, la funzione Aziendale all'uopo preposta deve comunicare, annualmente, all'Odv, un'informativa periodica, riepilogativa degli omaggi, delle liberalità e delle spese di rappresentanza effettuate durante l'anno con l'indicazione per ciascuna di esse del beneficiario, della data, dell'importo e della causale.

SI PRECISA CHE, AI FINI DEL PRESENTE PROTOCOLLO, VALGONO LE SEGUENTI DEFINIZIONI:

• **PER OMAGGI** si intendono le elargizioni di beni di modico valore offerte, nell'ambito delle ordinarie relazioni di affari, al fine di promuovere l'immagine di GETOPEN;

• **PER SPESE DI RAPPRESENTANZA** si intendono le spese sostenute da GETOPEN nell'espletamento delle relazioni commerciali, destinate a promuovere e migliorare l'immagine della Società (ad es. spese per rinfreschi, per forme di accoglienza ed ospitalità, ecc.);

• **PER INIZIATIVE DI BENEFICENZA** si intendono le elargizioni in denaro che GETOPEN destina esclusivamente ad Enti senza fini di lucro;

• **PER SPONSORIZZAZIONI** si intendono la promozione, la valorizzazione ed il potenziamento dell'immagine della GETOPEN attraverso la stipula di contratti atipici (in forma libera, di natura patrimoniale, a prestazioni corrispettive) con Enti esterni (ad es.: Enti senza fini di lucro, Enti territoriali ed organismi locali, ecc.).

Una gestione non trasparente dei processi relativi a omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni potrebbe, infatti, consentire la commissione di tali reati, ad esempio attraverso il riconoscimento/concessione di vantaggi ad esponenti della Pubblica Amministrazione e/o ad esponenti apicali, e/o a persone loro subordinate, di società o enti controparti o in relazione con la Società, al fine di favorire interessi di GETOPEN ovvero la creazione di disponibilità utilizzabili per la realizzazione dei reati in questione.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte di GETOPEN, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

6 PROCESSO DI GESTIONE E SELEZIONE DEI PARTENER COMMERCIALI

LA REGOLAMENTAZIONE DELL'ATTIVITÀ PREVEDE:

1. che i partner devono essere solo enti ben noti, affidabili e con un'eccellente reputazione in quanto a onestà e pratiche commerciali corrette;

2. che sia eseguita la qualifica su ogni partner; tale qualifica potrebbe non risultare necessaria per esempio, in ragione della consuetudine delle relazioni col Partner, la sua riconosciuta reputazione, la sua dimostrata affidabilità, l'eccellente reputazione del Partner sotto il profilo etico;

3. la formalizzazione dell'iter decisionale e delle motivazioni che hanno portato alla

scelta del Partner;

4. la definizione dei requisiti minimi di affidabilità/onorabilità/attendibilità commerciale del Partner sulla base di alcuni indici rilevanti (es. dati pregiudizievoli pubblici - protesti, procedure concorsuali - o acquisizione di informazioni commerciali sulla azienda, sui soci e sugli amministratori tramite società specializzate e/o mediante ottenimento di specifica autocertificazione da parte della controparte e/o mediante la presentazione del Certificato Generale del Casellario Giudiziario);

5. la tracciabilità della documentazione rilevante, il livello di formalizzazione e modalità/tempistiche di archiviazione;

6. specifiche clausole con cui i terzi si obbligano a non tenere alcun comportamento, non porre in essere alcun atto od omissione e non dare origine ad alcun fatto da cui possa derivare una responsabilità ai sensi del D.Lgs. n. 231/2001 e dichiarino di conoscere e si obblighino a rispettare i principi generali contenuti nel Codice Etico e nel Modello adottati da GETOPEN nonché clausole che prevedano l'applicazione di sanzioni nel caso di violazione di tali obblighi.

Orbene, tutti coloro che, in ragione del proprio incarico o della propria funzione, sono coinvolti nella gestione del processo relativo alla scelta dei partner commerciali devono:

- garantire la completa tracciabilità dell'*iter* decisionale, autorizzativo e delle attività di controllo svolte;
- garantire che la scelta dei fornitori di beni e sevizi o e dei consulenti sia aderente rispetto alle reali esigenze aziendali, evitando la configurazione di ogni possibile situazione di conflitto di interessi;
- informare i fornitori di beni e servizi, le società committenti/appaltatrici ed i professionisti esterni, che GETOPEN S.r.l. ha adottato il Modello di Organizzazione Gestione e Controllo previsto dal D.Lgs 231/2001 ed un Codice Etico, e richiedere l'impegno a rispettare le leggi e i regolamenti applicabili in Italia, nonché, ove ritenuto necessario, il rispetto dei principi di

comportamento e di controllo previsti dal predetto Modello e dal Codice Etico, compresa tutta la vigente normativa antiriciclaggio, il rispetto delle norme contributive, fiscali, previdenziali ed assicurative in favore dei propri dipendenti e collaboratori, degli obblighi di tracciabilità finanziaria, nonché l'assenza di provvedimenti a carico dei fornitori, dei professionisti e degli enti e/o dei suoi apicali, per i reati di cui al D.Lgs n. 231/2001;

- privilegiare, ove possibile, i fornitori dotati rispettivamente di un Sistema per la Gestione della Qualità, di un Sistema di Gestione Ambientale, di un Sistema di Gestione della Salute e Sicurezza certificato, nonché fornitori che si siano conformati al rispetto delle regole di prevenzione dei reati di cui al D.Lgs. 231/2001 e degli standard sociali minimi;
- scegliere i partner commerciali solo dopo aver svolto idonee verifiche sulla reputazione e sulla affidabilità sul mercato degli stessi.

7 OMAGGI, VANTAGGI ECONOMICI OFFERTI AL PERSONALE O RICEVUTI DAL PERSONALE

LA REGOLAMENTAZIONE DELL'ATTIVITÀ PREVEDE:

1) che qualsiasi omaggio, vantaggio economico o altra utilità offerto a, o ricevuto da, personale deve essere, da un punto di vista oggettivo, ragionevole e in buona fede;

2) deve essere comunicato all'Amministratore Unico l'omaggio o vantaggio economico offerto a, o ricevuto da, personale, qualora il suo valore effettivo o stimato ecceda singolarmente, la "soglia singola" definita in 150 euro o, cumulativamente, quando ricevuto da o offerto dallo stesso soggetto o ente in un anno, la "soglia cumulata" (corrispondente a quattro volte la "soglia singola"), anche se singolarmente ciascun omaggio o beneficio non supera la "soglia singola" indicata al punto precedente.

3) la registrazione (anche se rifiutato) in maniera accurata e trasparente in apposito registro, mantenuto dalla funzione competente che contiene le seguenti informazioni:

3.1 nome della persona personale al quale è stato offerto o che ha ricevuto l'omaggio, vantaggio economico (beneficiario);

3.2 nome della società e della persona che ha effettuato tale offerta o fornito l'omaggio, vantaggio economico;

3.3 data dell'offerta dell'omaggio al personale;

3.4 valore attuale o stimato;

3.5 indicazione dell'eventuale accettazione o rifiuto e delle relative motivazioni.

8 OMAGGI DATI A TERZE PARTI

LA REGOLAMENTAZIONE DELL'ATTIVITÀ PREVEDE:

1) che un omaggio è ragionevole e in buona fede quando è direttamente collegato:

1.1 alla promozione, dimostrazione o illustrazione di prodotti o servizi;

1.2 allo sviluppo e mantenimento di cordiali rapporti di business.

9 PRINCIPI GENERALI DI COMPORTAMENTO E DESCRIZIONE DEL PROCESSO

I Destinatari del Modello di Organizzazione Gestione e Controllo che, per ragione del proprio incarico o della propria funzione o mandato, siano coinvolti nella gestione di omaggi, liberalità e sponsorizzazioni devono garantire che:

• il valore, la natura e lo scopo dell'omaggio, della liberalità o della sponsorizzazione siano considerati eticamente corretti, ovvero tali da non compromettere l'immagine di GETOPEN;

• il valore e la natura del regalo siano tali da non poter essere interpretati come un mezzo per ottenere trattamenti di favore per GETOPEN;

• detti omaggi, liberalità e sponsorizzazioni siano stati debitamente autorizzati e siano documentati in modo adeguato.

È IN OGNI CASO FATTO DIVIETO DI:

❖ promettere o effettuare omaggi, liberalità e sponsorizzazioni, per finalità diverse da quelle istituzionali e di servizio;

❖ promettere o concedere omaggi o liberalità, dirette o indirette, non di modico valore – vale a dire eccedente le normali pratiche di cortesia – e comunque, rivolti ad acquisire illeciti trattamenti di favore nella conduzione di qualsiasi attività di GETOPEN;

❖ promettere o concedere vantaggi di qualsiasi natura al fine di influenzare l'indipendenza di giudizio o di ottenere un qualsiasi vantaggio per GETOPEN;

❖ disporre pagamenti per sponsorizzazioni (anche tramite bonifico) verso soggetti diversi da quelli previsti dal contratto;

❖ ricevere o sollecitare elargizioni in denaro o assimilati, omaggi, regali o vantaggi di altra natura; ai dipendenti e ai collaboratori è fatto divieto di accettare, anche in occasioni di festività, per sé o per altri, omaggi o altre utilità, ad eccezione dei regali d'uso di modico valore (inferiori all'ammontare approssimativo di Euro 150 - centocinquanta) e/o ascrivibili a normali corretti rapporti di cortesia, tali da non compromettere l'integrità o la reputazione di una delle parti né da poter essere interpretati, da un osservatore imparziale, come finalizzati ad acquisire vantaggi indebiti e/o in modo improprio. Il dipendente che, indipendentemente dalla sua volontà, riceva doni o altre utilità di non modico valore e comunque in difformità da quanto sopra stabilito, ne dà tempestiva comunicazione scritta all'Amministratore Unico, il quale potrà stabilire la restituzione di essi.

I PROCESSI DI GESTIONE DELLE SPESE PER BENEFICENZE E PER SPONSORIZZAZIONI SI ARTICOLANO NELLE SEGUENTI FASI:

- ricezione della richiesta, inviata dagli Enti, di elargizioni e di beneficenze o sponsorizzazioni per progetti, iniziative, manifestazioni;
- individuazione di società/organizzazioni cui destinare le elargizioni;
- effettuazione delle attività di due diligence di GETOPEN;
- esame/valutazione dell'iniziativa/progetto proposto;
- autorizzazione alla spesa e, qualora previsto, stipula dell'accordo/ contratto;
- erogazione delle elargizioni da parte di GETOPEN.

Le spese per omaggi sono consentite purché di modico valore e, comunque, tali da non compromettere l'integrità e la reputazione di una delle parti e da non influenzare l'autonomia di giudizio del beneficiario, le Funzioni Aziendali, a qualsiasi titolo coinvolte nella gestione di omaggi, delle spese di rappresentanza, delle beneficenze e delle sponsorizzazioni sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna, nonché le eventuali previsioni del Codice Etico e del Codice Disciplinare di GETOPEN, nonché dalle disposizioni in materia di anticorruzione.

IN PARTICOLARE:

- GETOPEN può effettuare erogazioni sotto forma di beneficenze o sponsorizzazioni per sostenere iniziative di enti regolarmente costituiti ai sensi di legge e che non contrastino con i principi etici della Società e nel caso di beneficenze, tali enti non devono avere finalità di lucro;
- eventuali iniziative la cui classificazione rientri nei casi previsti per le "sponsorizzazioni" non possono essere oggetto contemporaneo di erogazione per beneficenza;
- le erogazioni devono essere riconosciute esclusivamente su un conto corrente intestato all'ente beneficiario; non è consentito effettuare pagamenti in contanti, in un Paese diverso da quello dell'ente beneficiario o a un soggetto diverso dallo stesso.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- effettuare erogazioni, per iniziative di beneficenza o di sponsorizzazione, a favore di enti coinvolti vicende giudiziarie note, pratiche non rispettose dei diritti umani, o contrarie alle norme in tema di vivisezione e di tutela dell'ambiente. Non possono essere destinatari di erogazioni partiti e movimenti politici e le loro articolazioni organizzative, organizzazioni sindacali e di patronato, club, associazioni e gruppi

ricreativi, scuole private, parificate e/o legalmente riconosciute, salvo specifiche iniziative connotate da particolare rilievo sociale, culturale o scientifico che devono essere approvate dall'A;

• effettuare elargizioni/omaggi a favore di enti/esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero ad altre organizzazioni/persone ad essa collegate contravvenendo a quanto previsto nel presente protocollo;

• promettere o versare/offrire – anche a mezzo di intermediari - somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura a esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero altre organizzazioni con la finalità di promuovere o favorire interessi di GETOPEN, anche a seguito di illecite pressioni. Il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta al PRES per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;

• promettere o versare/offrire somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparte o in relazione con GETOPEN, al fine di favorire indebitamente gli interessi della Società;

• dare in omaggio beni per i quali non sia stata accertata la legittima provenienza ed il rispetto delle disposizioni che tutelano le opere dell'ingegno, i marchi e i diritti di proprietà industriale in genere, nonché le indicazioni geografiche e le denominazioni di origine protette.

Le Funzioni Aziendali interessate sono tenute a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

9.1 PRINCIPI DI CONTROLLO

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

• LIVELLI AUTORIZZATIVI DEFINITI:

o per quanto attiene ai beni destinati ad omaggi ed alle spese di rappresentanza, l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe e/o apposite autorizzazioni in essere, che stabiliscano le facoltà di autonomia gestionale per natura di spesa e impegno.

---

o gli omaggi o le altre utilità di valore superiore a 150 euro possono essere ammissibili in via eccezionale, in considerazione del profilo del donante o del beneficiario, e comunque nei limiti della ragionevolezza, previa autorizzazione scritta del PRES.

• ATTIVITÀ DI CONTROLLO:

O IN PARTICOLARE È PREVISTA:

▪ l'analisi e la verifica del tipo di organizzazione e della finalità per la quale è costituita;

▪ la verifica ed approvazione di tutte le erogazioni da parte del PRES;

▪ la verifica che le erogazioni complessive siano stabilite annualmente e trovino capienza in apposito budget deliberato dagli Organi competenti;

o per le sponsorizzazioni è necessaria una puntuale verifica del corretto adempimento della controprestazione acquisendo idonea documentazione comprovante l'avvenuta esecuzione della stessa.

o disporre che venga regolarmente tenuto in evidenza l'elenco dei beneficiari, l'importo delle erogazioni ovvero gli omaggi distribuiti nonché le relative date/occasioni di elargizioni e tale elenco verrà condiviso nell'apposita piattaforma digitale all'uopo preposta come TEAMS (o simili).

• TRACCIABILITÀ DEL PROCESSO SIA A LIVELLO DI SISTEMA INFORMATIVO SIA IN TERMINI DOCUMENTALI:

o tracciabilità a livello documentale e di sistema dei processi di gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni anche attraverso la redazione di una reportistica sulle erogazioni effettuate e/o sui contratti stipulati;

o al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, le Funzioni Aziendali interessate sono responsabili dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni e, pertanto, dovranno provvedere a caricare tutta la documentazione nell'apposita piattaforma digitale all'uopo preposta come TEAMS (o simili).

10 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

Tutti i *Destinatari* coinvolti nella selezione e gestione dei fornitori di beni, servizi e incarichi professionali informano tempestivamente l'Organismo di Vigilanza di:

- ✓ situazioni anomale e/o poste in essere in deroga alla presente procedura;
- ✓ comportamenti posti in essere in violazione a quanto previsto nel Modello e nel Codice Etico.

Nell'ipotesi in cui si dubiti della moralità dei *partner* commerciali, la funzione aziendale che ha chiesto la fornitura/consulenza dovrà informare tempestivamente l'Organismo di Vigilanza, nonché comunicare l'eventuale insorgenza di criticità nei rapporti con il *partner*.

I *Destinatari* devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, tenendo a disposizione dell'Organismo di Vigilanza – in un archivio ordinato – tutta la documentazione all'uopo necessaria.

Si precisa che, deve, essere annualmente trasmesso all'Organismo di Vigilanza l'elenco degli omaggi erogati a soggetti appartenenti alla Pubblica Amministrazione e/o a soggetti privati.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse ai Processi Sensibili al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute; infatti, è obbligo per chiunque segnalare, tempestivamente, all'OdV anomalie e/o violazione della presente procedura, del Modello e del Codice Etico relativi ai processi di gestione riguardanti le scelte dei partner commerciali, nonché quelli riguardanti l'elargizione degli omaggi, delle spese di rappresentanza, delle beneficenze e delle sponsorizzazioni.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 20.03.2024	ADOZIONE
Rev. 1	Determina dell'Amministratore Unico del 05.08.2024	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231)

PARTE SPECIALE -7-

SOMMARIO

1 OBIETTIVI E FUNZIONI DEL MODELLO

Il presente protocollo ha lo scopo di presidiare le aree di attività aziendali a rischio-reato nell'ambito della gestione del contenzioso, in cui la Società è coinvolta, condotte dai destinatari del Modello.

Coerentemente con la Parte Generale del Modello, il documento definisce le linee guida comportamentali nonché i presidi operativi di controllo a cui tutti i destinatari si attengono nello svolgimento della propria attività al fine di prevenire o mitigare il rischio di commissione dei reati presupposto di cui agli artt. 24, 25, 25-ter e 25-quinquiesdecies D.Lgs. 231/2001.

Il presente protocollo, redatto in conformità alle previsioni del D.Lgs. 231/2001, costituisce pertanto parte integrante del Modello

Ai sensi del D. Lgs. 231/2001, il processo relativo alla gestione dei contenziosi giudiziali e stragiudiziali, nonchè delle dichiarazioni da rendere all'Autorità Giudiziaria, potrebbe presentare occasioni per la commissione dei reati di "*Corruzione contro la Pubblica Amministrazione*", "*Induzione indebita a dare o promettere utilità*", "*Traffico di influenze illecite*", e "*Truffa ai danni dello Stato o di altro Ente pubblico*" nonché del reato di "In*duzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*".

Inoltre, sussiste, altresì, il rischio della commissione dei reati di "*Corruzione tra privati*" e "*Istigazione alla corruzione tra privati*".

2 ACRONIMI AZIENDALI

AU	Amministratore Unico
RSPP	Responsabile del Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC/RPROG	Responsabile Tecnico/ Responsabile Progettazione
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
REC	Responsabile Esterno Contabilità

PER L'IDENTIFICAZIONE DEI SOGGETTI CHE CORRISPONDONO AGLI ACRONIMI AZIENDALI SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI GETOPEN S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di GETOPEN S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di GETOPEN S.r.l..

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

Il presente protocollo si applica a tutte le Funzioni Aziendali e/o ad eventuali consulenti esterni coinvolti nella gestione dei contenziosi giudiziali e stragiudiziali (ad es. amministrativo, civile, penale, fiscale, giuslavoristico e previdenziale) e degli accordi transattivi con enti pubblici o con soggetti privati, nonché a tutti i *Destinatari* (compresi i Collaboratori ed i Consulenti esterni all'uopo incaricati) che, in occasione di procedimenti penali, entrino in contatto con l'Autorità Giudiziaria e che ricoprano la qualità di imputati o coimputati in un procedimento connesso o collegato.

Il Responsabile della procedura è l'Amministratore Unico.

5 PRINCIPI GENERALI DI COMPORTAMENTO E DESCRIZIONE DEL PROCESSO

I Destinatari a qualsiasi titolo coinvolti nella gestione di un contenzioso in cui sia coinvolta GETOPEN in ordine agli ambiti di applicazione sopra richiamati sono tenuti a osservare, oltre alle previsioni del presente protocollo, le norme di legge applicabili, i principi di condotta previsti nel Codice Etico nonché i principi previsti nella Parte Generale del Modello.

È FATTO DIVIETO DI:

• adottare comportamenti reticenti, omissivi o che possano risultare, anche indirettamente, di intralcio all'operato dell'autorità giudiziaria e degli ausiliari della stessa;

• operare qualsivoglia pressione, anche mediante l'utilizzo di violenza o minaccia, o di offerta di denaro o altra utilità, al fine di indurre un soggetto a non rendere dichiarazioni ovvero a rendere dichiarazioni false avanti all'autorità giudiziaria o ad ausiliari della stessa.

È FATTO OBBLIGO DI:

• assicurare che, in caso di contenzioso, i rapporti con gli studi legali siano intrattenuti solo da esponenti aziendali dotati del potere di rappresentanza processuale e muniti di apposito mandato;

• assicurare che eventuali transazioni aventi ad oggetto contenziosi in cui è coinvolta la Società siano autorizzate e sottoscritte solo da procuratori della Società muniti di adeguati poteri.

Il processo di gestione degli accordi transattivi riguarda tutte le attività necessarie per prevenire o dirimere una controversia attraverso accordi o reciproche rinunce e concessioni, al fine di evitare l'instaurarsi o il proseguire di procedimenti giudiziari.

6 PRESIDI DI CONTROLLO SPECIFICI PER ATTIVITÀ SENSIBILE

GESTIONE DEL CONTENZIOSO

CON RIFERIMENTO ALL'ATTIVITÀ SENSIBILE IN OGGETTO:

• le attività inerenti ai contenziosi in cui è coinvolta la Società sono gestite esclusivamente dall'Amministratore Unico a cui è attribuito: **1)** il potere di rappresentanza della Società in giudizio, nonché il potere di nominare e revocare avvocati, procuratori, arbitri, commercialisti e consulenti tecnici, conferendo loro l'incarico di esperire le azioni giudiziarie necessarie nell'interesse della società; **2)** il potere di transigere vertenze in sede sia giudiziale sia stragiudiziale, accettare

concordati sia giudiziali sia concorsuali in ordine all'attività aziendale, con facoltà di riscuotere o di pagare le somme previamente autorizzate dall'AU;

• l'Attività Sensibile in esame è regolata da una specifica procedura/policy che disciplina le fasi principali, gli attori coinvolti, i relativi ambiti di intervento e di responsabilità, le modalità di tracciabilità e documentabilità, con particolare riferimento a:

- identificazione dei principi di indirizzo per la definizione delle iniziative da intraprendere tenuto conto della natura, dell'oggetto e del valore della causa e relativi livelli approvativi o comunque di condivisione;
- i legali esterni devono essere nominati con apposita procura; solo i legali esterni all'uopo autorizzati, si possono interfacciare con i soggetti coinvolti in procedimenti giudiziari o che sono chiamati a rendere dichiarazioni davanti all'Autorità Giudiziaria;
- formalizzazione dell'incarico;
- identificazione di una figura di riferimento interna, coerentemente con l'oggetto della materia;
- soggetti coinvolti, ambiti di responsabilità e processo decisionale/autorizzativo nella definizione e sottoscrizione di accordi transattivi;
- archiviazione della documentazione prodotta;

• la tracciabilità e la verificabilità ex post delle attività riconducibili all'Attività Sensibile in esame sono garantite dall'archiviazione della documentazione prodotta durante le varie fasi della stessa da parte delle Funzioni coinvolte, in linea con le modalità di archiviazione previste dalla citata procedura.

7 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

TUTTE LE FUNZIONI AZIENDALI ED I COLLABORATORI ESTERNI COINVOLTI NELLA GESTIONE DEI CONTENZIOSI, DEGLI ACCORDI TRANSATTIVI E DELLE DICHIARAZIONI RESE ALL'AUTORITÀ GIUDIZIARIA, NELL'AMBITO DI PROCEDIMENTI PENALI, DEVONO, TEMPESTIVAMENTE, COMUNICARE ALL'ORGANISMO DI VIGILANZA:

- di essere a conoscenza di situazioni anomale e/o in contrasto con la presente procedura;
- di essere a conoscenza di eventuali comportamenti non conformi alle disposizioni del Codice Etico e del Modello.
- di essere a conoscenza di procedimenti giudiziari incardinati nei confronti dei soggetti che operano nella GETOPEN S.r.l.

I *Destinatari* della presente procedura devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposto nell'apposita piattaforma informatica di condivisione – tutta la documentazione necessaria.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV DOVRÀ, IN PARTICOLARE, EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di *corporate governance* per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 20.03.2024	ADOZIONE
Rev. 1	Determina dell'Amministratore Unico del 05.08.2024	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231)

PARTE SPECIALE -8-

SOMMARIO

1 OBIETTIVI E LA FUNZIONE DEL MODELLO

Il presente protocollo definisce i ruoli, le responsabilità operative, le attività di controllo ed i principi di comportamento adottati da GETOPEN S.r.l. nell'ambito del processo di gestione ed utilizzo di opere dell'ingegno per le attività a rischio connesse alle fattispecie di reato previste dall'art. 25 novies *"Reati in materia di violazione del diritto di autore"*, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione, nonché tracciabilità delle attività.

Inoltre, al fine di contrastare ancor più severamente la pirateria delle opere dell'ingegno e i gravi danni economici arrecati agli autori e all'industria connessa, la presente procedura rimanda ai reati contemplati dalla legge sul diritto d'autore (L. 633/1941).

Le prescrizioni della presente procedura integrano, altresì, i principi di comportamento contenuti nel Codice Etico di GETOPEN.

2 ACRONIMI AZIENDALI

AU	Amministratore Unico
RSGQ	Responsabile Sistema di Gestione Qualità
RAM	Responsabile Amministrazione - Risorse Umane
RTEC/RPROG	Responsabile Tecnico/Responsabile Progettazione
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RSCM	Responsabile singola commessa
RATTR	Responsabile Attrezzature e Mezzi
PROG	Programmatori

PER L'IDENTIFICAZIONE DEI SOGGETTI CHE CORRISPONDONO AGLI ACRONIMI AZIENDALI SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI GETOPEN S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di GETOPEN S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di GETOPEN S.r.l..

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

La presente procedura si applica a tutti i *Destinatari* coinvolti nelle attività di gestione ed utilizzo di opere dell'ingegno all'interno della Società.
Il principale responsabile della procedura è l'AU.

5 REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

La presente sezione della Parte Speciale si riferisce ai reati in materia di violazione del diritto d'autore, richiamati dall'art 25 novies del D.Lgs.231/2001 ed in particolare riporta le singole fattispecie di reato considerate rilevanti per la responsabilità amministrativa di GETOPEN. Individua inoltre le cosiddette attività "sensibili" (quelle dove è teoricamente possibile la commissione del reato e che sono state individuate nell'ambito dell'attività di risk assessment) specificando i principi comportamentali ed i presidi di controllo operativi per l'organizzazione, lo svolgimento e la gestione delle operazioni svolte nell'ambito delle sopracitate attività "sensibili". In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di GETOPEN i seguenti reati:

- **DIVULGAZIONE TRAMITE RETI TELEMATICHE DI UN'OPERA DELL'INGEGNO PROTETTA (ART. 171 COMMA 1 LETT. A-BIS E COMMA 3. LEGGE SUL DIRITTO D'AUTORE)**

In relazione alla fattispecie delittuosa di cui all'art. 171 della Legge sul Diritto d'Autore, il Decreto ha preso in considerazione esclusivamente due fattispecie, ovvero:

• la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa;

• la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore o alla reputazione dell'autore.

Se dunque nella prima ipotesi ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere lese le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete, nella seconda ipotesi il bene giuridico protetto non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera, ma il suo onore e la sua reputazione.

- **REATI IN MATERIA DI SOFTWARE E BANCHE DATI (ART. 171-BIS, LEGGE 633/41)**

Punisce chi abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); ovvero chi, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati.

Tale norma è posta a tutela penale del software e delle banche dati. Con il termine "software", si intendono i programmi per elaboratore, in qualsiasi forma espressi, purché originali, quale risultato della creazione intellettuale dell'autore; mentre con "banche dati", si intendono le raccolte di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo.

6 IDENTIFICAZIONE DELLE ATTIVITA' A RISCHIO REATO

L'analisi dei processi aziendali ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamata dall'articolo 25-novies del d.lgs. 231/01. Di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai delitti in materia di violazione del diritto d'autore:

- Gestione della riproduzione e diffusione al pubblico attraverso i sistemi informativi aziendali e/o dei Social Media di opere tutelate dal diritto di autore e dai diritti connessi;
- Utilizzo di software soggetto a licenze nell'ambito dei sistemi informativi aziendali.

7 PRINCIPI GENERALI DI COMPORTAMENTO

Coerentemente con i principi deontologici aziendali di cui alla Parte Generale del Modello Organizzativo ex D.Lgs.231/2001 e del Codice Etico adottati dalla Società, nello svolgimento delle attività sensibili sopra citate, tutti i Destinatari del Modello sono tenuti ad osservare i seguenti principi di comportamento e controllo.

In via generale, a tali soggetti è fatto divieto di:

- utilizzare e, in particolare, diffondere al pubblico – anche attraverso siti internet, opere di terzi tutelate dal diritto d'autore in mancanza di accordi contrattuali formalizzati per iscritto con i relativi titolari per lo sfruttamento economico delle stesse nonché in violazione dei termini e delle condizioni previste in detti accordi;
- duplicare e/o installare opere tutelate dal diritto d'autore non recanti il contrassegno SIAE o recanti detto contrassegno contraffatto (ad esempio libri, riviste, cd, etc);
- riprodurre, nei documenti della Società, immagini, contenuti, oggetti protetti dal diritto d'autore senza averne pagato i relativi diritti o averne comunque concordato l'uso con i legittimi proprietari;
- utilizzare software privi delle necessarie autorizzazioni o licenze nell'ambito dei sistemi informativi aziendali;

• duplicare e/o diffondere in qualsiasi forma programmi e files se non nelle forme e per gli scopi di servizio per i quali sono stati assegnati e nel rispetto delle licenze ottenute;

• riprodurre CD, banche dati e, più in generale, supporti sottoposti a licenza d'uso, violandone i limiti di utilizzo ivi declinati;

• installare e utilizzare, sui sistemi informatici della Società, software mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di files senza alcuna possibilità di controllo da parte della Società;

• riprodurre o diffondere, in qualunque forma e senza diritto, l'opera intellettuale altrui, in mancanza di accordi contrattuali formalizzati per iscritto con i relativi titolari per lo sfruttamento economico o in violazione dei termini e delle condizioni previste in detti accordi.

8 IL SISTEMA DEI CONTROLLI E I PRESIDI A MITIGAZIONE DEI RISCHI REATO

Per ognuna delle attività sensibili identificate sono stati individuati i sistemi dei controlli e i presidi in essere a mitigazione dei rischi reato in riferimento ai reati di delitti in materia di violazione del diritto di autore,

IN PARTICOLARE:

- Adozione di regole comportamentali all'interno del Codice Etico che prevedono il divieto a tutte le funzioni aziendali, nell'ambito delle proprie attività lavorative e/o mediante utilizzo delle risorse di GETOPEN di porre in essere comportamenti di qualsivoglia natura atti a ledere diritti di proprietà intellettuale altrui, assicurando il rispetto delle leggi e delle disposizioni regolamentari nazionali, comunitarie e internazionali poste a tutela della proprietà industriale, della proprietà intellettuale e del diritto d'autore;
- disporre una regola comportamentale che impone ai dipendenti di curare diligentemente gli adempimenti di carattere amministrativo connessi all'utilizzo di opere protette dal diritto d'autore (software, banche dati,

ecc.) nell'ambito dell'utilizzo di applicazioni software di terzi;

- **PER QUANTO ATTIENE ALL'USO DELLE DOTAZIONI INFORMATICHE È RICHIESTO AI DIPENDENTI DI NON:**

- ✓ utilizzare in azienda apparecchiature informatiche private, connettendole in qualsiasi modo alla rete informatica aziendale;
- ✓ installare sui computer o sui dispositivi aziendali assegnati programmi (software) provenienti dall'esterno ovvero dispositivi di memorizzazione, comunicazione o altro (masterizzatori, modem, chiavi USB);
- ✓ duplicare CD e DVD od ogni altro supporto multimediale atto a contenere dati di qualsiasi natura protetti dalla normativa a tutela del diritto d'autore.
- GETOPEN garantisce che i software di terzi utilizzati per lo svolgimento delle attività aziendali, siano opportunamente identificati e che il pagamento delle licenze ai rispettivi fornitori, sia oggetto di un controllo periodico.

9 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Tutte le Funzioni Aziendali coinvolte nelle attività di gestione ed utilizzo delle opere di ingegno sono tenuti a comunicare tempestivamente all'Organismo di Vigilanza:

- ➢ qualsiasi violazione ai principi di comportamento adottati;
- ➢ qualsiasi situazione non conforme alla normativa;
- ➢ qualsiasi violazione del Modello e del Codice Etico, indicando le ragioni delle difformità e rilevando il processo autorizzativo seguito.

I *Destinatari* devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio ordinato – tutta la documentazione all'uopo necessaria.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di corporate governance per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 20.03.2024	ADOZIONE
Rev. 1	Determina dell'Amministratore Unico del 05.08.2024	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231)

PARTE SPECIALE -9-

SOMMARIO

1 OBIETTIVI E FUNZIONI DEL MODELLO

Il D.Lgs. 7 luglio 2011, n. 121 - recante "*Attuazione della Direttiva 2008/99/CE sulla tutela penale dell'ambiente e della direttiva 2009/123/CE che modifica la direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni*" – ha introdotto, nell'ambito dei reati presupposto di cui al d.lgs. 231/01, l'art. 25-undecies, che prevede la responsabilità degli enti per i reati ambientali.

Più recentemente, la Legge 22 maggio 2015 n. 68 recante "Disposizioni in materia di delitti contro l'ambiente" (G.U. Serie Generale n.122 del 28-5-2015), oltre ad aver modificato in maniera significativa il d.lgs.152/2006 in materia, ha introdotto all'interno del codice penale un lungo elenco di reati ambientali (collocati nel nuovo Titolo VI-bis intitolato "Dei delitti contro l'ambiente"), una buona parte dei quali è configurato dalla Legge stessa come reato presupposto atto a far scattare la responsabilità amministrativa dell'impresa, con conseguente modificazione e integrazione dell'articolo 25-undecies del decreto legislativo 8 giugno 2001 n.231.

IN PARTICOLARE:

I delitto di inquinamento ambientale (art. 425-bis c.p.);
II delitto di disastro ambientale (art. 452-quater c.p.);
III delitti colposi contro l'ambiente (art.452-quinquies c.p.);
IV delitti associativi aggravati ai sensi dell'articolo 452-octies;
V delitto di traffico e abbandono di materiale ad alta radioattività (art. 452 sexies c.p.).

Successivamente il D.lgs 21/2018 ha abrogato l'art. 260 del D.Lgs. 152/2006, introducendo l'art. 452-quaterdecies nel codice penale (Attività organizzate per il traffico illecito di rifiuti) al quale oggi l'articolo 25-undecies del decreto legislativo 8 giugno 2001 n.231 deve intendersi far riferimento.

La legge dispone inoltre che nei casi di condanna per i reati di inquinamento ambientale e di disastro ambientale si applichino, oltre alle sanzioni pecuniarie ivi

previste, le sanzioni interdittive previste dall'articolo 9 del D.Lgs. 231/01, per un periodo non superiore a un anno in relazione al delitto di inquinamento.

Nel seguito si riporta, dunque, il testo dei relativi reati presupposto, suddivisi in:

- reati potenzialmente realizzabili;
- reati la cui commissione è considerata remota/non ipotizzabile.

REATO	RIFERIMENTO	REALIZZABILITA'
Attività di gestione di rifiuti non autorizzata	Art. 256 d.lgs. 152/2006	Possibile
Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari	Art. 258 d.lgs. 152/2006	Possibile
Inquinamento ambientale	Art. 452-bis cp	Possibile
Delitti colposi contro l'ambiente	Art.452-quinquies cp	Possibile
Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette	Art. 727-bis c.p.	Non ipotizzabile
Distruzione o deterioramento di habitat all'interno di un sito protetto	Art. 733-bis c.p	Non ipotizzabile
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. 137 d.lgs.152/2006	Non ipotizzabile
Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee	Art. 257 d.lgs.152/2006)	Non ipotizzabile
Traffico illecito di rifiuti	Art. 259 d.lgs.152/2006	Non ipotizzabile
Attività organizzate per il traffico illecito di rifiuti	Art. 452-quaterdecies c.p.	Non ipotizzabile
Sistema informatico di controllo della tracciabilità	Art. 260 – bis d.lgs.152/2006	Non ipotizzabile

dei rifiuti		
Traffico esemplari	Art. 1 Legge 150/1992	Non ipotizzabile
Traffico esemplari	Art. 2 Legge 150/1992	Non ipotizzabile
Animali pericolosi	Art. 6 Legge 150/1992	Non ipotizzabile

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

ATTIVITÀ DI GESTIONE DI RIFIUTI NON AUTORIZZATA (ART. 256 D.LGS. 152/2006)

"*1. Chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214, 215 e 216 è punito: a) con la pena dell'arresto da tre mesi a un anno o con l'ammenda da duemilaseicento euro a ventiseimila euro se si tratta di rifiuti non pericolosi; b) con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro se si tratta di rifiuti pericolosi. (omissis)3. Chiunque realizza o gestisce una discarica non autorizzata è punito con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro. Si applica la pena dell'arresto da uno a tre anni e dell'ammenda da euro cinquemiladuecento a euro cinquantaduemila se la discarica è destinata, anche in parte, allo smaltimento di rifiuti pericolosi.*

Alla sentenza di condanna o alla sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale, consegue la confisca dell'area sulla quale è realizzata la discarica abusiva se di proprietà dell'autore o del compartecipe al reato, fatti salvi gli obblighi di bonifica o di ripristino dello stato dei luoghi. 4. Le pene di cui ai commi 1, 2 e 3 sono ridotte della metà nelle ipotesi di inosservanza delle prescrizioni contenute o richiamate nelle autorizzazioni, nonché nelle ipotesi di carenza dei requisiti e delle condizioni richiesti per le iscrizioni o comunicazioni. 5. Chiunque, in violazione del divieto di cui all'articolo 187, effettua attività non consentite di miscelazione di rifiuti,

è punito con la pena di cui al comma 1, lettera b). 6. Chiunque effettua il deposito temporaneo presso il luogo di produzione di rifiuti sanitari
pericolosi, con violazione delle disposizioni di cui all'articolo 227, comma 1, lettera b), è punito con la pena dell'arresto da tre mesi ad un anno o con la pena dell'ammenda da duemilaseicento euro a ventiseimila euro. Si applica la sanzione amministrativa pecuniaria da duemilaseicento euro a quindicimilacinquecento euro per i quantitativi non superiori a duecento litri o quantità equivalenti. (omissis)".

VIOLAZIONE DEGLI OBBLIGHI DI COMUNICAZIONE, DI TENUTA DEI REGISTRI OBBLIGATORI E DEI FORMULARI (ART. 258 D.LGS. 152/2006)

"(omissis) 4. Le imprese che raccolgono e trasportano i propri rifiuti non pericolosi di cui all'articolo 212, comma 8, che non aderiscono, su base volontaria, al sistema di controllo della tracciabilità dei rifiuti (SISTRI) di cui all'articolo 188-bis, comma 2, lettera a), ed effettuano il trasporto di rifiuti senza il formulario di cui all'articolo 193 ovvero indicano nel formulario stesso dati incompleti o inesatti sono puniti con la sanzione amministrativa pecuniaria da milleseicento euro a novemilatrecento euro. Si applica la pena di cui all'articolo 483 del codice penale a chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto. (omissis)".

INQUINAMENTO AMBIENTALE (ART. 452-BIS CODICE PENALE)

"*E' punito con la reclusione da due a sei anni e con la multa da euro 10.000 a euro 100.000 chiunque abusivamente cagiona una compromissione o un deterioramento significativi e misurabili: 1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo; 2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna. Quando l'inquinamento è prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette, la pena è aumentata.*"

Commette tale reato (delitto) chiunque abusivamente cagiona una compromissione o un deterioramento significativi e misurabili:
- delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo;
- di un ecosistema, della biodiversità, anche agraria, della flora o della fauna.

Il reato prevede un'aggravante per la persona fisica nel caso in cui l'inquinamento sia prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette. In caso di responsabilità amministrativa della persona giuridica, la sanzione pecuniaria per l'azienda va da 250 a 600 quote. E' prevista espressamente l'applicazione delle sanzioni interdittive elencate nell'art. 9 del D.Lgs.231/01 per l'azienda, per un periodo non superiore ad un anno.

DELITTI COLPOSI CONTRO L'AMBIENTE (ART.452-QUINQUIES DEL CODICE PENALE)

"Se taluno dei fatti di cui agli articoli 452-bis e 452-quater è commesso per colpa, le pene previste dai medesimi articoli sono diminuite da un terzo a due terzi. Se dalla commissione dei fatti di cui al comma precedente deriva il pericolo di inquinamento ambientale o di disastro ambientale le pene sono ulteriormente diminuite di un terzo."

La fattispecie dei delitti colposi contro l'ambiente, che sono reati-presupposto (al pari dei precedenti) per la responsabilità amministrativa dell'ente, prevede che se taluno dei fatti di cui ai reati di "inquinamento ambientale" e "disastro ambientale" (rispettivamente artt.452-bis e 452-quater c.p.) è commesso per colpa, le pene per le persone fisiche sono diminuite. Se dalla commissione dei fatti indicati sopra deriva il pericolo di inquinamento ambientale o di disastro ambientale, le pene sono ulteriormente diminuite. In caso di responsabilità amministrativa dell'Ente, la sanzione pecuniaria per l'azienda va da 200 a 500 quote.

* * *

I reati la cui commissione è stata ritenuta remota/non ipotizzabile:

UCCISIONE, DISTRUZIONE, CATTURA, PRELIEVO, DETENZIONE DI ESEMPLARI DI SPECIE ANIMALI O VEGETALI SELVATICHE PROTETTE (ART. 727-BIS C.P.)

"*1. Salvo che il fatto costituisca più grave reato, chiunque, fuori dai casi consentiti, uccide, cattura o detiene esemplari appartenenti ad una specie animale selvatica protetta è punito con l'arresto da uno a sei mesi o con l'ammenda fino a 4.000 euro, salvo i casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie. 2. Chiunque, fuori dai casi consentiti, distrugge, preleva o detiene esemplari appartenenti ad una specie vegetale selvatica protetta è punito con l'ammenda fino a 4.000 euro, salvo i casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie.*"

DISTRUZIONE O DETERIORAMENTO DI HABITAT ALL'INTERNO DI UN SITO PROTETTO (ART. 733-BIS C.P.)

"Chiunque, fuori dai casi consentiti, distrugge un habitat all'interno di un sito protetto o comunque lo deteriora compromettendone lo stato di conservazione, è punito con l'arresto fino a diciotto mesi e con l'ammenda non inferiore a 3.000 euro."

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. 137 D.LGS. 152/2006)

"1. Chiunque apra o comunque effettui nuovi scarichi di acque reflue industriali, senza autorizzazione, oppure continui ad effettuare o mantenere detti scarichi dopo che l'autorizzazione sia stata sospesa o revocata, è punito con l'arresto da due mesi a due anni o con l'ammenda da millecinquecento euro a diecimila euro. 2. Quando le condotte descritte al comma 1 riguardano gli scarichi di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del presente decreto, la pena è dell'arresto da tre mesi a tre anni. 3. Chiunque, al di fuori delle ipotesi di cui al comma 5, effettui uno scarico di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del presente decreto senza osservare le prescrizioni dell'autorizzazione, o le altre prescrizioni dell'autorità competente a

norma degli articoli 107, comma 1, e 108, comma 4, è punito con l'arresto fino a due anni. (omissis)5. Chiunque, in relazione alle sostanze indicate nella tabella 5 dell'Allegato 5 alla parte terza del presente decreto, nell'effettuazione di uno scarico di acque reflue industriali, superi i valori limite fissati nella tabella 3 o, nel caso di scarico sul suolo, nella tabella 4 dell'Allegato 5 alla parte terza del presente decreto, oppure i limiti più restrittivi fissati dalle regioni o dalle province autonome o dall'Autorità competente a norma dell'articolo 107, comma 1, è punito con l'arresto fino a due anni e con l'ammenda da tremila euro a trentamila euro. Se sono superati anche i valori limite fissati per le sostanze contenute nella tabella 3/A del medesimo Allegato 5, si applica l'arresto da sei mesi a tre anni e l'ammenda da seimila euro a centoventimila euro (430). 6. Le sanzioni di cui al comma 5 si applicano altresì al gestore di impianti di trattamento delle acque reflue urbane che nell'effettuazione dello scarico supera i valori-limite previsti dallo stesso comma. (omissis) 11. Chiunque non osservi i divieti di scarico previsti dagli articoli 103 e 104 è punito con l'arresto sino a tre anni. (omissis) 13. Si applica sempre la pena dell'arresto da due mesi a due anni se lo scarico nelle acque del mare da parte di navi od aeromobili contiene sostanze o materiali per i quali è imposto il divieto assoluto di sversamento ai sensi delle disposizioni contenute nelle convenzioni internazionali vigenti in materia e ratificate dall'Italia, salvo che siano in quantità tali da essere resi rapidamente innocui dai processi fisici, chimici e biologici, che si verificano naturalmente in mare e purché in presenza di preventiva autorizzazione da parte dell'autorità competente. (omissis)"

INQUINAMENTO DEL SUOLO, DEL SOTTOSUOLO, DELLE ACQUE SUPERFICIALI O DELLE ACQUE SOTTERRANEE (ART. 257 D.LGS. 152/2006)

"1. Chiunque cagiona l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio è punito con la pena dell'arresto da sei mesi a un anno o con l'ammenda da duemilaseicento euro a ventiseimila euro, se non provvede alla bonifica in conformità al progetto approvato dall'autorità competente nell'ambito del procedimento di cui agli

articoli 242 e seguenti. In caso di mancata effettuazione della comunicazione di cui all'articolo 242, il trasgressore è punito con la pena dell'arresto da tre mesi a un anno o con l'ammenda da mille euro a ventiseimila euro. 2. Si applica la pena dell'arresto da un anno a due anni e la pena dell'ammenda da cinquemiladuecento euro a cinquantaduemila euro se l'inquinamento è provocato da sostanze pericolose. 3. Nella sentenza di condanna per la contravvenzione di cui ai commi 1 e 2, o nella sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale, il beneficio della sospensione condizionale della pena può essere subordinato alla esecuzione degli interventi di emergenza, bonifica e ripristino ambientale. 4. L'osservanza dei progetti approvati ai sensi degli articoli 242 e seguenti costituisce condizione di non punibilità per i reati ambientali contemplati da altre leggi per il medesimo evento e per la stessa condotta di inquinamento di cui al comma 1."

TRAFFICO ILLECITO DI RIFIUTI (ART. 259 D.LGS. 152/2006)

"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 millecinquecentocinquanta euro a ventiseimila euro e con l'arresto fino a due anni. La pena è aumentata in caso di spedizione di rifiuti pericolosi. (omissis)"

ATTIVITÀ ORGANIZZATE PER IL TRAFFICO ILLECITO DI RIFIUTI (452-QUATERDECIES C.P.)

"1. Chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti è punito con la reclusione da uno a sei anni. 2. Se si tratta di rifiuti ad alta radioattività si applica la pena della reclusione da tre a otto anni. 3. Alla condanna conseguono le pene accessorie di cui agli articoli 28, 30, 32-bis e 32-ter del codice penale, con la limitazione di cui all'articolo 33 del medesimo codice. 4. Il giudice, con la sentenza di condanna o con quella emessa ai sensi dell'articolo 444 del codice di procedura

penale, ordina il ripristino dello stato dell'ambiente e può subordinare la concessione della sospensione condizionale della pena all'eliminazione del danno o del pericolo per l'ambiente; 4bis. E' sempre ordinata la confisca delle cose che servirono a commettere il reato o che costituiscono il prodotto o il profitto del reato, salvo che appartengano a persone estranee al reato. Quando essa non sia possibile, il giudice individua beni di valore equivalente di cui il condannato abbia anche indirettamente o per interposta persona la disponibilità e ne ordina la confisca."

SISTEMA INFORMATICO DI CONTROLLO DELLA TRACCIABILITÀ DEI RIFIUTI (ART. 260 – BIS D.LGS. 152/2006)

"(omissis) 6. Si applica la pena di cui all'articolo 483 c.p. a colui che, nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi inserisce un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti. 7. Il trasportatore che omette di accompagnare il trasporto dei rifiuti con la copia cartacea della scheda SISTRI - AREA MOVIMENTAZIONE e, ove necessario sulla base della normativa vigente, con la copia del certificato analitico che identifica le caratteristiche dei rifiuti è punito con la sanzione amministrativa pecuniaria da 1.600 euro a 9.300 euro. Si applica la pena di cui all'art. 483 del codice penale in caso di trasporto di rifiuti pericolosi. Tale ultima pena si applica anche a colui che, durante il trasporto fa uso di un certificato di analisi di rifiuti contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati. 8. Il trasportatore che accompagna il trasporto di rifiuti con una copia cartacea della scheda SISTRI - AREA Movimentazione fraudolentemente alterata è punito con la pena prevista dal combinato disposto degli articoli 477 e 482 del codice penale. La pena è aumentata fino ad un terzo nel caso di rifiuti pericolosi. (omissis)"

SANZIONI (ART. 279 D.LGS. 152/2006)

"*1. Chi inizia a installare o esercisce uno stabilimento in assenza della prescritta autorizzazione ovvero continua l'esercizio con l'autorizzazione scaduta, decaduta, sospesa o revocata è punito con la pena dell'arresto da due mesi a due anni o*

dell'ammenda da 258 euro a 1.032 euro. Con la stessa pena è punito chi sottopone uno stabilimento ad una modifica sostanziale senza l'autorizzazione prevista dall'articolo 269, comma 8. Chi sottopone uno stabilimento ad una modifica non sostanziale senza effettuare la comunicazione prevista dall'articolo 269, comma 8, è assoggettato ad una sanzione amministrativa pecuniaria pari a 1.000 euro, alla cui irrogazione provvede l'autorità competente. 2. Chi, nell'esercizio di uno stabilimento, viola i valori limite di emissione o le prescrizioni stabiliti dall'autorizzazione, dagli Allegati I,II, III o V alla parte quinta del presente decreto, dai piani e dai programmi o dalla normativa di cui all'articolo 271 o le prescrizioni altrimenti imposte dall'autorità competente ai sensi del presente titolo è punito con l'arresto fino ad un anno o con l'ammenda fino a 1.032 euro. Se i valori limite o le prescrizioni violati sono contenuti nell'autorizzazione integrata ambientale si applicano le sanzioni previste dalla normativa che disciplina tale autorizzazione.
3. Chi mette in esercizio un impianto o inizia ad esercitare un'attività senza averne dato la preventiva comunicazione prescritta ai sensi dell'articolo 269, comma 6, o ai sensi dell'articolo 272, comma 1, è punito con l'arresto fino ad un anno o con l'ammenda fino a milletrentadue euro. 4. Chi non comunica all'autorità competente i dati relativi alle emissioni ai sensi dell'articolo 269, comma 6, é punito con l'arresto fino a sei mesi o con l'ammenda fino a milletrentadue euro. 5. Nei casi previsti dal comma 2 si applica sempre la pena dell'arresto fino ad un anno se il superamento dei valori limite di emissione determina anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa. 6. Chi, nei casi previsti dall'articolo 281, comma 1, non adotta tutte le misure necessarie ad evitare un aumento anche temporaneo delle emissioni è punito con la pena dell'arresto fino ad un anno o dell'ammenda fino a milletrentadue euro. 7. Per la violazione delle prescrizioni dell'articolo 276, nel caso in cui la stessa non sia soggetta alle sanzioni previste dai commi da 1 a 6, e per la violazione delle prescrizioni dell'articolo 277 si applica una sanzione amministrativa pecuniaria da quindicimilaquattrocentonovantatre euro a centocinquantaquattromilanovecentotrentasette euro. All'irrogazione di tale sanzione

provvede, ai sensi degli articoli 17 e seguenti della legge 24 novembre 1981, n. 689, la regione o la diversa autorità indicata dalla legge regionale. La sospensione delle autorizzazioni in essere è sempre disposta in caso di recidiva."

ART. 1 LEGGE 7 FEBBRAIO 1992, N. 150 - TRAFFICO ESEMPLARI

"1. Salvo che il fatto costituisca più grave reato, è punito con l'arresto da tre mesi ad un anno e con l'ammenda da lire quindici milioni a lire centocinquanta milioni chiunque, in violazione di quanto previsto dal Regolamento (CE) n. 338/97 del Consiglio del 9 dicembre 1996, e successive attuazioni e modificazioni, per gli esemplari appartenenti alle specie elencate nell'allegato A del Regolamento medesimo e successive modificazioni: a) importa, esporta o riesporta esemplari, sotto qualsiasi regime doganale, senza il prescritto certificato o licenza, ovvero con certificato o licenza non validi ai sensi dell'articolo 11, comma 2a, del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni; b) omette di osservare le prescrizioni finalizzate all'incolumità degli esemplari, specificate in una licenza o in un certificato rilasciati in conformità al Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni e del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997, e successive modificazioni; c) utilizza i predetti esemplari in modo difforme dalle prescrizioni contenute nei provvedimenti autorizzativi o certificativi rilasciati unitamente alla licenza di importazione o certificati successivamente;
d) trasporta o fa transitare, anche per conto terzi, esemplari senza la licenza o il certificato prescritti, rilasciati in conformità del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni e del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997, e successive modificazioni e, nel caso di esportazione o riesportazione da un Paese terzo parte contraente della Convenzione di Washington, rilasciati in conformità della stessa, ovvero senza una prova sufficiente della loro esistenza; e) commercia piante riprodotte artificialmente in contrasto con le prescrizioni stabilite in base all'articolo 7, paragrafo 1, lettera b), del Regolamento (CE) n. 338/97 del Consiglio, del 9

dicembre 1996, e successive attuazioni e modificazioni e del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997 e successive modificazioni; f) detiene, utilizza per scopi di lucro, acquista, vende, espone o detiene per la vendita o per fini commerciali, offre in vendita o comunque cede esemplari senza la prescritta documentazione. 2. In caso di recidiva, si applica la sanzione dell'arresto da tre mesi a due anni e dell'ammenda da lire venti milioni a lire duecento milioni. Qualora il reato suddetto viene commesso nell'esercizio di attività di impresa, alla condanna consegue la sospensione della licenza da un minimo di sei mesi ad un massimo di diciotto mesi. (omissis)"

ART. 2 LEGGE 7 FEBBRAIO 1992, N. 150 – TRAFFICO ESEMPLARI

"1. Salvo che il fatto costituisca più grave reato, è punito con l'ammenda da lire venti milioni a lire duecento milioni o con l'arresto da tre mesi ad un anno, chiunque, in violazione di quanto previsto dal Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni, per gli esemplari appartenenti alle specie elencate negli allegati B e C del Regolamento medesimo e successive modificazioni:

a) importa, esporta o riesporta esemplari, sotto qualsiasi regime doganale, senza il prescritto certificato o licenza, ovvero con certificato o licenza non validi ai sensi dell'articolo 11, comma 2a, del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni;

b) omette di osservare le prescrizioni finalizzate all'incolumità degli esemplari, specificate in una licenza o in un certificato rilasciati in conformità al Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni, e del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997, e successive modificazioni;

c) utilizza i predetti esemplari in modo difforme dalle prescrizioni contenute nei provvedimenti autorizzativi o certificativi rilasciati unitamente alla licenza di importazione o certificati successivamente;

d) trasporta o fa transitare, anche per conto terzi, esemplari senza licenza o il certificato prescritti, rilasciati in conformità del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni, e del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997, e successive modificazioni e, nel caso di esportazione o riesportazione da un Paese terzo parte contraente della Convenzione di Washington, rilasciati in conformità della stessa, ovvero senza una prova sufficiente della loro esistenza;

e) commercia piante riprodotte artificialmente in contrasto con le prescrizioni stabilite in base all'articolo 7, paragrafo 1, lettera b), del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni, e del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997, e successive modificazioni;

f) detiene, utilizza per scopi di lucro, acquista, vende, espone o detiene per la vendita o per fini commerciali, offre in vendita o comunque cede esemplari senza la prescritta documentazione, limitatamente alle specie di cui all'allegato B del Regolamento.

2. In caso di recidiva, si applica la sanzione dell'arresto da tre mesi a un anno e dell'ammenda da lire venti milioni a lire duecento milioni. Qualora il reato suddetto viene commesso nell'esercizio di attività di impresa, alla condanna consegue la sospensione della licenza da un minimo di quattro mesi ad un massimo di dodici mesi. 3. L'introduzione nel territorio nazionale, l'esportazione o la riesportazione dallo stesso di oggetti personali o domestici relativi a specie indicate nel comma 1, in violazione delle disposizioni del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997, e successive modificazioni, è punita con la sanzione amministrativa da lire due milioni a lire dodici milioni. Gli oggetti introdotti illegalmente sono confiscati dal Corpo forestale dello Stato, ove la confisca non sia disposta dall'Autorità giudiziaria. 4. Salvo che il fatto costituisca reato, chiunque omette di presentare la notifica di importazione, di cui all'articolo 4, paragrafo 4, del Regolamento (CE) n. 338/97, del Consiglio, del 9 dicembre 1996, e successive

attuazioni e modificazioni, ovvero il richiedente che omette di comunicare ilrigetto di una domanda di licenza o di certificato in conformità dell'articolo 6, paragrafo 3, del citato Regolamento, è punito con la sanzione amministrativa da lire due milioni a lire dodici milioni. 5. L'autorità amministrativa che riceve il rapporto previsto dall'articolo 17, primo comma, della legge 24 novembre 1981, n. 689, per le violazioni previste e punite dalla presente legge, è il servizio CITES del Corpo forestale dello Stato."

ART. 6 LEGGE 7 FEBBRAIO 1992, N. 150 – ANIMALI PERICOLOSI

"*1. Fatto salvo quanto previsto dalla legge 11 febbraio 1992, n. 157, è vietato a chiunque detenere esemplari vivi di mammiferi e rettili di specie selvatica ed esemplari vivi di mammiferi e rettili provenienti da riproduzioni in cattività che costituiscano pericolo per la salute e per l'incolumità pubblica. (omissis)4. Chiunque contravviene alle disposizioni di cui al comma 1 è punito con l'arresto fino a tre mesi o con l'ammenda da lire quindici milioni a lire duecento milioni. (omissis)"*

ART.3- BIS LEGGE 7 FEBBRAIO 1992, N. 150

"*1. Alle fattispecie previste dall'articolo 16, paragrafo 1, lettere a), c), d), e), ed l), del Regolamento (CE) n. 338/97 del Consiglio del 9 dicembre 1996, e successive modificazioni, in materia di falsificazione o alterazione di certificati, licenze, notifiche di importazione, dichiarazioni, comunicazioni di informazioni al fine di acquisizione di una licenza o di un certificato, di uso di certificati o licenze falsi o alterati si applicano le pene di cui al libro II, titolo VII, capo III del codice penale.*

2. In caso di violazione delle norme del decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, le stesse concorrono con quelle di cui agli articoli 1, 2 e del presente articolo."

CESSAZIONE E RIDUZIONE DELL'IMPIEGO DELLE SOSTANZE LESIVE (ART. 3, COMMA 6, LEGGE 28 DICEMBRE 1993, N. 549)

"*1. La produzione, il consumo, l'importazione, l'esportazione, la detenzione e la commercializzazione delle sostanze lesive di cui alla tabella A allegata alla presente legge sono regolati dalle disposizioni di cui al regolamento (CE) n. 3093/94.*

2. A decorrere dalla data di entrata in vigore della presente legge è vietata l'autorizzazione di impianti che prevedano l'utilizzazione delle sostanze di cui alla

tabella A allegata alla presente legge, fatto salvo quanto disposto dal regolamento (CE) n. 3093/94.

3. Con decreto del Ministro dell'ambiente, di concerto con il Ministro dell'industria, del commercio e dell'artigianato, sono stabiliti, in conformità alle disposizioni ed ai tempi del programma di eliminazione progressiva di cui al regolamento (CE) n. 3093/94, la data fino alla quale è consentito l'utilizzo di sostanze di cui alla tabella A, allegata alla presente legge, per la manutenzione e la ricarica di apparecchi e di impianti già venduti ed installati alla data di entrata in vigore della presente legge, ed i tempi e le modalità per la cessazione dell'utilizzazione delle sostanze di cui alla tabella B, allegata alla presente legge, e sono altresì individuati gli usi essenziali delle sostanze di cui alla tabella B, relativamente ai quali possono essere concesse deroghe a quanto previsto dal presente comma. La produzione, l'utilizzazione, la commercializzazione, l'importazione e l'esportazione delle sostanze di cui alle tabelle A e B allegate alla presente legge cessano il 31 dicembre 2008, fatte salve le sostanze, le lavorazioni e le produzioni non comprese nel campo di applicazione del regolamento (CE) n. 3093/94, secondo le definizioni ivi previste.

4. L'adozione di termini diversi da quelli di cui al comma 3, derivati dalla revisione in atto del regolamento (CE) n. 3093/94, comporta la sostituzione dei termini indicati nella presente legge ed il contestuale adeguamento ai nuovi termini.

5. Le imprese che intendono cessare la produzione e l'utilizzazione delle sostanze di cui alla tabella B, allegata alla presente legge, prima dei termini prescritti possono concludere appositi accordi di programma con i Ministeri dell'industria, del commercio e dell'artigianato e dell'ambiente, al fine di usufruire degli incentivi di cui all'articolo 10, con priorità correlata all'anticipo dei tempi di dismissione, secondo le modalità che saranno fissate con decreto del Ministro dell'industria, del commercio e dell'artigianato, d'intesa con il Ministro dell'ambiente.

6. Chiunque viola le disposizioni di cui al presente articolo è punito con l'arresto fino a due anni e con l'ammenda fino al triplo del valore delle sostanze utilizzate per fini produttivi, importate o commercializzate. Nei casi più gravi, alla condanna consegue

la revoca dell'autorizzazione o della licenza in base alla quale viene svolta l'attività constituente illecito."

DISASTRO AMBIENTALE (ART. 452-QUATER DEL CODICE PENALE)

"*Fuori dai casi previsti dall'articolo 434, chiunque abusivamente cagiona un disastro ambientale è punito con la reclusione da cinque a quindici anni. Costituiscono disastro ambientale alternativamente:*

1) l'alterazione irreversibile dell'equilibrio di un ecosistema;

2) l'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali;

3) l'offesa alla pubblica incolumità in ragione della rilevanza del fatto per l'estensione della compromissione o dei suoi effetti lesivi ovvero per il numero delle persone offese o esposte a pericolo.

Quando il disastro è prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette, la pena è aumentata."

Commette tale reato (delitto) chiunque, fuori dai casi previsti dall'articolo 434 c.p., abusivamente cagiona un disastro ambientale. Costituiscono disastro ambientale alternativamente: **1)** l'alterazione irreversibile dell'equilibrio di un ecosistema; **2)** l'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali; **3)** l'offesa alla pubblica incolumità in ragione della rilevanza del fatto per l'estensione della compromissione o dei suoi effetti lesivi ovvero per il numero delle persone offese o esposte a pericolo.

La sanzione pecuniaria per l'azienda va da 400 a 800 quote.

E' prevista espressamente l'applicazione delle sanzioni interdittive elencate nell'art. 9 del D.Lgs.231/01 per l'azienda.

DELITTI ASSOCIATIVI AGGRAVATI (ART.452-OCTIES DEL CODICE PENALE)

La sanzione pecuniaria per l'azienda va da 300 a 1000 quote.

TRAFFICO E ABBANDONO DI MATERIALE AD ALTA RADIOATTIVITÀ (ART.452-SEXIES DEL CODICE PENALE)

"*Salvo che il fatto costituisca più grave reato, è punito con la reclusione da due a sei anni e con la multa da euro 10.000 a euro 50.000 chiunque abusivamente cede, acquista, riceve, trasporta, importa, esporta, procura ad altri, detiene, trasferisce, abbandona o si disfa illegittimamente di materiale ad alta radioattività.*

La pena di cui al primo comma è aumentata se dal fatto deriva il pericolo di compromissione o deterioramento:

1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo;

2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna.

Se dal fatto deriva pericolo per la vita o per l'incolumità delle persone, la pena è aumentata fino alla metà."

Il reato punisce chiunque abusivamente cede, acquista, riceve, trasporta, importa, esporta, procura ad altri, detiene, trasferisce, abbandona o si disfa illegittimamente di materiale ad alta radioattività. La norma prevede alcune fattispecie aggravate.

La sanzione pecuniaria per l'azienda va da 250 a 600 quote.

2 ACRONIMI AZIENDALI

AU	Amministratore Unico
RSPP	Responsabile del Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC/RPROG	Responsabile Tecnico/Responsabile Progettazione
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RPROG	Responsabile Progettazione
RATTR	Responsabile Attrezzature e Mezzi

PER L'IDENTIFICAZIONE DEI SOGGETTI CHE CORRISPONDONO AGLI ACRONIMI AZIENDALI SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI GETOPEN S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di GETOPEN S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di GETOPEN S.r.l.

4 CAMPO DI APPLICAZIONE RESPONSABILE DELLA PROCEDURA

La presente procedura si applica a tutti coloro i quali agiscono in nome e per conto della Società e la cui attività possa comportare la commissione dei reati di cui all'art. 25-undecies.

Le disposizioni della presente Parte Speciale hanno per Destinatari tutti i soggetti coinvolti nei processi sopra identificati, affinché gli stessi adottino regole di condotta conformi a quanto prescritto al fine di prevenire il verificarsi dei delitti ivi considerati.

NELLO SPECIFICO LA PRESENTE PARTE SPECIALE HA LO SCOPO DI:

a) indicare i principi che i destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo di Vigilanza, ed ai Responsabili delle funzioni aziendali che con lo stesso cooperano, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

Il principale responsabile della presente procedura è all'Amministratore Unico.

5 PRINCIPI GENERALI DI COMPORTAMENTO

Al fine di prevenire i reati sopra enunciati, tutti i destinatari devono rispettare, oltre i principi di comportamento già previsti ed espressi nel Codice Etico, anche quelli riportati nei documenti organizzativi adottati dalla Società, nonché tenere comportamenti conformi a quanto previsto dalle vigenti norme di legge. Inoltre, i Destinatari del Modello, competenti per le attività oggetto di regolamentazione della presente Parte speciale, sono tenuti ad osservare i seguenti ulteriori principi:

- assicurare il regolare funzionamento delle attività di competenza;

- garantire l'attuazione del principio di segregazione dei compiti e delle funzioni anche attraverso la predisposizione di specifiche procedure;
- garantire la tracciabilità e la documentabilità di tutte le operazioni effettuate, prevedendo specifici obblighi di archiviazione;
- garantire che le attività a rischio prevedano i necessari controlli gerarchici, che devono essere tracciati/documentati;
- garantire la piena collaborazione alle Finzioni Aziendali all'uopo preposte al controllo, oltre che nell'ambito di eventuali indagini/accertamenti da parte di organi esterni;
- garantire la corretta applicazione del Sistema disciplinare, in caso di mancato rispetto dei principi e dei protocolli contenuti nel Modello;
- assicurare la corretta raccolta e il corretto smaltimento dei rifiuti;
- segnalare tempestivamente al DL e all'OdV eventuali criticità riscontrate;
- assicurare il corretto aggiornamento del DVR.

6 LEGGE N. 137/2023 – LA TUTELA PENALE DELL'AMBIENTE

La Legge n. 137/2023 che ha convertito in legge, con modificazioni, il D.L. 10 agosto 2023 n. 105 (cd. Decreto Giustizia) ha previsto la trasformazione da illecito amministrativo a reato contravvenzionale della fattispecie di abbandono di rifiuti di cui all'art. 255 D.Lgs. n. 152/2006.

La norma punisce con l'ammenda da 1.000 a 10.000 euro – fatto salvo quanto disposto dall'art. 256, comma 2, in materia di responsabilità penale per abbandono di rifiuti dei responsabili di enti o imprese – chiunque abbandoni o depositi rifiuti ovvero li immetta nelle acque superficiali o sotterranee in violazione degli artt. 192, commi 1 e 2 (che vietano l'abbandono e il deposito incontrollati di rifiuti sul suolo e nel suolo e l'immissione di rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali e sotterranee), 226 comma 2 (che vieta l'immissione di imballaggi terziari nel normale circuito di raccolta dei rifiuti urbani), e 231, commi 1 e 2 (in materia di demolizione di veicoli fuori uso), del cd. Codice dell'Ambiente.

La pena è aumentata fino al doppio se l'abbandono riguarda rifiuti pericolosi.
Il legislatore è intervenuto, inoltre, sulle disposizioni in materia di confisca di cui all'art. 240-bis c.p., estendendo il catalogo dei reati per i quali è prevista, in caso di condanna o patteggiamento, la confisca del denaro o dei beni di cui il condannato abbia la disponibilità in valore sproporzionato rispetto al proprio reddito e di cui non possa giustificare la provenienza (cd. confisca allargata).
In particolare, viene estesa la confisca, già prevista per i delitti di disastro ambientale (art. 452-quater c.p.) e di associazione a delinquere finalizzata alla commissione di delitti contro l'ambiente (art. 452-octies, primo comma, c.p.), anche alle seguenti fattispecie:

- l'inquinamento ambientale (art. 452-bis c.p.);
- la morte o lesioni come conseguenza del delitto di inquinamento ambientale (art. 452-ter c.p.);
- il traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.);
- le attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.).

7 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO

I *Destinatari* devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposto su apposita piattaforma informatica – tutta la documentazione necessaria.
Conclusa l'ispezione, l'AU, o il responsabile della Funzione aziendale interessata, all'uopo incaricata, dovrà inviare una relazione riepilogativa all'OdV.
In ogni caso, il Responsabile della procedura informa, tempestivamente, l'Organismo di Vigilanza sulle ispezioni della Pubblica Amministrazione e sugli adempimenti richiesti alla Società.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse ai Processi Sensibili, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di *corporate governance* per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 20.03.2024	ADOZIONE
Rev. 1	Determina dell'Amministratore Unico del 05.08.2024	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231)

PARTE SPECIALE -10-

SOMMARIO

1 OBIETTIVI E FUNZIONE DEL MODELLO

La legge n. 123 del 3 agosto 2007 ha dettato nuove misure in materia di tutela della salute e della sicurezza sui luoghi di lavoro e ha conferito al Governo delega per il riassetto e la riforma della normativa in materia.

Tra le principali novità è intervenuta la modifica del D. Lgs. n. 231/2001 ai sensi dell'articolo 9 della citata Legge 123 relativamente all'estensione della responsabilità amministrativa degli enti per gli illeciti commessi con la violazione di norme di sicurezza e antinfortunistiche. Dopo l'articolo 25 sexies il Legislatore ha infatti ritenuto di inserire l'articolo 25 septies che fa riferimento ai reati di cui agli artt. 589 c.p. (omicidio colposo) e 590 terzo comma c.p. (lesioni personali colpose gravi o gravissime), commessi con la violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di GETOPEN i seguenti reati:

• **OMICIDIO COLPOSO (ART. 589 C.P.)**

La condotta punita dalla presente fattispecie di reato si concretizza in quei comportamenti che, violando le norme dettate ai fini della prevenzione degli infortuni sul lavoro e della tutela dell'igiene e della salute sui luoghi di lavoro, cagionano il decesso di una persona.

• **LESIONI PERSONALI COLPOSE GRAVI O GRAVISSIME (ART. 590 C.P.)**

Il reato si configura nel caso in cui per colpa si cagionino ad una persona lesioni gravi o gravissime, a seguito della violazione delle norme per la prevenzione degli infortuni sul lavoro. Le lesioni si considerano gravi nel caso in cui: **a)** dal fatto deriva 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 quaranta giorni; **b)** il fatto produce l'indebolimento permanente di un senso o di un organo (art. 583, comma 1, c.p.).

Ai fini della integrazione dei suddetti reati, non è richiesto l'elemento soggettivo del dolo, ovvero la coscienza e la volontà di cagionare l'evento lesivo, ma la mera negligenza, impudenza o imperizia del soggetto agente, ovvero l'inosservanza da parte di quest'ultimo di leggi, regolamenti, ordini o discipline (art. 43 c.p.).

Il presente protocollo, uniformemente e ad integrazione del sistema di sicurezza sul lavoro adottato da GETOPEN S.r.l., individua una serie di procedure, in conformità all'art. 30 D.lgs 81/2008 e decreto del 13 febbraio 2014 emanato dal Ministero del Lavoro e Politiche Sociali, atte a verificare e controllare la corretta applicazione degli adempimenti previsti dalla vigente legislazione nazionale in materia di tutela della salute e della sicurezza negli ambienti di lavoro.

Le prescrizioni della presente procedura integrano, altresì, i principi di comportamento contenuti nel Modello e nel Codice Etico di GETOPEN.

Il presente protocollo ha lo scopo di fornire all'OdV e alle Funzioni Aziendali che con lo stesso cooperano, gli strumenti per esercitare le attività di controllo, monitoraggio e verifica previste in materia di tutela della salute e della sicurezza negli ambienti di lavoro.

In particolare, il Datore di Lavoro, i delegati *ex* art. 16 D. Lgs. 81/2008 (ove presenti) nonché tutti i soggetti aventi compiti e responsabilità nella gestione degli adempimenti previsti delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, quali, a titolo esemplificativo, Responsabile del Servizio di Prevenzione e Protezione (RSPP), Preposti, Medico Competente - così come individuati dalla Società coerentemente alle previsioni della vigente legislazione - devono garantire, ognuno nell'ambito di propria competenza:

- l'applicazione degli obiettivi per la sicurezza e la salute dei lavoratori, l'identificazione continua dei rischi nonché la predisposizione delle misure di prevenzione e protezione conseguenti;
- il rispetto degli *standard* tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici, anche attraverso un processo continuo di aggiornamento sullo stato dell'arte degli *standard* e la

manutenzione ordinaria e straordinaria degli impianti, delle attrezzature di lavoro e, in generale, delle strutture aziendali;

- un adeguato livello di informazione/formazione dei lavoratori, così come definiti dal D.lgs. 81/2008 ss.mm.ii., sulla gestione delle attività in materia di sicurezza e salute della Società e sulle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole di comportamento e controllo definite dalla Società. In particolare, ciascun lavoratore dovrà ricevere formazione sufficiente ed adeguata con particolare riferimento al proprio posto di lavoro ed alle proprie mansioni. La suddetta formazione deve essere fatta in occasione dell'assunzione, del trasferimento o cambiamento di mansioni o dell'introduzione di nuove attrezzature di lavoro o di nuove tecnologie, di nuove sostanze e preparati pericolosi;
- la definizione e l'aggiornamento (in base ai cambiamenti nella struttura organizzativa ed operativa dalla Società nonché l'evolversi del panorama normativo) di procedure specifiche per la prevenzione di infortuni e malattie, in cui siano, tra l'altro, disciplinate le modalità di gestione degli incidenti e delle emergenze;
- l'idoneità delle risorse umane – in termini di numero e qualifiche professionali, formazione – e materiali, necessarie al raggiungimento degli obiettivi prefissati dalla Società per la sicurezza e la salute dei lavoratori.

I lavoratori devono comunicare tempestivamente, alle funzioni individuate e con le modalità definite nelle procedure operative, situazioni di pericolo, quasi infortuni, infortuni (indipendentemente dalla loro gravità) e violazioni alle regole di comportamento e alle procedure operative.

2 ACRONIMI AZIENDALI

DL	Datore di Lavoro
AU	Amministratore Unico
RSPP	Responsabile del Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità

RTEC/RPROG Responsabile Tecnico/Responsabile Progettazione
MC Medico Competente
RAM Responsabile Amministrazione - Risorse Umane
RCOM/APVG Responsabile Commerciale - Approvvigionamento
RATTR Responsabile Attrezzature
RLS Rappresentante Lavoratori per la Sicurezza

PER L'IDENTIFICAZIONE DEI SOGGETTI CHE CORRISPONDONO AGLI ACRONIMI AZIENDALI SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI GETOPEN S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di GETOPEN S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di GETOPEN S.r.l..

4 CAMPO DI APPLICAZIONE E RESPONSABILE DEL MODELLO

Le norme antinfortunistiche e di tutela dell'igiene e della salute sul lavoro hanno come destinatari alcuni specifici soggetti e cioè il datore di lavoro, i preposti ed i lavoratori; alcune specifiche disposizioni riguardano il responsabile del servizio di prevenzione e protezione ed il rappresentante per la sicurezza.
I reati di omicidio e di lesioni colpose commessi in violazione delle norme antinfortunistiche e di tutela dell'igiene e della salute sul lavoro interessano, a diverso titolo secondo le attribuzioni, i compiti e/o le responsabilità assegnate, principalmente i soggetti in questione.
Con riferimento ai reati ex art. 25 septies, i processi sensibili ritenuti teoricamente a rischio, in ambito GETOPEN riguardano proprio la gestione degli adempimenti in materia di salute e sicurezza dei luoghi di lavoro.
A tal fine è stato predisposto il documento di valutazione dei rischi che ha analizzato ogni ipotetico rischio che i lavoratori potrebbero dover affrontare; tale documento deve essere soggetto a modifiche, qualora le esperienze maturate

suggeriscano la necessità di implementare il livello di sicurezza in ambito aziendale.

E' stato inoltre predisposto un organigramma societario con il quale sono stati definiti i ruoli secondo una struttura gerarchica.

GETOPEN si adopera al fine di promuovere l'attività di informazione e formazione dei lavoratori che viene svolta puntualmente per dare attuazione, nel modo più ampio e completo possibile, al rispetto della legislazione in materia di salute e sicurezza sul lavoro; viene prestata, inoltre, particolare attenzione affinché ogni lavoratore sia provvisto ed utilizzi i dispositivi di protezione individuale previsti dalla legislazione.

Il presente protocollo si applica a tutte le Funzioni Aziendali che operano per GETOPEN, a tutti coloro che, esterni alla Società, intrattengano rapporti contrattuali con la stessa, nonché a tutti i terzi che accedono, a qualsiasi titolo, nei luoghi di lavoro in cui la Società svolge la propria attività.

I responsabili del sistema sicurezza sopra indicati devono essere valutati in base alle competenze, al titolo di studio e alle precedenti esperienze lavorative. Le verifiche devono essere effettuate attraverso l'acquisizione dei *curricula*.

5 AREA SENSIBILE CONCERNENTE I REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO

L'art. 25 septies del Decreto prevede tra gli illeciti presupposto della responsabilità degli Enti i delitti di omicidio colposo e di lesioni colpose gravi o gravissime, se commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Il Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro, (D. Lgs. 9 aprile 2008 n. 81) che ha profondamente riordinato le molteplici fonti normative previgenti in materia, ha previsto all'art. 30 le caratteristiche che deve presentare il Modello di organizzazione, gestione e controllo al fine della prevenzione dei reati in esame.

Finalità delle citate disposizioni è quella di fornire più efficaci mezzi di prevenzione e repressione in relazione alla recrudescenza del fenomeno degli incidenti sul lavoro ed alla esigenza di tutela dell'integrità psicofisica dei lavoratori e della sicurezza degli ambienti lavorativi.

Viene riportato, di seguito, il testo delle disposizioni del Codice Penale espressamente richiamate dall'art. 25-septies del D.lgs 231/01, unitamente ad un breve commento delle singole fattispecie.

OMICIDIO COLPOSO (ART. 589 C.P.)

"*Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni. Se il fatto è commesso con violazione delle norme sulla disc iplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul la voro la pena è della reclusione da due a sette anni. Si applica la pena della reclusio ne da tre a dieci anni se il fatto è commesso con violazione delle norme sulla discipli na della circolazione stradale da:1.soggetto in stato di ebbrezza alcolica ai sensi de ll'articolo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285, e s uccessive modificazioni; 2.soggetto sotto l'effetto di sostanze stupefacenti o psicotro pe. Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesio ni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la penanon può superare gli anni quindici*".

Il reato si configura nel caso in cui si cagioni la morte di una persona.

Ai fini dell'integrazione del reato, non è richiesto l'elemento soggettivo del dolo, ov vero la coscienza e la volontà di cagionare l'evento lesivo, ma la mera negligenza, i mprudenza o imperizia del soggetto agente, ovvero l'inosservanza, da parte di que st'ultimo di leggi, regolamenti, ordini o discipline (art. 43 c.p.). Il secondo comma dell'articolo 589 prevede come specifica aggravante del delitto di omicidio colposo la violazione delle norme per la prevenzione degli infortuni sul lavoro. Con riferimento a tale particolare negligenza, la giurisprudenza ha precisato che, sotto il profilo della colpa, l'aggravante in questione sussiste non solo quando sia

contestata la violazione di specifiche norme per la prevenzione degli infortuni sul lavoro (la cosiddetta negligenza specifica) ma anche quando la contestazione abbia ad oggetto l'omissione dell'adozione di misure ed accorgimenti per la più efficace tutela della integrità fisica dei lavoratori, in violazione dell'articolo 2087 del Codice Civile.

Questa norma, infatti, lungi dall'avere valore astratto ed ammonitivo (come pure sostenuto), prevede un preciso obbligo dell'imprenditore diretto ad eliminare nell'esercizio dell'impresa, ogni situazione di pericolo dalla quale possa verificarsi un evento dannoso; anche la violazione di questo obbligo, dunque, rientra tra le violazioni di norme antinfortunistiche di cui al secondo comma dell'articolo 589 c.p. e, quindi, costituiscono comportamento colposo ai fini della punibilità per l'eventuale morte del dipendente.

La responsabilità del datore di lavoro è esclusa solo in caso di comportamento abnorme dei lavoratori, per tale intendendosi l'imprudenza realizzata al di fuori delle sue mansioni dunque della prevedibilità da parte dei datori di lavoro, ma anche quella che, pur rientrando nelle mansioni affidategli, si traduca in un comportamento ontologicamente lontano dalle prevedibili imprudenze del lavoratore nell'esecuzione del lavoro.

LESIONI PERSONALI COLPOSE (ART. 590 C.P.)

"*Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusion e fino a tre mesi o con la multa fino a euro 309,00.*

Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da e uro 123,00 a euro 619,00, se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309,00 a euro 1.239,00.

Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla d isciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della m ulta da euro 500,00 a euro 2.000,00 e la pena per le lesioni gravissime è della reclu sione da uno a tre anni. Nei casi di violazione delle norme sulla circolazione stradal

e, se il fatto è commesso da soggetto in stato di ebbrezza alcolica ai sensi dell'artico lo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285, e successi ve modificazioni, ovvero da soggetto sotto l'effetto di sostanze stupefacenti o psicotr ope, la pena per le lesioni gravi è della reclusione da sei mesi a due anni e la pena per le lesioni gravissime è della reclusione da un anno e sei mesi a quattro anni. Ne l caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusio ne non può superare gli anni cinque.

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

LA LESIONE È CONSIDERATA GRAVE (ART. 583 C.P., C. 1) NEI SEGUENTI CASI:

1.se dal fatto deriva 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 quaranta giorni;

2.se il fatto produce l'indebolimento permanente di un senso o di un organo.

LA LESIONE È CONSIDERATA INVECE GRAVISSIMA SE DAL FATTO DERIVA (ART. 583 C.P., C. 2):

1.una malattia certamente o probabilmente insanabile;

2.la perdita di un senso;

3.la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;

4. la deformazione, ovvero lo sfregio permanente del viso.

Il reato potrebbe astrattamente realizzarsi, ad esempio, qualora si cagionino lesioni, gravi o gravissime, ad un lavoratore, conseguenti ad una violazione delle norme in materia di salute e sicurezza sul lavoro, finalizzata, ad esempio, ad un risparmio economico o di tempi da parte della Società.

L'evento dannoso, sia esso rappresentato dalla lesione grave o gravissima o dalla morte, può essere perpetrato tramite un comportamento attivo (l'agente pone in

essere una condotta con cui lede l'integrità di un altro individuo), ovvero mediante una condotta omissiva (l'agente semplicemente non interviene a impedire l'evento dannoso). Di norma, si ravvisa una condotta attiva nel dipendente che svolge direttamente mansioni operative e che materialmente danneggia altri, mentre la condotta omissiva è usualmente ravvisabile nel personale apicale che non ottempera agli obblighi di vigilanza e controllo e in tal modo non interviene ad impedire l'evento da altri causato. L'elemento comune ad entrambe le fattispecie di reato (omicidio colposo, lesioni personali, colpose gravi o gravissime) è la colpa, come definita dall'art. 43 del c.p.. A tale riguardo, si rammenta che un delitto è da configurarsi come colposo, o contro l'intenzione, quando l'evento, anche se preveduto, non è voluto dall'agente e si verifica a causa di negligenza o imprudenza o imperizia (c.d. colpa generica), ovvero per inosservanza di leggi, regolamenti, ordini o discipline (c.d. colpa specifica).

È proprio in tema di omicidio e lesioni colpose che si sviluppa il principale banco di prova delle varie teorie che si prospettano sulla causalità nei reati omissivi (ovvero nei reati che si commettono con una colpevole inerzia).

È noto che nei reati omissivi per accertare il nesso di causalità tra omissione ed evento dannoso non ci si basa su un accertamento di fatto, come avviene per i reati di azione, bensì solo su un giudizio ipotetico cosiddetta prognosi postuma, ricostruendo mentalmente sia pure sulla base delle regole oggettive della scienza e della tecnica, cosa sarebbe successo là dove fosse stata compiuta l'azione doverosa mancante. Orbene, il risultato di tale giudizio ipotetico può portare, in caso di risposta affermativa, a tre diverse conclusioni:

- la certezza del mancato verificarsi dell'evento dannoso;
- la probabilità del mancato verificarsi dell'evento dannoso;
- la possibilità del mancato verificarsi dell'evento dannoso.

Entrambi i reati richiamati rilevano, ai fini del Decreto, unicamente nel caso in cui sia ascrivibile al soggetto agente, sotto il profilo dell'elemento soggettivo, la c.d. "colpa specifica", consistente nella violazione delle norme in materia di salute e sicurezza sul lavoro. Le norme in materia di salute e sicurezza sul lavoro

individuano nel Datore di Lavoro il garante "dell'integrità fisica e della personalità morale dei prestatori di lavoro" e la sua posizione di garanzia è comunque trasferibile ad altri soggetti, a patto che la relativa delega di poteri all'interno dell'organizzazione aziendale sia sufficientemente specifica, predisposta mediante atto scritto e idonea a trasferire tutti i poteri autoritativi e decisori necessari per tutelare l'incolumità dei dipendenti. Il prescelto a ricoprire l'incarico deve essere persona capace e competente per la materia oggetto del trasferimento di responsabilità. Questo tipo di delega comporta anche una procura notarile, che estrinseca nei confronti anche dei terzi i poteri conferiti al soggetto.

In base alla normativa introdotta dal legislatore in materia di responsabilità amministrativa d'impresa, la condotta lesiva dell'agente deve essere necessariamente aggravata, ossia conseguire alla violazione di norme concernenti la tutela della salute e sicurezza sul lavoro.

AI FINI DELL'IMPLEMENTAZIONE DEL MODELLO È NECESSARIO COMUNQUE CONSIDERARE CHE:

- il rispetto degli standard minimi di sicurezza previsti dalla normativa specifica di settore non esaurisce l'obbligo di diligenza complessivamente richiesto (aspetto relativo alla colpa specifica);
- è necessario garantire l'adozione di standard di sicurezza tali da minimizzare (e, se possibile, eliminare) ogni rischio di infortunio e malattia, anche in base dalla miglior tecnica e scienza conosciuta, secondo le particolarità del lavoro (aspetto relativo alla colpa generica);
- non esclude le responsabilità in capo all'Ente il comportamento del lavoratore infortunato che abbia dato occasione all'evento perché non ha adottato cautele che, se adottate, avrebbero neutralizzato il rischio; l'obbligo di prevenzione è escluso solo in presenza di comportamenti del dipendente che presentino il carattere dell'eccezionalità, dell'abnormità, dell'esorbitanza rispetto al procedimento lavorativo, del mancato rispetto delle direttive organizzative ricevute e alla comune prudenza.

Sotto il profilo dei soggetti tutelati, le norme in materia di salute e sicurezza sul lavoro non tutelano solo i dipendenti, ma tutte le persone che legittimamente si introducono nei locali adibiti allo svolgimento della prestazione lavorativa.
Per quanto concerne i soggetti attivi, possono commettere queste tipologie di reato coloro che, in ragione della loro mansione, svolgano attività sensibili in materia.

AD ESEMPIO:

- il lavoratore che, attraverso le proprie azioni e/o omissioni, può pregiudicare la propria ed altrui salute e sicurezza;
- l'Amministratore Unico e il Preposto, ai quali possono competere, tra gli altri, i compiti di coordinamento e supervisione delle attività, di formazione e di informazione;
- il Datore di Lavoro quale principale attore nell'ambito della prevenzione e protezione.

Assumendo specifica rilevanza la legislazione prevenzionistica vigente, ai fini della presente Parte Speciale è stata considerata, in particolare, la normativa di cui al D.lgs n. 81/2008 e successive modifiche, in attuazione della delega di cui all'art. 1 L. n. 123/2007 (c.d. "Testo Unico" in materia di salute e sicurezza sul lavoro, di seguito, anche "TU").

6 LE SANZIONI PREVISTE IN RELAZIONE ALL'ART. 25-SEPTIES DEL D.LGS 231/2001

Si riporta di seguito una tabella riepilogativa delle sanzioni previste con riferimento ai reati contemplati dall'art. 25-septies del D.lgs n. 231/01 a carico della Società qualora, per effetto della commissione dei reati indicati al precedente paragrafo da parte dei Soggetti Apicali e/o dei Soggetti Sottoposti, derivi allo stesso Ente un interesse o un vantaggio.

Reato	Sanzione Pecuniaria	Sanzione Interdittiva
omicidio colposo (art. 589 c.p.)	1.000 quote (nel caso in cui il delitto sia commesso con violazione dell'articolo 55, comma 2, del Decreto legislativo attuativo della delega di	Sanzioni interdittive di cui all'articolo 9, comma 2 del D.lgs 231/01 (interdizione dall'esercizio

	cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro)	dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi), per una durata non inferiore a tre mesi e non superiore ad un anno (nel caso di condanna per la commissione del delitto con violazione dell'articolo 55, comma 2, del Decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro). In caso di condanna di cui all'articolo 9, comma 2, del D.lgs 231/01 per una durata non inferiore a tre mesi e non superiore ad un anno (negli altri casi).
lesioni personali colpose (art. 590 c.p.)	fino a 250 quote	Sanzioni interdittive di cui all'art. 9 comma 2 del D.lgs 231/01 per una durata non superiore a 6 mesi (in caso di condanna)

Alle sanzioni sopraccitate vanno in ogni caso considerate le ulteriori forme di sanzione per gli illeciti amministrativi dipendenti da reato previste dalla normativa di riferimento:

 la confisca del prezzo o del profitto del reato, sempre disposta con la sentenza di condanna, salvo che per la parte che può essere restituita al danneggiato;

 la pubblicazione della sentenza di condanna (una sola volta, per estratto o per intero, in uno o più giornali indicati dal Giudice nella sentenza nonché mediante affissione nel comune ove l'ente ha la sede principale), che può essere disposta quando nei confronti dell'ente viene applicata una sanzione interdittiva.

7 INDIVIDUAZIONE DELLE AREE A RISCHIO, DELLE ATTIVITÀ SENSIBILI E DEI RUOLI AZIENDALI COINVOLTI

Le principali aree aziendali a potenziale rischio reato relativamente alle fattispecie di cui all'art. 25-septies del D.lgs 231/01 sono identificate e valutate nell'ambito dei documenti aziendali di valutazione dei rischi, predisposti ai sensi della normativa di riferimento e costantemente aggiornati in relazione all'evoluzione delle caratteristiche dell'attività societaria. Tuttavia, come precisato dalle Linee Guida di Confindustria per la costruzione dei Modelli di organizzazione, gestione e controllo ex D.lgs 231/01, non è possibile individuare e limitare, aprioristicamente, alcun ambito di attività, dal momento che tale casistica di reati può, di fatto, investire la totalità delle componenti aziendali.

In altri termini, i reati oggetto della presente Parte Speciale potrebbero astrattamente essere commessi in tutti i casi in cui vi sia, in seno all'azienda, una violazione degli obblighi e delle prescrizioni in materia di salute e sicurezza sul lavoro.

Poiché la valutazione dei rischi rappresenta l'adempimento cardine per la garanzia della salute e della sicurezza dei lavoratori e poiché costituisce il principale strumento per procedere all'individuazione delle misure di tutela, siano esse la riduzione o l'eliminazione del rischio, l'operazione di individuazione e di rilevazione dei rischi deve essere effettuata con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza.

Il Modello, pertanto, prevede un costante aggiornamento del Documento di Valutazione dei Rischi (di seguito "DVR"), fornendo così evidenza del suo continuo adeguamento e della sua completezza.

8 PRINCIPI GENERALI DI COMPORTAMENTO

La presente procedura detta le Regole di condotta generali che, unitamente ai Principi generali di comportamento sopra evidenziati, dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi dei Reati descritti in premessa.

TUTTI I DIPENDENTI ED I COLLABORATORI DELLA SOCIETÀ SONO TENUTI A:

1) rispettare le norme, gli obblighi e i principi posti dalla normativa vigente e dalle norme/linee guide in materia di salute e sicurezza elencate nella presente procedura;

2) rispettare le regole di condotta generale, i principi di controllo e le prescrizioni specifiche formulate nel presente Modello;

3) promuovere il rispetto delle suddette norme, regole e principi ed assicurare gli adempimenti in materia di salute e sicurezza sul lavoro;

4) adottare una condotta di massima collaborazione e trasparenza e rispettare i principi di condotta e comportamento sopra precisati nei rapporti con gli enti pubblici competenti in materia salute e sicurezza sul lavoro, sia in fase di stesura e comunicazione di eventuali dichiarazioni, sia in occasione di accertamenti/verifiche ispettive;

5) promuovere l'informazione e formazione interna in tema di rischi specifici connessi allo svolgimento delle proprie mansioni e attività, di struttura e regolamento aziendale in materia di salute e sicurezza, procedure e misure di prevenzione e protezione e/o prendere atto dell'informazione fornita e/o partecipare attivamente ai corsi di formazione;

6) utilizzare correttamente i macchinari, le apparecchiature, gli utensili, i materiali, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;

7) segnalare ai Responsabili o ai soggetti responsabili per la gestione della salute e sicurezza violazioni delle norme definite ed ogni situazione di pericolo potenziale o reale;

8) attenersi scrupolosamente alle linee guida, direttive ed indicazioni operative impartite dalla funzione Qualità, Sicurezza e Ambiente.

Il Datore di Lavoro e tutti i soggetti aventi compiti, attribuzioni e/o responsabilità nella gestione degli adempimenti previsti delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, quali, a titolo esemplificativo, Responsabile del Servizio di Prevenzione e Protezione (R.S.P.P.), Rappresentante dei Lavoratori per la Sicurezza (R.L.S.), Medico Competente (M.C.), addetti al primo soccorso, addetti emergenze in caso d'incendio, ognuno nell'ambito di propria competenza, devono garantire:

a) la definizione degli obiettivi per la sicurezza e la salute dei lavoratori;

b) l'identificazione continua dei rischi;

c) un adeguato livello di informazione/formazione dei dipendenti e dei fornitori/ appaltatori, sul sistema di gestione della sicurezza e salute definito da GETOPEN e sulle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole di comportamento e controllo definite dalla Società;

d) la definizione e l'aggiornamento (in base a cambiamenti nella struttura organizzativa ed operativa della Società) di procedure specifiche per la prevenzione di infortuni e malattie, in cui siano, tra l'altro, disciplinate le modalità di gestione degli incidenti e delle emergenze, nonché dei segnali di rischio / pericolo quali "quasi incidenti";

e) l'idoneità delle risorse, umane - in termini di numero e qualifiche professionali, formazione - e materiali, necessarie al raggiungimento degli obiettivi prefissati dalla Società per la sicurezza e la salute dei lavoratori;

f) la manutenzione ordinaria e straordinaria degli strumenti e delle strutture aziendali.

In generale tutti i soggetti sopra individuati devono rispettare gli obblighi previsti dal D.lgs. 81/2008 ("Testo Unico sulla Sicurezza") e dalla normativa vigente in materia di salute e sicurezza sul lavoro – così come anche modificati dal nuovo Testo Unico sulla Sicurezza - nonché quanto definito dalla Società, al fine di preservare la salute e la sicurezza dei lavoratori e comunicare tempestivamente,

alle strutture individuate e nelle modalità definite nelle procedure aziendali, eventuali segnali di rischio / pericolo (ad esempio "quasi incidenti"), incidenti (indipendentemente dalla loro gravità) e violazioni alle regole di comportamento e alle procedure aziendali.

INOLTRE È FATTO ESPRESSO DIVIETO A TUTTI I SOGGETTI SOPRA INDIVIDUATI DI:

g) porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-septies del D.Lgs. 231/2001);

h) porre in essere o dare causa a violazioni dei principi comportamentali e delle procedure aziendali.

9 GESTIONE DEI RISCHI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO

La gestione dei rischi in materia di salute e sicurezza sul lavoro riguarda qualunque tipologia di attività finalizzata a sviluppare ed assicurare un sistema di prevenzione e protezione dei rischi esistenti sul luogo di lavoro, in ottemperanza a quanto previsto dal D. Lgs. 81/2008 (di seguito Testo Unico).

Si rammenta anzitutto che, ai sensi del Testo Unico compete al Datore di lavoro la responsabilità per la definizione della politica aziendale riguardante la salute e la sicurezza dei lavoratori sul luogo di lavoro e compete al Committente e/o ai suoi delegati la responsabilità e la gestione dei cantieri temporanei o mobili disciplinati dal Titolo IV del Testo Unico nonché compete ad entrambi, per gli ambiti di rispettiva pertinenza, il rispetto degli obblighi relativi all'affidamento di contratti d'appalto, d'opera o di somministrazione previsti dall'art. 26 del medesimo Testo Unico.

In ottemperanza a quanto disposto dalla predetta normativa, GETOPEN adotta e tiene aggiornato il "Documento di Valutazione dei Rischi" (DVR), che rappresenta l'evidenza documentale di un processo permanente di prevenzione dei rischi per la salute e la sicurezza dei lavoratori.

Il DVR è un documento elaborato dal Datore di Lavoro, in collaborazione con il Responsabile del Servizio di Prevenzione e Protezione e con il Medico Competente nei casi in cui sia obbligatoria la sorveglianza sanitaria, previa consultazione del Rappresentante dei Lavoratori per la Sicurezza.

"DOCUMENTO DI VALUTAZIONE DEI RISCHI" CONTIENE:

• la valutazione dei rischi per la sicurezza e la salute durante l'attività lavorativa;

• l'individuazione delle misure di prevenzione e protezione poste a tutela dei lavoratori ed il programma delle misure ritenute opportune per garantire il miglioramento nel tempo del livello di sicurezza;

• l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;

• l'indicazione del nominativo del Responsabile del Servizio di Prevenzione e Protezione, dei Rappresentanti dei Lavoratori per la Sicurezza e dei Medici Competenti che hanno partecipato alla valutazione del rischio;

• l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento;

• l'individuazione delle misure di prevenzione, di protezione e dei dispositivi di protezione individuale, conseguente alla valutazione dei rischi connessi all'esercizio dell'attività lavorativa esercitata. Sul punto, il RSPP e i Preposti compilano scheda di consegna/gestione dei dispositivi di protezione individuali, necessari per la lavorazione e ne verificano il loro stato d'uso nonché l'eventuale scadenza.

IL PRESENTE DOCUMENTO DI VALUTAZIONE DEI RISCHI:

•è stato redatto ai sensi dell'art. 17 del D.lgs. 81/08;

•è soggetto ad aggiornamento periodico ove si verificano significativi mutamenti che potrebbero averlo reso superato.

La valutazione dei rischi è stata effettuata dal Datore di Lavoro con la collaborazione del Medico Competente, per quanto di sua competenza, del Servizio di Prevenzione e Protezione ed il coinvolgimento preventivo del Rappresentante dei Lavoratori per la Sicurezza.

Il Documento di Valutazione dei Rischi individua, all'interno dell'organizzazione aziendale, le responsabilità, le procedure, i processi e le risorse per la realizzazione della propria politica di prevenzione nel rispetto delle norme di salute e sicurezza vigenti.

La valutazione dei rischi consiste in un esame sistematico di tutti gli aspetti dell'attività lavorativa, volto a stabilire cosa può provocare lesioni o danni, se è possibile eliminare i pericoli e, nel caso in cui ciò non sia possibile, quali misure di prevenzione o di protezione sono o devono essere messe in atto per controllare i rischi.

L'adozione e l'applicazione di procedure operative di sicurezza aiutano a mitigare gli eventuali rischi residui in tutte quelle attività di lavoro per le quali, pur attuando tutte le disposizioni di sicurezza previste dalla normativa, restano in atto dei rischi direttamente correlati al tipo di attrezzatura utilizzata, all'ambiente di lavoro, ai prodotti impiegati e alle interferenze.

La politica aziendale in tema di salute e sicurezza sul lavoro deve essere diffusa, compresa, applicata ed aggiornata a tutti i livelli organizzativi, a tal fine vengono predisposti piani formativi adeguati e rispondenti alla normativa in materia, che tengano in considerazione il ruolo aziendale ricoperto, l'esposizione a specifici rischi e l'assegnazione di particolari incarichi per la gestione delle situazioni di emergenza. Le linee d'azione generali di GETOPEN devono essere orientate a un costante miglioramento della qualità della sicurezza e devono contribuire allo sviluppo effettivo di un "sistema di prevenzione e protezione". Tutte le Funzioni Aziendali devono osservare le disposizioni in materia di salute, di sicurezza e di igiene del lavoro e tenerne conto in occasione di qualsivoglia modifica degli assetti esistenti, compresi ristrutturazioni/allestimenti di siti operativi.

La valutazione dei rischi è aggiornata, utilizzando le informazioni ottenute dall'attività di monitoraggio e, comunque, ogni volta che intervengono cambiamenti significativi del processo produttivo o di organizzazione del lavoro, cambiamenti legislativi, evoluzione della tecnica o a seguito di eventi, quali emergenze, infortuni.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte di GETOPEN, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

DESCRIZIONE DEL PROCESSO

Il processo di gestione dei rischi in materia di salute e sicurezza sul lavoro prevede le seguenti fasi:

• identificazione dei pericoli e loro classificazione (pericoli per la sicurezza e pericoli per la salute dei lavoratori);

• valutazione dei rischi;

• individuazione e predisposizione delle misure di prevenzione e di protezione;

• definizione di un piano di intervento con l'identificazione delle strutture aziendali competenti all'attuazione di detti interventi;

• realizzazione degli interventi pianificati nell'ambito di un programma;

• verifica dell'attuazione e controllo sull'efficacia delle misure adottate.

La valutazione dei rischi esamina in maniera sistematica tutti gli aspetti dei luoghi di lavoro, per definire le possibili od eventuali cause di lesioni o danni.

LA VALUTAZIONE DEI RISCHI

La valutazione dei rischi è uno strumento finalizzato alla programmazione delle misure di protezione e prevenzione, quindi, alla più generale organizzazione della prevenzione aziendale volta a salvaguardare la salute e la sicurezza dei lavoratori.

Il D. Lgs. 9 Aprile 2008, n. 81 e s.m.i. ribadisce l'obbligo della valutazione di tutti i rischi per la sicurezza e la salute dei lavoratori, con la conseguente elaborazione del documento previsto dall'art. 28.

La valutazione riguarderà anche la scelta delle attrezzature di lavoro e delle sostanze e dei preparati chimici impiegati, la sistemazione dei luoghi di lavoro, i

rischi dei gruppi di lavoro esposti a rischi particolari (stress lavoro-correlato, lavoratrici in stato di gravidanza, minori, ect.), nonché quelli connessi alle differenze di genere, di età, di provenienza.

Ai sensi dell'art. 28, infatti, il documento redatto a conclusione della valutazione deve avere data certa e contenere:

a) Una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa;

b) l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuali adottati, a seguito della valutazione di cui all'articolo 17, comma 1, lettera a);

c) il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;

d) l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;

e) l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o di quello territoriale e del medico competente che ha partecipato alla valutazione del rischio;

f) l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

Il documento sarà utilizzato come guida da tutti i soggetti facenti parte del sistema organizzativo della sicurezza, al fine di applicare tutte le misure da adottare in relazione ai rischi presenti.

Tutti saranno soggetti alla piena osservanza e applicazione delle misure di sicurezza riportate nel presente documento.

AI FINI DELLA SCELTA DEI DPI, IL DATORE DI LAVORO:

• deve effettuare l'analisi e la valutazione dei rischi che non possono essere evitati con altri mezzi;
• deve individuare le caratteristiche dei DPI necessarie affinché questi siano adeguati ai rischi stessi, tenendo conto delle eventuali ulteriori fonti di rischio rappresentate dagli stessi DPI;
• deve valutare, sulla base delle informazioni e delle norme d'uso fornite dal fabbricante a corredo dei DPI, le caratteristiche dei DPI disponibili sul mercato e le ha raffrontate con le caratteristiche individuate nella scelta degli stessi;
• deve provvedere ad aggiornare la scelta ogni qualvolta intervenga una variazione significativa negli elementi di valutazione.

10 SALUTE E SICUREZZA SUI LUOGHI DI LAVORO – GESTIONE EMERGENZA COVID 19

Per quanto concerne il rischio biologico, in relazione all'emergenza Coronavirus in atto sul territorio Italiano ed in considerazione dei recenti sviluppi e del continuo aggiornamento delle disposizioni governative per il contenimento del virus COVID-19 ed in particolare ai DPCM emanati dal Consiglio dei Ministri si pone l'obbligo per tutto il personale di attenersi alle misure emanate dalle autorità statali così come integrato nel "*Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus COVID-19 negli ambienti di lavoro e nei cantieri temporanei e mobili*". Si pone l'obbligo del rispetto delle ordinanze regionali e delle procedure di sicurezza adottate dal datore di lavoro per rispondere all'emergenza sanitaria.
Il "*Protocollo condiviso di regolazione delle misure per il contrasto ed il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro*" visto la fine dell'emergenza viene gestito in maniera puntuale dal Servizio di Prevenzione e Protezione e dall'ufficio preposto con comunicazioni via mail o informative dirette in modo da raggiungere in maniera più efficace possibile i lavoratori dell'organizzazione.

11 RISPETTO DEGLI STANDARD TECNICO STRUTTURALI DI LEGGE

Il RSPP, su indicazione del DL, con la collaborazione del MC, per quanto di sua competenza, e con il coinvolgimento preventivo del RLS, è tenuto a compilare e aggiornare un elenco di tutte le norme di salute e sicurezza applicabili all'azienda in cui riportare il campo di applicazione, la Funzione Aziendale interessata, il responsabile dell'aggiornamento della normativa e della sua diffusione alle funzioni interessate.

12 L'ACQUISTO, UTILIZZO E MANUTENZIONE DELLE ATTREZZATURE

Tutte le attrezzature utilizzate dal personale GETOPEN Srl sono sottoposte a corretta manutenzione, ordinaria e straordinaria, e opportunamente correlate da libretto di uso e manutenzione e marcature CE.

Con la cadenza prevista nei libretti d'uso e manutenzione delle apparecchiature e degli impianti il RATTR, anche avvalendosi di personale esperto e qualificato, dovrà effettuare verifiche di adeguatezza, integrità e regolarità degli stessi, in maniera documentale, facendole vistare dal RSPP, e sottoponendole all'approvazione dell'AU.

IL RATTER SI ASSICURERÀ, INOLTRE, CHE LE ATTREZZATURE DI LAVORO:

- siano oggetto di idonea manutenzione al fine di garantire la permanenza dei requisiti di sicurezza
- siano corredate, ove necessario, da apposite istruzioni d'uso e libretto di manutenzione.

Anche i dispositivi personali di protezione devono essere tenuti in buono stato e sottoposti alla necessaria manutenzione.

A seguito di tali manutenzioni, ogni qualvolta siano effettuate, dovrà essere compilata una scheda con indicazione dell'intervento effettuato, delle parti eventualmente sostituite, la data dell'intervento, la firma del manutentore e la data del successivo intervento.

Il RAM/APVG, annualmente, deve monitorare le spese relative alla "gestione delle manutenzioni", assicurandosi che esse siano in linea con quelli sostenuti negli esercizi precedenti; a tal fine, deve vistare e conservare la documentazione (es. bilanci analitici).Gli appaltatori per poter operare all'interno o in collaborazione con la Società devono dare evidenza del rispetto e adempienza di tutte le norme vigenti applicabili, nonché dei parametri definiti dalla Società all'interno delle proprie procedure.

Il Datore di Lavoro, attraverso la propria struttura organizzativa, secondo quanto previsto dall'art. 26 del D. Lgs 81/2008, qualora siano presenti interferenze, promuove la cooperazione ed il coordinamento di cui ai punti precedenti, elaborando un Documento Unico di Valutazione dei Rischi per le Interferenze, nel quale siano indicate le misure adottate per eliminare o, laddove non sia possibile, per ridurre al minimo le interferenze. Tale documento deve allegarsi al contratto di appalto o d'opera, già in fase di procedura di affidamento. Il documento può essere, eventualmente, aggiornato all'atto della consegna delle aree.

È, peraltro, obbligatorio attivare le procedure di cui al TITOLO IV del D. Lgs. 81/2008 nel caso si tratti di cantieri temporanei e mobili.

Durante l'effettuazione dei lavori, il DL o un suo incaricato direttamente o tramite il soggetto identificato per il controllo, deve verificare che gli appaltatori operino ed agiscano in maniera compatibile e congruente con le indicazioni di SSL stabilite in sede di contratto, con la Politica dell'azienda, e con il DUVRI.

Viene regolamentata, anche attraverso *check list* compilative, la dotazione dei mezzi di trasporto al momento della partenza per i cantieri di competenza, del *travel kit* di primo soccorso, dei DPI, dell'attrezzatura per la recinzione dei cantieri e dei dispositivi in dotazione per contattare il Servizio Sanitario Nazionale in caso di infortunio, il tutto in misura adeguata al numero di lavoratori assegnati al cantiere.

Nei contratti di somministrazione (art. 1559 c.c.), di appalto (art. 1655 c.c.) e di subappalto (art. 1656 c.c.), devono essere specificamente indicati i costi relativi alla sicurezza del lavoro con particolare riferimento a quelli propri connessi allo

specifico appalto. A tali dati possono accedere tutte le figure coinvolte con le modalità previste dal D. Lgs 81/2008, su richiesta, nonché il RSPP.

13 GESTIONE EMERGENZE E PRIMO SOCCORSO

Il DL o un suo incaricato pianifica la gestione delle emergenze come segue:

1. designa i lavoratori, previa consultazione del RSPP e del RLS, incaricati dell'attuazione delle misure di prevenzione e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza. Gli addetti, prima di essere adibiti a tali mansioni, devono essere formati ed addestrati come previsto dalla legge. Gli addetti alle emergenze e al primo soccorso devono essere disponibili all'occorrenza; la pronta disponibilità è intesa come presenza fisica, sempre assicurata, all'interno degli ambienti di lavoro. Pertanto, nella loro individuazione, è necessario tenere conto: della dislocazione dei lavoratori in più sedi aziendali, dei turni e della presenza di disabili. L'elenco degli addetti antincendio/primo soccorso viene reso noto a tutti i lavoratori e messo loro a disposizione, ad esempio, tramite apposita lista affissa in bacheca;
2. definisce le necessarie misure organizzative e gestionali, da attuare in caso di emergenza, affinché tutto il personale non impegnato nella gestione dell'emergenza possa mettersi al sicuro individuando le vie di esodo, i punti di raccolta, le raccomandazioni rispetto agli atteggiamenti da tenere durante l'evacuazione e redige il Piano di emergenza;
3. organizza le modalità di comunicazione con i servizi pubblici competenti in materia di primo soccorso, salvataggio, lotta antincendio e gestione delle emergenze;
4. stabilisce le modalità di diramazione dell'allarme (es.: sonoro, vocale, luminoso, *etc.*);
5. informa i lavoratori circa le misure predisposte e i comportamenti da adottare;
6. garantisce la presenza di planimetrie chiare, con l'indicazione delle vie di fuga e dei presidi antincendio;

7. organizza esercitazioni con cadenza annuale (similarmente a quanto previsto nel DVR), simulando le emergenze possibili, identificate e riportate, ove presente, nel piano di emergenza. Le esercitazioni sono necessarie al fine di verificare la consapevolezza dei lavoratori e degli addetti alle emergenze relativamente a: vie di fuga; porte resistenti al fuoco, ove esistenti, ubicazione dei dispositivi di allarme e delle attrezzature di spegnimento; collocazione della cassetta di primo soccorso, posizione dei luoghi di raccolta *etc.* L'esito delle prove di emergenza deve essere oggetto di attenta valutazione dell'adeguatezza delle misure di gestione delle emergenze programmate e può dare luogo a miglioramenti delle stesse.

Per la gestione delle emergenze si rinvia a quanto previsto dal sistema di gestione della sicurezza sul lavoro.

Il Datore di Lavoro, in collaborazione con il Medico Competente, organizza il servizio di primo soccorso.

14 COMUNICAZIONE E RAPPORTO CON L'ESTERNO

Il RSPP gestisce le comunicazioni interne ed esterne relativamente alle tematiche di Salute e Sicurezza, coinvolgendo, se opportuno, i lavoratori dell'azienda, come previsto dalla legislazione vigente e dai contratti collettivi di lavoro, raccogliendo osservazioni, commenti e proposte dai lavoratori e dagli altri soggetti interessati (enti locali, cittadini, dipendenti diretti e indiretti, clienti e fornitori, *etc.*).

15 CONSULTAZIONE E PARTECIPAZIONE

L'efficace attuazione del Modello presuppone la piena responsabilizzazione di tutti i soggetti presenti nel luogo di lavoro. L'Azienda promuove, quindi, la piena adesione al Modello di tutti i lavoratori, nonché la cooperazione in materia di salute e sicurezza negli ambienti di lavoro. L'Azienda assicura il tempo necessario per lo svolgimento del proprio incarico (contratti collettivi di lavoro) e la massima collaborazione. I lavoratori devono essere consultati, in particolare. per quanto

previsto dalla legislazione vigente (un momento specifico di consultazione è la riunione *ex* art 35 del D.lgs. 81/2008).

16 ATTIVITÀ DI INFORMAZIONE E FORMAZIONE DEI LAVORATORI

Il DL ha la responsabilità di fornire i mezzi e le risorse adeguate allo svolgimento delle attività di addestramento, formazione ed informazione, incluse le competenze esterne o interne necessarie per la loro esecuzione; a questi spetta il compito di approvare il "Programma di formazione, informazione ed addestramento" proposto dal RSPP in collaborazione col RLS ed il Medico Competente; detto programma deve essere aggiornato in occasione della revisione ed eventuale rielaborazione della valutazione dei rischi, nel caso di modifiche legislative, di nuove assunzioni, di cambiamenti nelle mansioni, nei cambiamenti di attività o processi (nuove macchine, attrezzature, impianti, nuove modalità operative, etc.), dell'evoluzione tecnica.

Il RSPP ha il dovere di compilare il registro personale della formazione/informazione/addestramento per ciascun lavoratore e per i neo assunti e ha la responsabilità di conservare, nell'archivio delle registrazioni, la documentazione comprovante la formazione, l'informazione e l'addestramento effettuato (verbali di addestramento, copie di attestati di partecipazione, diplomi, etc.), i risultati relativi alla verifica delle qualifiche e all'efficacia delle azioni formative eseguite.

Al termine degli interventi formativi, deve essere verificato il grado di apprendimento secondo le modalità previste dall'Accordo Stato Regioni in materia di Formazione alla salute e sicurezza nei luoghi di lavoro, sia per i corsi organizzati dal DL stesso che per quelli erogati presso soggetti esterni.

Nell'ambito del programma di formazione è obbligatorio, inoltre, formare i lavoratori sugli aspetti principali del MOG e su ruoli, compiti e responsabilità di ciascuna figura in esso coinvolta.

Si precisa che la gestione dell'informazione dei lavoratori verrà implementata nell'organizzazione aziendale con l'ausilio di uno strumento didattico, ovvero di

un opuscolo informativo includente gli argomenti del D.Lgs 81/08, redatto dal RSPP in modo da risultare facilmente comprensibile e soprattutto specifico per l'attività svolta dall'azienda.

GETOPEN assicura, altresì, ai propri dipendenti un'informazione ed una formazione adeguata in ragione del tipo di attività resa. Infatti, è prevista una formazione specifica che, tuttavia, non è sostitutiva della formazione obbligatoria spettante, comunque, a tutti i lavoratori e realizzata ai sensi dell'articolo 37 del d.lgs. n. 81/2008. Tale formazione deve, pertanto, considerarsi integrativa della formazione prevista dall'accordo Stato-Regioni di cui all'articolo 37, comma 2, del d.lgs. n. 81/2008.

I CORSI AGGIUNTIVI SONO DIRETTI A:

- lavoratori adibiti all'installazione ed alla rimozione della segnaletica di cantieri stradali in presenza di traffico o comunque addetti ad attività in presenza di traffico;
- preposti alle attività di cui all'articolo 1 del presente decreto;
- lavoratori addetti che svolgono attività lavorativa negli ambienti sospetti di inquinamento (artt. 66 e 121 del D. Lgs 81/2008) o spazi confinati (allegato IV – punto 3 del D. Lgs 81/2008). In particolare, i lavoratori devono essere in possesso di adeguata esperienza professionale, formazione, addestramento nonché specifica idoneità sanitaria.

OBBLIGHI DEI LAVORATORI

I lavoratori si sottopongono al programma di formazione e addestramento organizzato dal datore di lavoro. I lavoratori utilizzano i DPI e DPC messi a loro disposizione conformemente all'informazione e alla formazione ricevute e all'addestramento eventualmente organizzato, inoltre hanno cura dei DPI messi a loro disposizione e non vi apportano modifiche di propria iniziativa (art. 78 comma 3 D. Lgs. 81/08).

Al termine dell'utilizzo i lavoratori seguono le procedure aziendali in materia di riconsegna dei DPI e segnalano immediatamente al datore di lavoro o al dirigente

o al preposto qualsiasi difetto o inconveniente da essi rilevato nei DPI messi a loro disposizione (art. 78, comma 4 e 5, D. Lgs. 81/08)

17 LO STANZIAMENTO DI FONDI PER LA GESTIONE DEL SSL

L'Amministratore Unico, in occasione dell'assemblea annuale di approvazione del bilancio, deve sottoporre all'assemblea dei soci lo stanziamento di adeguati fondi da destinare, nell'anno, in favore della Sicurezza e della Salute dei Lavoratori.
E' compito dell'Organismo di Vigilanza verificare l'effettiva approvazione del predetto stanziamento.

18 RIESAME E VERIFICA ATTUAZIONE ED EFFICACIA DEL MODELLO

Il DL deve riesaminare, annualmente, in relazione agli adempimenti relativi alla sicurezza sul lavoro, e con l'ausilio di consulenti all'uopo preposti, il Modello Organizzativo Gestionale per verificare che:

- sia attuato con efficacia;
- sia idoneo per il mantenimento ed il miglioramento delle misure adottate;
- garantisca il raggiungimento degli obiettivi di SSL;
- permetta di esprimere una valutazione sulle prestazioni complessive;
- consenta di programmare le attività per il miglioramento continuo.

IN PARTICOLARE, IL DL DOVRÀ VERIFICARE:

- ✓ i risultati del monitoraggio interno, con riferimento al grado di raggiungimento degli obiettivi;
- ✓ gli esiti delle azioni intraprese nel precedente riesame e la loro efficacia;
- ✓ i dati sugli infortuni e malattie professionali;
- ✓ le analisi delle cause di eventuali infortuni, incidenti e situazioni di emergenza;
- ✓ le relazioni del Medico Competente, se nominato;

- ✓ i cambiamenti, interni ed esterni, rilevanti per l'impresa (nuove lavorazioni, personale, contratti, nuove leggi, novità in relazione al progresso scientifico e tecnologico, *etc.*) e l'emergere di eventuali nuovi rischi;
- ✓ rapporti sulle prove di emergenza;
- ✓ risultati delle azioni correttive e preventive intraprese sul modello;
- ✓ risultati della consultazione e del coinvolgimento;
- ✓ dati sulla formazione e addestramento effettuati;
- ✓ report o segnalazioni da parte dell'OdV;
- ✓ eventuali sanzioni applicate.

Qualora il DL lo ritenga opportuno può far coincidere il Riesame con la riunione periodica, ove prevista, *ex* art. 35 del D.lgs, 81/2008 e ss.mm.ii. In questo caso, le Figure Aziendali interessate ed i temi trattati devono rispettare anche quanto previsto dalla legislazione.

19 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

Le Funzioni Aziendali responsabili dell'individuazione, dell'attuazione e del controllo sulle misure relative alla sicurezza, all'igiene e alla salute nei luoghi di lavoro sono tenuti a comunicare, tempestivamente e direttamente, all'Organismo di Vigilanza (OdV) qualsiasi condotta posta in essere in difformità al Modello, alla presente procedura ed al Codice Etico, indicando le ragioni delle difformità e precisando il processo autorizzativo seguito.

IL DATORE DI LAVORO, O SOGGETTO DEBITAMENTE AUTORIZZATO, INFORMA TEMPESTIVAMENTE L'ODV CIRCA:

- ➢ quasi infortuni e tutti gli infortuni che si verificano;
- ➢ eventuali azioni e/o interventi e/o provvedimenti dell'Autorità Giudiziaria nonché della Polizia Giudiziaria (compresa la ASL con funzione di Polizia Giudiziaria), o di altra Autorità competente, in caso di verifica circa il rispetto della normativa vigente in materia di sicurezza sui luoghi di lavoro;

- i *report* rilasciati dagli organismi di certificazione in sede di *audit*, e delle eventuali non conformità riscontrate.

In particolare, il Datore di Lavoro – coadiuvato dal Responsabile del Servizio di Prevenzione e Protezione – almeno annualmente provvede a informare/inviare l'OdV:

- in merito agli esiti delle verifiche sulla corretta attuazione della normativa vigente, informando lo stesso, costantemente, relativamente allo stato dei suggerimenti avanzati in sede di attività ispettiva;
- in merito alle statistiche relative agli incidenti verificatisi sul luogo di lavoro, specificandone la causa, l'avvenuto riconoscimento di infortuni e la relativa gravità;
- in merito all'andamento della sorveglianza sanitaria ed ai relativi esiti (relazione sanitaria annuale del medico competente e denunce di malattie professionali);
- in merito ad ogni variazione che richieda, o che abbia richiesto, l'aggiornamento della valutazione dei rischi;
- in merito agli acquisti/investimenti in situazioni di emergenza ed *extra-budget*;
- il verbale della riunione periodica (art. 35 D.lgs. 81/2008);
- il piano della formazione;
- lo stato di avanzamento rispetto al programma di miglioramento in materia di salute e sicurezza sul luogo di lavoro;
- eventuali provvedimenti disciplinari adottati nei confronti dei destinatari della presente procedura, per violazioni riguardanti la salute e sicurezza nei luoghi di lavoro.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di corporate governance per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari;

• proporre un eventuale aggiornamento del Modello o delle procedure previste per la sua attuazione, previa condivisione con il Datore di Lavoro.

Le Funzioni Aziendali devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio ordinato – tutta la documentazione all'uopo necessaria.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 20.03.2024	ADOZIONE
Rev. 1	Determina dell'Amministratore Unico del 05.08.2024	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231)

PARTE SPECIALE -11-

SOMMARIO

1 OBIETTIVI E FUNZIONI DEL MODELLO

L'art. 24 ter del Decreto, inserito dalla L. 94/2009, prevede innanzitutto un gruppo di reati inerenti alle varie forme di associazioni criminose, e cioè:

• Associazione per delinquere generica (art. 416 c.p., primi cinque commi);

• Associazione di tipo mafioso, anche straniera e scambio elettorale politico-mafioso (artt. 416 bis e 416 ter);

• Associazione per delinquere finalizzata alla commissione di delitti in tema di schiavitù, di tratta di persone e di immigrazione clandestina (art. 416 c.p., commi 6 e 7);

• Associazione per delinquere finalizzata al traffico illecito di sostanze stupefacenti o psicotrope(art. 74 D.P.R. n. 309/1990).

Con riferimento alle fattispecie di associazioni per delinquere sopra considerate, la sanzione penale è ricollegata al solo fatto della promozione, costituzione, partecipazione ad una associazione criminosa formata da tre o più persone, indipendentemente dall'effettiva commissione (e distinta punizione) dei reati che costituiscono il fine dell'associazione. Ciò significa che la sola cosciente partecipazione ad una associazione criminosa da parte di un esponente o di un dipendente dell'ente potrebbe determinare la responsabilità amministrativa dell'ente stesso, sempre che la partecipazione o il concorso all'associazione risultasse strumentale al perseguimento anche dell'interesse o del vantaggio dell'ente medesimo. È inoltre richiesto che il vincolo associativo si esplichi attraverso un minimo di organizzazione a carattere stabile nel tempo e la condivisione di un programma di realizzazione di una serie indeterminata di delitti. Non basta cioè l'occasionale accordo per la commissione di uno o più delitti determinati. La giurisprudenza ritiene altresì possibile il concorso nel reato di associazione criminosa da parte di colui che, pur non partecipando all'associazione stessa, fornisca un apporto sostanziale, anche se episodico, alla sua sussistenza od al perseguimento dei suoi scopi.

L'associazione di tipo mafioso (art. 416 bis c.p.) si distingue dalla associazione per delinquere generica per il fatto che 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 delitti, oppure - anche non mediante la commissione di delitti, ma pur sempre con l'uso del metodo mafioso - per acquisire in modo diretto od indiretto la gestione o comunque 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 in occasione di consultazioni elettorali.

La norma si applica anche alla camorra e alle altre associazioni, comunque denominate, anche straniere, che presentino i connotati mafiosi predetti. Lo scambio elettorale politico-mafioso invece è commesso da chi propone o accetta la promessa di procurare voti con l'uso del metodo mafioso in cambio dell'erogazione o della promessa di denaro o di altra utilità.

Gli altri due tipi di associazioni criminose (art. 416, commi 6 e 7, c.p. e art. 74 D.P.R. n. 309/1990) sono invece caratterizzate dall'essere preordinate al fine della commissione degli specifici reati in esse considerati, vale a dire: dei reati in tema di schiavitù, di tratta di persone, di immigrazione clandestina, di traffico di organi, di reati sessuali contro i minori nonché dei reati di illecita produzione, traffico o detenzione di sostanze stupefacenti o psicotrope. Alcuni di questi specifici reati-fine costituiscono di per sé autonomi reati presupposto della responsabilità dell'ente, come meglio si dirà nel prosieguo a proposito dei reati contro la persona e dei reati transnazionali.

L'art. 24 ter prevede inoltre la generica categoria dei delitti di qualsivoglia tipo, commessi avvalendosi del metodo mafioso od al fine di favorire l'attività di una associazione mafiosa, fermo restando, per la responsabilità dell'ente, il requisito dell'interesse o del vantaggio del medesimo.

La prima circostanza si ritiene ricorra allorquando il soggetto agente, pur senza appartenere al sodalizio criminoso o concorrere con esso, pone in essere una condotta idonea ad esercitare una particolare intimidazione, quale ad esempio la minaccia avvalendosi dello sfruttamento della "fama" di organizzazioni criminali operanti nell'ambito di un determinato territorio. L'ipotesi della commissione di un reato di qualsiasi tipo atto ad agevolare l'attività di una associazione mafiosa si verifica quando il soggetto abbia agito con tale scopo specifico e la sua condotta sia concretamente idonea a realizzare tale risultato, come ad esempio nel caso del reato di riciclaggio compiuto essendo a conoscenza della riferibilità dell'operazione ad una associazione mafiosa.

Infine, ai sensi del medesimo art. 24 ter, rilevano i seguenti reati, solitamente, anche se non necessariamente, realizzati nell'ambito di organizzazioni criminali.

Dunque, l'associazione per delinquere di cui all'art. 416 c.p. si configura: "*Quando tre o più persone si associano allo scopo di commettere più delitti*"; la condotta incriminata consiste sia nel "*promuovere, costituire od organizzare*" l'associazione, sia nel "*partecipare*" all'associazione. Elemento fondamentale è la coscienza e volontà di far parte in maniera permanente di un sodalizio criminoso, ed anche l'"*intenzione di contribuire all'attuazione del generico programma criminoso",* tuttavia non è necessario che la volontà abbia quale oggetto immediato la realizzazione di delitti specificamente individuati.

Orbene, l'inserimento del delitto di associazione per delinquere nel catalogo 231 comporta che laddove un numero non inferiore a tre di soggetti operanti in seno alla società (subordinati o apicali) si associ allo scopo di commettere reati, potrebbe essere contestata la fattispecie di associazione per delinquere anche a carico dell'ente che sarebbe chiamato a rispondere patrimonialmente per tale evento.

Pertanto, poiché la contestazione dell'art. 416 c.p. - in quanto disposizione "aperta", idonea a ricomprendere nei reati-presupposto qualsiasi reato - determina una violazione del principio di tassatività del sistema sanzionatorio del D.lgs.vo n. 231 del 2001, è necessario trasferire gli elementi costitutivi del delitto di associazione

per delinquere sul piano aziendale, al fine di eseguire una concreta mappatura del rischio di tale fattispecie criminosa.

Infatti, con la presente procedura si vogliono definire le regole di condotta e le procedure concrete che tutti i Destinatari sono tenuti ad asservare, al fine preciso di individuare le attività a rischio-reato ai sensi dell'articolo 6, comma 2, lett. a) del D.Lgs. 231/2001 e prevenire la commissione dei delitti di criminalità organizzata, tenendo presente che la stessa natura del reato impedisce l'individuazione di peculiari settori dell'attività aziendale in cui vi sia rischio di perpetrazione dello stesso.

Ancora, la necessità di implementare la presente procedura è data dalle novità introdotte dal Codice dei contratti pubblici D.Lgs. n. 36/2023 e dall'interazione dello stesso decreto con il D.Lgs. 231/2001.

Invero, tra le novità di maggior interesse per le imprese private apportate dal nuovo Codice degli appalti, vi è quella relativa alle causa di esclusione automatica di un operatore economico dalla procedura (art. 94), senza alcun margine valutativo per la stazione appaltante, relativa alla condanna (per l'ente, nel procedimento 231, o per un esponente aziendale, in sede penale) per una serie di reati, tra i quali: **1)** associazione per delinquere; **2)** associazione di stampo mafioso; **3)** associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope; **4)** contrabbando; **5)** traffico illecito di rifiuti; **6)** reati contro la pubblica amministrazione; **7)** turbata libertà degli incanti; **8)** frode nelle pubbliche forniture; **9)** false comunicazioni sociali; **10)** reati di terrorismo; **11)** reati di riciclaggio; **12)** sfruttamento del lavoro minorile; **13)** tratta di esseri umani e **14)** ogni altro reato da cui derivi la pena accessoria dell'incapacità di contrattare con la pubblica amministrazione.

Ancora, in ordine alle interazioni del nuovo Codice degli Appalti con il D.Lgs. n. 231/2001, le previsioni di cui sopra collegano espressamente l'esclusione degli operatori economici al sistema della responsabilità amministrativa degli enti ed in particolare:

• esclusione automatica nel caso di condanna dell'ente, ai sensi del D.Lgs. n. 231/2001, per uno dei gravi reati-presupposto dell'art. 94, comma 1, del Codice degli appalti;

• esclusione automatica nel caso di condanna penale delle persone fisiche legate all'ente (art. 94, comma 3) per uno dei gravi reati-presupposto dell'art. 94, comma 1, del Codice degli appalti;

• esclusione automatica degli enti già destinatari della sanzione interdittiva di cui all'art. 9, comma 2, lett. c), del D.Lgs. n. 231/2001 («*il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio*») o di altra sanzione che comporta il divieto di contrarre con la pubblica amministrazione (senza vincolo alcuno, in questo caso, all'elenco dei gravi reati-presupposto dell'art. 94, comma 1, del Codice degli appalti);

• esclusione non automatica dell'ente di cui si accerti la commissione di un illecito professionale grave, desumibile – fra gli altri motivi – dalla commissione o dalla mera contestazione di un qualsiasi reato-presupposto di cui al D.Lgs. n. 231/2001.

2 ACRONIMI AZIENDALI

AU	Amministratore Unico
RSPP	Responsabile del Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC/RPROG	Responsabile Tecnico/Responsabile Progettazione
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RATTR	Responsabile Attrezzature e Mezzi
GRPROG	Gruppo Progettisti
PROG	Programmatori
RSCM	Responsabile singola commessa
CDL	Consulente del lavoro
REC	Responsabile esterno contabilità

PER L'IDENTIFICAZIONE DEI SOGGETTI CHE CORRISPONDONO AGLI ACRONIMI AZIENDALI SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI GETOPEN S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di GETOPEN S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di GETOPEN S.r.l.

4 CAMPO DI APPLICAZIONE RESPONSABILE DELLA PROCEDURA

La presente procedura si applica a tutti coloro i quali agiscono in nome e per conto della Società e la cui attività possa comportare la commissione dei reati di cui all'24-ter rubricato "*Delitti di criminalità organizzata*".

Le disposizioni della presente Parte Speciale hanno tutte le Funzioni Aziendali che agiscono in nome e per conto della Società affinché gli stessi adottino regole di condotta conformi a quanto prescritto al fine di prevenire il verificarsi dei delitti ivi considerati.

NELLO SPECIFICO LA PRESENTE PARTE SPECIALE HA LO SCOPO DI:

a) indicare i principi che i destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo di Vigilanza, ed ai Responsabili delle funzioni aziendali che con lo stesso cooperano, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

Il principale responsabile della presente procedura è l'Amministratore Unico.

5 I REATI DI CUI ALL'ART. 24-TER DEL DECRETO

L'art. 24 ter, d.lgs. 231/2001 prevede sanzioni pecuniarie ed interdittive per l'ente che si rende responsabile di uno degli illeciti dipendenti dai reati di criminalità organizzata.

Il reato di associazione per delinquere di cui all'art. 416 c.p. è un delitto di tipo associativo caratterizzato dalla concretizzazione di uno determinato e predefinito

programma sociale criminale, caratterizzato dall'accordo tra più persone per formare una compagine stabile.

La fattispecie di cui all'art. 416 bis c.p. è invece un delitto contraddistinto dal controllo di settori di attività finanziarie ed economiche, di appalti e servizi pubblici, dal turbamento del libero esercizio del voto. È però possibile parlare di associazione di tipo mafioso, solo se l'attività criminale è caratterizzata dall'utilizzo della forza intimidatrice, mentre le vittime devono trovarsi in una condizione di assoggettamento e omertà nei confronti dell'organizzazione stessa in ragione dell'intimidazione da questa esercitata.

Ai fini dell'applicazione d.lgs. 231/2001, in ambito aziendale e societario, i reati presupposto in argomento vengono annoverati nell'ambito delle attività cd. sensibili ed astrattamente realizzabili, in via prioritaria, nell'ambito di attività di gestione e funzionamento del soggetto giuridico (sponsorizzazioni, gestione risorse umane, rapporti con i fornitori).

5.1. - ASSOCIAZIONE PER DELINQUERE (ART. 416 C.P.)

Ai sensi dell'art. 416 c.p. "*Quando tre o più persone si associano allo scopo di commettere più delitti, coloro che promuovono o costituiscono od organizzano l'associazione sono puniti, per ciò solo, con la reclusione da tre a sette anni. Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni.*

I capi soggiacciono alla stessa pena stabilita per i promotori. Se gli associati scorrono in armi le campagne o le pubbliche vie, si applica la reclusione da cinque a quindici anni. La pena è aumentata se il numero degli associati è di dieci o più.

Se l'associazione è diretta a commettere taluno dei delitti di cui agli articoli 600, 601, 601-bis e 602, nonché all'articolo 12, comma 3-bis, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, nonché agli articoli 22, commi 3 e 4, e 22-bis, comma 1, della legge 1° aprile 1999, n. 91, si applica la reclusione da

cinque a quindici anni nei casi previsti dal primo comma e da quattro a nove anni nei casi previsti dal secondo comma 2.

Se l'associazione è diretta a commettere taluno dei delitti previsti dagli articoli 600-bis, 600-ter, 600- quater, 600-quater.1, 600-quinquies, 609-bis, quando il fatto è commesso in danno di un minore di anni diciotto, 609-quater, 609-quinquies, 609-octies, quando il fatto è commesso in danno di un minore di anni diciotto, e 609-undecies, si applica la reclusione da quattro a otto anni nei casi previsti dal primo comma e la reclusione da due a sei anni nei casi previsti dal secondo comma".

Si tratta di una fattispecie che ha natura plurisoggettiva, essendo necessaria per la configurabilità del reato la partecipazione di almeno tre persone.

Il reato è commesso da chiunque, in numero di tre o più persone, si associa allo scopo di commettere più delitti.

La fattispecie distingue i capi, ovvero coloro che promuovono, costituiscono o organizzano l'associazione da coloro che vi aderiscono con mera partecipazione, ritenendo il reato più grave nella prima ipotesi.

Il reato è aggravato se il numero degli associati è uguale o maggiore a dieci e nel caso in cui gli associati scorrano in armi per le pubbliche vie.

IL REATO ASSOCIATIVO SI CARATTERIZZA PER TRE ELEMENTI FONDAMENTALI COSTITUITI:

a. da un vincolo associativo tendenzialmente permanente;

b. dall'indeterminatezza del programma criminoso;

c. dall'esistenza di una struttura organizzativa, sia pur minima.

Elemento essenziale è l'accordo associativo.

5.2. – ASSOCIAZIONE DI TIPO MAFIOSO ANCHE STRANIERA (ART. 416-BIS C.P.)

Il reato si configura mediante la partecipazione ad un'associazione di tipo mafioso formata da tre o più persone. 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 delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di

attività economiche, di concessioni, di autorizzazioni, di appalti e di 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 in occasione di consultazioni elettorali.

"*Chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone, è punito con la reclusione da dieci a quindici anni.*

Coloro che promuovono, dirigono o organizzano l'associazione sono puniti, per ciò solo, con la reclusione da dodici a diciotto anni. 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 delitti, per acquisire in modo diretto o indiretto la gestione o comunque 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 in occasione di consultazioni elettorali.

Se l'associazione è armata si applica la pena della reclusione da dodici a venti anni nei casi previsti dal primo comma e da quindici a ventisei anni nei casi previsti dal secondo comma.

L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito.

Se le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto di delitti, le pene stabilite nei commi precedenti sono aumentate da un terzo alla metà.

Nei confronti del condannato è sempre obbligatoria la confisca delle cose che servirono o furono destinate a commettere il reato e delle cose che ne sono il prezzo, il prodotto, il profitto o che ne costituiscono l'impiego. [Decadono inoltre di diritto le licenze di polizia, di commercio, di commissionario astatore presso i mercati annonari all'ingrosso, le concessioni di acque pubbliche e i diritti ad esse inerenti nonché le

iscrizioni agli albi di appaltatori di opere o di forniture pubbliche di cui il condannato fosse titolare].

Le disposizioni del presente articolo si applicano anche alla camorra, alla 'ndrangheta 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."

5.3. – SCAMBIO ELETTORALE POLITICO MAFIOSO (ART. 416-TER C.P.)

L'articolo prevede "*Chiunque accetta la promessa di procurare voti mediante le modalità di cui al terzo comma dell'articolo 416-bis in cambio dell'erogazione o della promessa di erogazione di denaro o di altra utilità è punito con la reclusione da sei a dodici anni. La stessa pena si applica a chi promette di procurare voti con le modalità di cui al primo comma."*

Detto reato reprime la condotta di chiunque accetta la promessa di procurare voti, mediante le modalità di cui al terzo comma dell'articolo 416-bis, in cambio dell'erogazione o della promessa di erogazione di denaro o di altra utilità.

La pena prevista dal Legislatore è reclusione da quattro a dieci anni e la stessa pena si applica a chi promette di procurare voti con le modalità di cui al primo comma.

5.4. - SEQUESTRO DI PERSONA A SCOPO DI ESTORSIONE (ART. 630 C.P.)

Ai sensi della norma in commento "*Chiunque sequestra una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione, è punito con la reclusione da venticinque a trenta.*

Se dal sequestro deriva comunque la morte, quale conseguenza non voluta dal reo, della persona sequestrata, il colpevole è punito con la reclusione di anni trenta. Se il colpevole cagiona la morte del sequestrato si applica la pena dell'ergastolo.

Al concorrente che, dissociandosi dagli altri, si adopera in modo che il soggetto passivo riacquisti la libertà, senza che tale risultato sia conseguenza del prezzo della

liberazione, si applicano le pene previste dall'articolo 605. Se tuttavia il soggetto passivo muore, in conseguenza del sequestro, dopo la liberazione, la pena è della reclusione da sei a quindici anni.

Nei confronti del concorrente che, dissociandosi dagli altri, si adopera, al di fuori del caso previsto dal comma precedente, per evitare che l'attività delittuosa sia portata a conseguenze ulteriori ovvero aiuta concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di prove decisive per l'individuazione o la cattura dei concorrenti, la pena dell'ergastolo è sostituita da quella della reclusione da dodici a venti anni e le altre pene sono diminuite da un terzo a due terzi.

Quando ricorre una circostanza attenuante, alla pena prevista dal secondo comma è sostituita la reclusione da venti a ventiquattro anni; alla pena prevista dal terzo comma è sostituita la reclusione da ventiquattro a trenta anni. Se concorrono più circostanze attenuanti, la pena da applicare per effetto delle diminuzioni non può essere inferiore a dieci anni, nell'ipotesi prevista dal secondo comma, ed a quindici anni, nell'ipotesi prevista dal terzo comma.

I limiti di pena preveduti nel comma precedente possono essere superati allorché ricorrono le circostanze attenuanti di cui al quinto comma del presente articolo".

Tale reato si configura nel caso di sequestro di una persona allo scopo di perseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione. Il reato è aggravato nel caso in cui dal sequestro derivi la morte non voluta della persona sequestrata.

5.5. - TRATTAMENTO SANZIONATORIO PER LE FATTISPECIE DI CUI ALL'ART. 24-TER DEL DECRETO

1. In relazione alla commissione di taluno dei delitti di cui agli articoli 416, sesto comma, 416-bis, 416-ter e 630 del codice penale, ai delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonchè ai delitti previsti dall'articolo 74 del testo unico di cui al decreto del Presidente della Repubblica 9

ottobre 1990, n. 309, si applica la sanzione pecuniaria da quattrocento a mille quote.

2. In relazione alla commissione di taluno dei delitti di cui all'articolo 416 del codice penale, ad esclusione del sesto comma, ovvero di cui all'articolo 407, comma 2, lettera a), numero 5), del codice di procedura penale, si applica la sanzione pecuniaria da trecento a ottocento quote.

3. Nei casi di condanna per uno dei delitti indicati nei superiori punti 1 e 2, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2 del Decreto, per una durata non inferiore ad un anno.

4. Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati nei superiori punti 1 e 2, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'articolo 16, comma 3 del Decreto.

6. – ATTIVITA' SENSIBILI A RISCHIO REATO, PRESIDI DI CONTROLLO E PRESCRIZIONI SPECIFICHE

L'inserimento, nell'ambito del D.Lgs. 231/2001, dei reati di criminalità organizzata trova fondamento nella Decisione quadro 2008/841/GAI del Consiglio Europeo del 24 ottobre 2008, relativa alla lotta contro la criminalità organizzata, avente come obiettivo il riavvicinamento del diritto penale sostanziale degli Stati membri dell'Unione Europea per il contrasto comune al crimine organizzato e richiamante anche l'obbligo per gli Stati dell'UE di prevedere una responsabilità per le persone giuridiche in relazione ai delitti associativi.

I reati considerati presuppongono condotte lesive dell'ordine pubblico, inteso come buon assetto e regolare andamento del vivere civile, tendendo alla protezione di beni e valori essenziali alla pacifica convivenza associata ed all'ordinato funzionamento dell'ordinamento democratico.

IN PARTICOLARE, IL DELITTO DI ASSOCIAZIONE PER DELINQUERE (ART. 416 C.P.) SI CARATTERIZZA PER LA PRESENZA DEI SEGUENTI ELEMENTI:

a) esistenza di un vincolo associativo tra almeno tre soggetti, tendenzialmente permanente, o comunque stabile, destinato a durare anche oltre la realizzazione dei delitti concretamente programmati dall'associazione;

b) esistenza di un programma criminoso (ovvero volto alla realizzazione di una serie di delitti, c.d. "delitti fine") a carattere indeterminato, per quanto concerne il numero, le modalità, i tempi, gli obiettivi dei delitti programmati (che possono anche essere della stessa specie);

c) esistenza di una struttura organizzativa, sia pur minima, che sia idonea ed adeguata a realizzare gli obiettivi criminosi presi di mira.

Tale struttura organizzativa, pur potendo anche essere preesistente alla ideazione criminosa e già adibita a finalità lecite, deve tuttavia distinguersi dalla normale struttura organizzativa societaria;

d) elemento psicologico: coscienza e volontà di far parte di un impegno collettivo permanente e di svolgere i propri compiti al fine di compiere i delitti oggetto del programma criminoso.

Per la "valutazione del rischio con riferimento ai reati di criminalità organizzata, pur ritenendo che la normativa in esame preveda che l'analisi dei rischi riguardi esclusivamente i reati di cui all'art. 24 ter d.lgs. 231/2001, la Società ha voluto, per propria scelta prudenziale, estendere l'analisi anche alla possibile realizzazione di quei "delitti fine" alla cui commissione il delitto di associazione per delinquere potrebbe essere finalizzato in ambito aziendale. Delitti che più frequentemente sono contestati dagli organi inquirenti in ambito societario e per i quali il rischio di realizzazione può apparire astrattamente maggiore, anche alla luce dell'assetto organizzativo e di business della Società.

Tale approccio, certamente non previsto dalla lettera dell'art. 24 ter del Decreto (che si limita per l'appunto a richiamare, quale reato presupposto, il delitto di associazione per delinquere di cui all'art. 416 c.p., e non i singoli "delitti fine" alla realizzazione dei quali l'associazione criminosa è finalizzata) è parso essere, come

detto, il più prudente nell'ottica di una anticipata analisi dei rischi in ambito di criminalità organizzata.

Conseguentemente GETOPEN, ritiene che la prevenzione dei reati di cui all'art. 24 ter d.lgs. 231/2001 debba essere garantita dal rispetto della Carta dei Valori e Codice Etico, del Modello nel suo complesso, dall'insieme delle procedure oltre che dalla stretta osservanza delle disposizioni di legge.

Inoltre, GETOPEN ha individuato ulteriori protocolli e strumenti di controllo specificamente per i "delitti fine", come qui sotto identificati.

TALI "DELITTI FINE" SONO STATI INDIVIDUATI NEI SEGUENTI:

a) Truffa (art. 640 c.p.);

b) Reati in materia di imposte sui redditi e sul valore aggiunto:

- emissione di fatture o altri documenti per operazioni inesistenti (art. 8 d.lgs. 74/2000);
- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 d.lgs. 74/2000);
- dichiarazione fraudolenta mediante altri artifici/Dichiarazione Infedele/Omessa dichiarazione (artt. 3, 4 e 5 d.lgs. 74/2000);

c) Attività organizzate per il traffico illecito di rifiuti (art. 260 D.Lgs. 152/2006).

Inoltre, qualora i "delitti fine" rientrino tra le fattispecie di reato-presupposto del d.lgs. 231/01 già considerate nel presente Modello (ad es. reati contro la Pubblica Amministrazione, reati di riciclaggio), varranno i presidi e i sistemi di controllo ivi previsti.

CON RIFERIMENTO SPECIFICO AI REATI IN TEMA DI CRIMINALITÀ ORGANIZZATA, I PROCESSI SENSIBILI POSSONO ESSERE IDENTIFICATI NEI SEGUENTI:

- approvvigionamento di beni;
- approvvigionamento di servizi;
- assegnazione e gestione di incarichi di consulenza esterna;
- gestione rifiuti;
- gestione agenti;

- gestione marketing/comunicazione;
- dazione o ricezione di omaggi, donazioni, liberalità,
- sponsorizzazioni;
- gestione dei rapporti con l'amministrazione finanziaria;
- gestione rapporti infragruppo;
- selezione-assunzione/gestione (in termini di definizione politica retributiva, benefits, premi e gestione spese di rappresentanza) delle risorse umane;
- gestione beni aziendali (assegnazione e utilizzo).

In particolare, data la peculiarità della natura dei reati oggetto della presente Parte Speciale, le analisi hanno portato anche all'individuazione di fasi di attività nelle quali astrattamente si potrebbero manifestare le opportunità di configurazione degli stessi.

Eventuali integrazioni dei suddetti Processi Sensibili a rischio potranno essere richieste a cura dell'Organismo di Vigilanza della Società, al quale viene dato mandato di identificare le relative ipotesi e di definire gli opportuni provvedimenti operativi affinché l'Amministratore Unico di GETOPEN provveda a modificare e/o integrare conseguentemente il Modello.

CON RIFERIMENTO A CIASCUN PROCESSO SENSIBILE VENGONO DI SEGUITO ILLUSTRATE:

a) una descrizione sintetica del Processo Sensibile ed in particolare delle Fasi rilevanti ai fini della Parte Speciale in oggetto;

b) in forma sintetica, le modalità attraverso le quali alcuni dei reati di criminalità organizzata possono essere commessi nell'ambito dei Processi Sensibili alla luce della realtà aziendale di GETOPEN.

6.1. APPROVVIGIONAMENTO DI BENI E SERVIZI

DESCRIZIONE DEL PROCESSO SENSIBILE

Il processo si riferisce alle attività di approvvigionamento di beni sia di consumo che di investimento.

Le Fasi Rilevanti del Processo, ai fini della commissione dei reati di criminalità organizzata (art. 24 ter) sono le seguenti:

- Selezione/qualifica Fornitori

La valutazione e qualifica dei Fornitori avviene a cura della funzione Acquisti che si avvale, per il processo di qualifica a seconda delle tipologie di beni o servizi della funzione Qualità, Sicurezza e Ambiente o entrambe.

I FORNITORI DI GETOPEN S.R.L. POSSONO ESSERE DISTINTI IN DUE CATEGORIE:

1. Fornitori tradizionali;
2. Fornitori nuovi.

- FATTURAZIONE PASSIVA

Le fatture pervenute sono registrate e messe in pagamento a cura previo abbinamento con l'ordine di riferimento e controllo di conformità allo stesso.

Il pagamento è predisposto dal RAM o dalla Funzione Aziendale all'uopo preposta.

NELL'AMBITO DI TALE PROCESSO SENSIBILE SI POTREBBERO ASTRATTAMENTE REALIZZARE:

- **reato di associazione per delinquere di tipo mafioso**.

Tale fattispecie di reato potrebbe astrattamente realizzarsi qualora un esponente di GETOPEN S.r.l., affiliato ad una associazione di tipo mafioso, utilizzi la forza intimidatrice del vincolo associativo al fine di ottenere un vantaggio ingiusto nei rapporti con i Fornitori di beni e servizi della Società;

- **reato di concorso esterno in associazione di tipo mafioso.**

Tale fattispecie di reato potrebbe astrattamente realizzarsi qualora uno più soggetti apicali di GETOPEN agevolino l'attività di una associazione di tipo mafioso, stipulando contratti di fornitura con Fornitori affiliati alla predetta associazione, o comunque indicati da esponenti affiliati alla predetta associazione, al fine di rafforzare l'associazione stessa e ottenendone in cambio vantaggi diretti o indiretti grazie all'influenza esercitata sul territorio dall'associazione di tipo mafioso;

IL REATO DI ASSOCIAZIONE PER DELINQUERE FINALIZZATA A:

a) **dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti**.

Tale fattispecie di reato potrebbe astrattamente realizzarsi nell'ipotesi in cui uno o più dipendenti della Società ed esponenti di una società terza fornitrice di beni, si associno con la finalità di evadere le imposte sui redditi o sul valore aggiunto e si avvalgano nella formazione delle dichiarazioni dei redditi della Società, di fatture o altri documenti - emessi da parte della società fornitrice di beni – a fronte di operazioni in tutto o in parte non realmente effettuate o che indichino i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, registrando tali documenti nelle scritture contabili obbligatorie di GETOPEN S.r.l..

Accordo che potrebbe anche prevedere una ricevuta fittizia del pagamento da parte di GETOPEN ai Fornitori delle operazioni non realmente effettuate, oppure un rientro non contabilizzato di quanto realmente pagato;

b) dichiarazione infedele/dichiarazione fraudolenta mediante altri artifici.

Tale fattispecie di reato potrebbe astrattamente realizzarsi, al di fuori del caso previsto dall'art. 2 d.lgs. 74/2000, nell'ipotesi in cui alcuni dipendenti della Società si associno con la finalità di evadere le imposte sui redditi o sul valore aggiunto, e indichino nelle dichiarazioni dei redditi della Società elementi passivi fittizi attinenti gli approvvigionamenti o omettano elementi attivi, ostacolando il possibile accertamento attraverso una falsa rappresentazione di tali dati nelle scritture contabili obbligatorie di GETOPEN.

I DESTINATARI COINVOLTI IN TALE ATTIVITÀ DEVONO:

- assicurare che la scelta di tali soggetti (Fornitori, Consulenti, partner, procacciatori, Appaltatori, dipendenti) avvenga attraverso procedure di qualifica chiare, certe e non discriminanti confrontando, ove possibile, una rosa di potenziali offerte e assicurando l'orientamento verso Fornitori che diano le maggiori garanzie sotto l'aspetto etico, organizzativo, tecnico, finanziario;
- assicurare che il suddetto processo di qualifica preveda la raccolta di informazioni sull'onorabilità della controparte, anche ad esempio attraverso la richiesta

sistematica di documenti quali il certificato antimafia, il certificato del casellario giudiziale, ovvero in alternativa autodichiarazioni circa l'assenza di procedimenti penali, visura camerale in caso di società;

- qualora non fosse possibile ottenere la documentazione indicata al punto precedente accertare l'onorabilità delle controparti attraverso strumenti/documentazione alternativa;
- in caso di avvio di una nuova iniziativa commerciale/imprenditoriale, valutare l'opportunità di effettuare un'analisi preventiva del territorio al fine di comprenderne il livello di rischio di infiltrazione criminosa;
- assicurare che la formalizzazione del rapporto con soggetti terzi quali Fornitori, Appaltatori, partner, collaboratori e Consulenti avvenga a seguito di opportune verifiche sui requisiti di professionalità e onorabilità al fine di evitare qualsiasi implicazione in attività che, anche potenzialmente, possano favorire la commissione dei reati di cui all'art. 24 ter D.Lgs. 231/2001, e nel pieno rispetto delle procedure interne aziendali nonché del Modello e del Codice Etico;
- assicurare il monitoraggio periodico di tali soggetti attraverso un processo di riqualifica;
- assicurare la corretta archiviazione e conservazione di tutta la documentazione prodotta al fine di garantire la tracciabilità delle attività di verifica preventiva circa la sussistenza dei requisiti di onorabilità e di ri-qualifica periodica dei soggetti terzi.

6.2 Assegnazione e gestione di incarichi di consulenza esterna

Descrizione del Processo Sensibile

Il processo riguarda le attività svolte nell'ambito dell'assegnazione e gestione, anche indiretta, di incarichi di consulenze esterne. La tipologia di consulenza di cui si avvale la Società varia in relazione alle diverse aree di attività. Ciascuna area può essere richiedente e curare il rapporto con i Consulenti di cui necessita. Sulla base della prassi consolidata ed in relazione alle casistiche che si sono manifestate le consulenze possono essere raggruppate nelle seguenti categorie:

1. consulenze per l'ottenimento di finanziamenti/agevolazioni;

2. consulenze legali, fiscali;

3. consulenze in tema di ricerca e sviluppo;

4. consulenze di tipo finanziario;

5. consulenze nell'ambito dei sistemi informativi;

6. consulenza in materia ambientale.

LE FASI RILEVANTI DEL PROCESSO, AI FINI DELLA COMMISSIONE DEI REATI DI CRIMINALITÀ ORGANIZZATA (ART. 24 TER) SONO LE SEGUENTI:

- SELEZIONE/QUALIFICA CONSULENTI

La determinazione dei fabbisogni di servizi e la scelta del consulente è definita direttamente dall'organo delegato su impulso delle funzioni richiedenti.

- FATTURAZIONE PASSIVA

Le fatture sono ricevute dalla funzione aziendale preposta, la quale provvede a confrontare il documento contabile con i contratti relativi ai fornitori. Il pagamento è predisposto dal RAM o dalla Funzione Aziendale all'uopo preposta.

ESEMPLIFICAZIONE REATI REALIZZABILI NELL'AMBITO DEL PROCESSO

NELL'AMBITO DI TALE PROCESSO SENSIBILE SI POTREBBERO ASTRATTAMENTE REALIZZARE:

- **il reato di associazione per delinquere di tipo mafioso.**

Tale fattispecie di reato potrebbe astrattamente realizzarsi qualora un esponente di GETOPEN S.r.l., affiliato ad una associazione di tipo mafioso, utilizzi la forza intimidatrice del vincolo associativo al fine di ottenere un vantaggio ingiusto nei rapporti con un consulente della Società;

- **il reato di concorso esterno in associazione di tipo mafioso**.

Tale fattispecie di reato potrebbe astrattamente realizzarsi qualora soggetti in posizione apicale di GETOPEN agevolino l'attività di un'associazione di tipo mafioso, stipulando contratti di consulenza con Consulenti affiliati alla predetta associazione, o comunque indicati da esponenti affiliati alla predetta associazione, al fine di rafforzare l'associazione e ottenendone in cambio vantaggi diretti o indiretti grazie all'influenza esercitata sul territorio dall'associazione di tipo mafioso;

- **il reato di associazione per delinquere finalizzata a:**

a) Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti.

Tale fattispecie di reato potrebbe astrattamente realizzarsi nell'ipotesi in cui uno o più soggetti apicali di GETOPEN ed un consulente, si associno con la finalità di evadere le imposte sui redditi o sul valore aggiunto e si avvalgano nella formazione delle dichiarazioni dei redditi della Società, di fatture o altri documenti - emessi da parte del consulente – a fronte di servizi in tutto o in parte non realmente effettuati o che indichino i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, registrando tali documenti nelle scritture contabili obbligatorie di GETOPEN, che potrebbe anche prevedere una ricevuta fittizia del pagamento da parte di GETOPEN al consulente delle operazioni non realmente effettuate, oppure un rientro non contabilizzato di quanto realmente pagato;

b) Dichiarazione infedele/dichiarazione fraudolenta mediante altri artifici.

Tale fattispecie di reato potrebbe astrattamente realizzarsi, al di fuori del caso previsto dall'art. 2 D.Lgs. 74/2000, nell'ipotesi in cui alcuni esponenti di GETOPEN si associno con la finalità di evadere le imposte sui redditi o sul valore aggiunto, e indichino nelle dichiarazioni dei redditi della Società elementi passivi fittizi attinenti le consulenze, ostacolando il possibile accertamento attraverso una falsa rappresentazione nelle scritture contabili obbligatorie di GETOPEN S.R.L..

I DESTINATARI COINVOLTI IN TALE ATTIVITÀ DEVONO:

- assicurare che gli accordi con agenti siano formalizzati mediante redazione di un contratto/lettera d'incarico, debitamente autorizzato da soggetti muniti di idonei poteri e che riportino indicazione del compenso pattuito, del dettaglio della eventuale prestazione di servizi da effettuare e di eventuali del verbale da produrre in relazione all'attività svolta (nel caso in cui la prestazione stessa lo preveda);
- assicurare che gli accordi sovra specificati contengano apposita clausola relativa al d.lgs. 231/01 che preveda la risoluzione del contratto in relazione ad eventuali

inadempienze dei principi contenuti nella Carta dei Valori e Codice Etico e nel Modello di organizzazione, gestione e controllo aziendale;

- nei contratti con gli agenti, assicurare il sistematico inserimento di una clausola volta a garantire il rispetto delle regole di correttezza commerciale nell'instaurare il rapporto con il cliente e nella conclusione del contratto con il cliente finale;
- assicurare il sistematico inserimento, nei contratti conclusi con agenti, di clausole che prevedano l'impegno a consegnare a GETOPEN, nell'ambito della verifica di requisiti sull'onorabilità, certificato antimafia, autodichiarazione circa l'assenza di procedimenti penali, certificato del casellario giudiziale, visura camerale.

Qualora il terzo sia una persona giuridica, tale clausola dovrà prevedere l'impegno al rispetto dei requisiti di onorabilità anche con riferimento ai dipendenti/collaboratori di quest'ultima;

- assicurare il sistematico inserimento, nei contratti conclusi con agenti di clausole che prevedano l'impegno a comunicare senza indugio a GETOPEN il venir meno dei requisiti di onorabilità e affidabilità ovvero qualsiasi circostanza che possa influire sul mantenimento di tali requisiti;
- assicurare che i contratti con i clienti siano chiari, dettagliati, trasparenti e conclusi in coerenza con le politiche aziendali;
- assicurare un sistematico aggiornamento degli standard contrattuali coerentemente con le evoluzioni della normativa anche speciale vigente (ad esempio regolamentazioni ministeriali).

6.3 GESTIONE RIFIUTI

DESCRIZIONE DEL PROCESSO SENSIBILE

Il processo si riferisce alle attività svolte nell'ambito della gestione dei rifiuti.

Allo stato attuale GETOPEN non si avvale di soggetti terzi per la gestione dei rifiuti, ma qualora dovesse avvalersene, la selezione di soggetti terzi (smaltitori, trasportatori, Appaltatori) è a cura dell'Amministratore Unico.

Il rapporto con tali soggetti è formalizzato mediante regolare contratto firmato da soggetti muniti di adeguati poteri.

ESEMPLIFICAZIONE REATI REALIZZABILI NELL'AMBITO DEL PROCESSO.

NELL'AMBITO DI TALE PROCESSO SENSIBILE SI POTREBBERO ASTRATTAMENTE REALIZZARE:

- **il reato di associazione per delinquere finalizzata ad attività organizzate per il traffico illecito di rifiuti** nell'ipotesi in cui, ad esempio, l'Amministratore Unico, unitamente ad altro dipendente GETOPEN ed un soggetto incaricato dalla Società si associno per smaltire illecitamente quantitativi di rifiuti non dichiarati, a tariffe più basse rispetto a quelle previste per lo smaltimento regolare dei suddetti rifiuti, o si accordino per documentare quantitativi di tipologie di rifiuti diverse dalle reali, così che possano essere illecitamente smaltiti a tariffe più basse rispetto a quelle previste per lo smaltimento regolare dei suddetti rifiuti;
- **il reato di concorso esterno in associazione di tipo mafioso** che si potrebbe astrattamente realizzare qualora l'Amministratore Unico, al fine di agevolare l'attività di una associazione di tipo mafioso, al di fuori di qualsiasi procedura per la qualifica e selezione del fornitore, affidi l'incarico per lo smaltimento di rifiuti ad un soggetto affiliato (o comunque indicati da soggetti affiliati) alla predetta associazione, affinché l'associazione stessa si adoperi per far conseguire a GETOPEN S.r.l. un vantaggio consistente nella conclusione di importanti contratti commerciali.

I DESTINATARI COINVOLTI NELLE ATTIVITÀ DI GESTIONE RIFIUTI DEVONO:

- osservare le prescrizioni definite nelle procedure aziendali inerenti il Processo Sensibile in oggetto;
- assicurare la scelta delle controparti contrattuali (quali smaltitori e gestori di rifiuti, autotrasportatori ecc.) in ossequio ai principi stabiliti dalla presente procedura speciale e la formalizzazione dei rapporti con le controparti contrattuali in osservanza ai medesimi principi;

- nei contratti concernenti la gestione e lo smaltimento di rifiuti, prevedere la facoltà per GETOPEN di effettuare verifiche/audit specifici circa la classificazione/gestione/smaltimento dei rifiuti stessi.

6.4. GESTIONE AGENTI E DEL RELATIVO PROCESSO DI VENDITA

DESCRIZIONE DEL PROCESSO SENSIBILE

Il processo descrive le attività inerenti la gestione dei rapporti con gli agenti.

Le Fasi Rilevanti del Processo, ai fini della commissione dei reati di criminalità organizzata (art. 24 ter) sono le seguenti:

- MODALITÀ DI GESTIONE DEL CONTRATTO CON GLI AGENTI

Sulla base degli accordi stipulati tra la Società e gli agenti viene riconosciuta una provvigione in relazione alle vendite effettuate. Le linee guida commerciali, le modalità di instaurazione della relazione con il cliente nonché le modalità di proposta dell'offerta sono definite dall'Amministratore Unico;

- MODALITÀ DI CONCLUSIONE DEL CONTRATTO CON I CLIENTI

Gli agenti propongono l'offerta attraverso presentazione del prodotto, delle specifiche tecniche, dei listini, ecc. Il rapporto con il cliente viene formalizzato mediante formulazione di un ordine di acquisto.

Gli ordini, preventivamente approvati dall'area marketing e commerciale vengono trasmessi dall'agente.

ESEMPLIFICAZIONE REATI REALIZZABILI NELL'AMBITO DEL PROCESSO

Nell'ambito di tale Processo Sensibile si potrebbero astrattamente realizzare:

- **il reato di associazione per delinquere di tipo mafioso**

Tale fattispecie di reato potrebbe astrattamente realizzarsi qualora un soggetto in posizione apicale di GETOPEN S.r.l. stipuli contratti di agenzia con agenti affiliati ad un'associazione di tipo mafioso, o comunque indicati da esponenti affiliati alla predetta associazione, ottenendone in cambio vantaggi diretti o indiretti per GETOPEN, grazie all'influenza esercitata sul territorio dall'associazione di tipo mafioso;

- **il reato di concorso esterno in associazione di tipo mafioso**

Tale fattispecie di reato potrebbe astrattamente realizzarsi qualora un soggetto in posizione apicale della Società, al fine di agevolare l'attività di una associazione di tipo mafioso, concluda un contratto di agenzia con un agente affiliato a detta associazione, allo scopo di sfruttarne la forza di intimidazione e la condizione di assoggettamento che ne deriva per ottenere la conclusione di contratti; il reato di

ASSOCIAZIONE PER DELINQUERE FINALIZZATA A:

a) Truffa

Tale fattispecie di reato potrebbe astrattamente realizzarsi qualora due esponenti di GETOPEN ed il singolo agente si associno per porre in essere stabilmente una serie di condotte fraudolente configuranti artifici e raggiri idonei ad indurre in errore il cliente finale sul reale contenuto della prestazione o sul corrispettivo contrattualmente pattuito;

b) Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti

Tale fattispecie di reato potrebbe astrattamente realizzarsi nell'ipotesi in cui uno o più soggetti apicali di GETOPEN ed un agente, si associno con la finalità di evadere le imposte sui redditi o sul valore aggiunto e si avvalgano nella formazione delle dichiarazioni dei redditi della Società, di fatture o altri documenti – emessi da parte dell'agente – a fronte di prestazioni in tutto o in parte non realmente effettuate o che indichino i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, registrando tali documenti nelle scritture contabili obbligatorie di GETOPEN S.R.L..

Accordo che potrebbe anche prevedere una ricevuta fittizia del pagamento da parte di GETOPEN all'agente delle operazioni non realmente effettuate, oppure un rientro non contabilizzato di quanto realmente pagato.

6.5 GESTIONE MARKETING/COMUNICAZIONE

DESCRIZIONE DEL PROCESSO SENSIBILE

Il processo in esame si riferisce alla gestione delle attività di marketing/comunicazione.

La gestione dell'intero processo è riconducibile principalmente al Responsabile Marketing e Comunicazione.

AI FINI DELLA COMMISSIONE DEI REATI DI CRIMINALITÀ ORGANIZZATA (ART. 24 TER) RILEVA LA SEGUENTE FASE:

- Selezione/qualifica soggetti terzi (Fornitori, Consulenti, agenzie pubblicitarie, studi di grafica, media planner, ecc.)

Per lo sviluppo e la realizzazione delle attività di marketing all'interno delle quali esiste l'ambito della comunicazione, GETOPEN si avvale di soggetti specializzati.

Tipicamente GETOPEN si avvale di soggetti aventi requisiti tecnici e di professionalità.

La selezione avviene a cura dell'Amministratore Unico, sulla base delle competenze richieste in merito alla specifica campagna pubblicitaria/promozionale che GETOPEN intende sviluppare/realizzare.

ESEMPLIFICAZIONE REATI REALIZZABILI NELL'AMBITO DEL PROCESSO.

NELL'AMBITO DI TALE PROCESSO SENSIBILE SI POTREBBERO ASTRATTAMENTE REALIZZARE:

- **il reato di associazione per delinquere finalizzato alla truffa** qualora due esponenti della Società e l'agenzia pubblicitaria incaricata di realizzare delle campagne pubblicitarie si associno per realizzare e diffondere messaggi pubblicitari ingannevoli al fine di indurre in errore il cliente finale sulle reali qualità del prodotto da promuovere;
- **il reato di concorso esterno in associazione di tipo mafioso** che potrebbe astrattamente realizzarsi qualora un soggetto apicale di GETOPEN affidi un incarico pubblicitario a un'agenzia affiliata ad una associazione di tipo mafioso, al fine di agevolare le attività di tale associazione ed ottenere in cambio un vantaggio quale ad esempio lo sfruttamento della forza di intimidazione e la condizione di assoggettamento della stessa per ottenere la conclusione di contratti.

6.6 DAZIONE O RICEZIONE DI OMAGGI, DONAZIONI, LIBERALITÀ, SPONSORIZZAZIONI

DESCRIZIONE DEL PROCESSO SENSIBILE

Il processo in esame è riconducibile ai seguenti aspetti:

A. gestione degli omaggi, regali o altre utilità;

B. gestione elargizioni liberali;

C. gestione sponsorizzazioni di eventi.

ESEMPLIFICAZIONE REATI REALIZZABILI NELL'AMBITO DEL PROCESSO

NELL'AMBITO DI TALE PROCESSO SENSIBILE SI POTREBBERO ASTRATTAMENTE REALIZZARE:

- **il reato di concorso esterno in associazione di tipo mafioso** qualora un responsabile di funzione di GETOPEN, al fine di agevolare l'attività di una associazione di tipo mafioso, concluda un contratto per la sponsorizzazione di un ente, apparentemente senza fine di lucro ma affiliato a detta associazione, allo scopo di avere in cambio dei vantaggi ottenuti con la forza di intimidazione dell'associazione mafiosa.

I DESTINATARI COINVOLTI NELLE ATTIVITÀ DI DAZIONE O RICEZIONE DI OMAGGI, DONAZIONI, LIBERALITÀ, SPONSORIZZAZIONI, DEVONO:

- effettuare tutte le attività inerenti il Processo Sensibile in questione in ossequio alle indicazioni contenute all'interno delle procedure aziendali in materia;
- verificare preliminarmente l'onorabilità dei soggetti, enti, associazioni, destinatari di donazioni e atti di liberalità, nonché di sponsor, mediante la raccolta di informazioni preliminari e/o richiesta di documentazione attestante l'esistenza dei requisiti di onorabilità in capo agli stessi;
- garantire che il valore, la natura e lo scopo del regalo/liberalità abbiano chiari scopi umanitari, di beneficienza, culturali, artistici e di ricerca scientifica e siano considerati legali ed eticamente corretti;
- assicurare che gli accordi di sponsorizzazione siano formalizzati, ove possibile, mediante redazione di un contratto/lettera d'incarico, siano debitamente autorizzati da soggetti muniti di idonei poteri e riportino indicazione del compenso pattuito, del dettaglio della prestazione da effettuare e di eventuali deliverable da produrre relativi all'attività svolta (es. esposizione del logo aziendale);

- assicurare che ogni accordo di sponsorizzazione contenga apposita clausola relativa al d.lgs. 231/01 che preveda la risoluzione del contratto in relazione ad eventuali inadempienze dei principi contenuti nel Codice Etico e nel Modello.

6.7 GESTIONE DEI RAPPORTI CON L'AMMINISTRAZIONE FINANZIARIA

DESCRIZIONE DEL PROCESSO SENSIBILE

Il processo in esame include le attività inerenti alla gestione dei rapporti con l'Amministrazione Finanziaria in merito alla gestione degli adempimenti e delle scadenze previste per il rispetto della normativa finanziaria vigente e volte, inoltre, ad offrire il necessario supporto ad eventuali verifiche ispettive da parte delle Autorità.

La funzione responsabile della predisposizione del Bilancio trasmette tutta la documentazione necessaria allo studio fiscale incaricato della redazione del Bilancio d'esercizio.

ESEMPLIFICAZIONE REATI REALIZZABILI NELL'AMBITO DEL PROCESSO

Nell'ambito di tale Processo Sensibile si potrebbero astrattamente realizzare:

- **il reato di associazione per delinquere finalizzata alla dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti** nell'ipotesi in cui due esponenti di GETOPEN, e un rappresentante di una società terza, si associno allo scopo di utilizzare delle fatture emesse per operazioni inesistenti da parte di quest'ultima nella formazione delle dichiarazioni dei redditi di GETOPEN, con la finalità di evadere le imposte sui redditi o sul valore aggiunto;
- **il reato di associazione per delinquere finalizzata alla dichiarazione infedele/dichiarazione fraudolenta mediante altri artifici**, al di fuori del caso previsto dall'art. 2 d.lgs. 74/2000, nell'ipotesi in cui alcuni esponenti di GETOPEN, appartenenti anche a diverse funzioni della Società, si associno allo scopo di falsamente rappresentare nelle scritture contabili obbligatorie di GETOPEN degli elementi passivi fittizi da indicare poi nelle dichiarazioni dei redditi della Società al fine di evadere le imposte.

6.7. SELEZIONE - ASSUNZIONE/GESTIONE (IN TERMINI DI DEFINIZIONE POLITICA RETRIBUTIVA, BENEFITS, PREMI E GESTIONE SPESE DI RAPPRESENTANZA) DELLE RISORSE UMANE.

DESCRIZIONE DEL PROCESSO SENSIBILE

IL PROCESSO SI RIFERISCE ALLA GESTIONE DELLE ATTIVITÀ INERENTI L'INSERIMENTO NELL'ORGANIZZAZIONE AZIENDALE DI RISORSE UMANE: dalla segnalazione del fabbisogno, alla selezione del candidato, fino alla definizione della modalità di inserimento (inquadramento e livello retributivo).
Le attività sono gestite nell'ambito dal Responsabile Risorse Umane.

NELL'AMBITO DEL PROCESSO SENSIBILE, AI FINI DELLA POTENZIALE COMMISSIONE DEI REATI IN ESAME, È STATA INDIVIDUATA LA SEGUENTE FASE RILEVANTE:

- SELEZIONE DELLE RISORSE

L'individuazione dei potenziali candidati avviene analisi di auto-candidature, società di ricerca, inserzioni, ecc. La lista dei candidati viene stilata a cura dell'ufficio risorse umane e della funzione richiedente. Per la valutazione dei candidati sono organizzati colloqui con il Responsabile delle risorse umane e con l'Amministratore Unico, nonché con un colloquio tecnico al fine di vagliare le competenze della risorsa.

LA VALUTAZIONE DEI CANDIDATI CONSISTE PRINCIPALMENTE NELL'ANALISI DEI SEGUENTI ASPETTI:

- curriculum vitae;
- valutazione della personalità e della motivazione;
- valutazione del profilo professionale rispetto alla posizione e all'ambiente di lavoro (confronto tra le caratteristiche del candidato e le caratteristiche richieste dalla posizione).

ESEMPLIFICAZIONE REATI REALIZZABILI NELL'AMBITO DEL PROCESSO.

NELL'AMBITO DI TALE PROCESSO SENSIBILE SI POTREBBERO ASTRATTAMENTE REALIZZARE:

- **il reato di associazione per delinquere di tipo mafioso** qualora GETOPEN assuma consapevolmente un dipendente affiliato ad una associazione di tipo mafioso, allo scopo di utilizzare la forza intimidatrice del vincolo associativo ed ottenere dei vantaggi consistenti ad esempio nella conclusione di contratti in favore della Società;

- **il reato di concorso esterno in associazione di tipo mafioso** che potrebbe astrattamente realizzarsi qualora un soggetto in posizione apicale della Società, al fine di agevolare l'attività di un'associazione di tipo mafioso, scegliesse di dare incarico ad una società esterna di selezione del personale.

I DESTINATARI COINVOLTI NELLE ATTIVITÀ DI SELEZIONE, ASSUNZIONE E GESTIONE DEL PERSONALE, DEVONO:

- assicurare che la selezione del personale avvenga sulla base di principi che garantiscano una valutazione dei candidati effettuata nel rispetto dei principi sanciti nella Carta dei Valori e Codice Etico e che sia garantita la tracciabilità del processo di selezione mediante l'utilizzo di apposita documentazione nelle diverse fasi del processo;
- prima di formalizzare l'assunzione di una risorsa selezionata, verificare la sussistenza dei requisiti di onorabilità in capo alla stessa, mediante la richiesta di autodichiarazione circa l'assenza di procedimenti penali pendenti ovvero certificato penale generale o certificato del casellario giudiziale.

6.8. GESTIONE BENI AZIENDALI (ASSEGNAZIONE E UTILIZZO)

DESCRIZIONE PROCESSO SENSIBILE

Il processo in esame si riferisce alla gestione dei beni aziendali quali ad esempio PC, telefonini, auto aziendali, e in particolare alle attività di assegnazione e utilizzo degli stessi.

DESCRIZIONE DELLA FASE RILEVANTE DEL PROCESSO SENSIBILE

NELL'AMBITO DEL PROCESSO SENSIBILE, LA FASE RILEVANTE AI FINI DELLA POTENZIALE COMMISSIONE DEI REATI IN ESAME È LA SEGUENTE:

- Assegnazione e gestione dei beni aziendali

Sulla base del tipo di inquadramento della risorsa, il Responsabile Risorse Umane provvede a comunicare con comunicazione scritta i beni aziendali da assegnare, indicando, per quanto riguarda il PC, la tipologia di profilazione dell'utenza.

ESEMPLIFICAZIONE REATI REALIZZABILI NELL'AMBITO DEL PROCESSO

Nell'ambito di tale Processo Sensibile si potrebbe astrattamente realizzare:

- **il reato di concorso esterno in associazione di tipo mafioso** qualora un dipendente della Società, al fine di agevolare l'attività di una associazione di tipo mafioso, garantisca a tale associazione l'utilizzo di macchine aziendali per lo spostamento dei propri affiliati, in cambio di indebiti vantaggi ottenuti con la forza di intimidazione dell'associazione mafiosa.

I DESTINATARI COINVOLTI NELLE ATTIVITÀ DI ASSEGNAZIONE BENI AZIENDALI DEVONO:

- gestire le attività di assegnazione dei beni aziendali in ossequio alle policy/procedure aziendali in materia;
- astenersi dall'utilizzare i beni aziendali assegnati in proprio favore in modo improprio, contrario alla legge e/o alle policy/procedure aziendali in materia;
- selezionare i Fornitori di beni in osservanza alle regole previste dalla presente procedura.

7 PRINCIPI GENERALI DI COMPORTAMENTO E REGOLE DI CONDOTTA

Al fine di prevenire i reati sopra enunciati, tutti i Destinatari devono rispettare, oltre i principi di comportamento già previsti ed espressi nel Codice Etico, anche quelli riportati nei documenti organizzativi adottati dalla Società, nonché tenere comportamenti conformi a quanto previsto dalle vigenti norme di legge. Inoltre, i Destinatari del Modello, competenti per le attività oggetto di regolamentazione della presente Parte Speciale, sono tenuti ad osservare i seguenti principi di comportamento:

- ottemperare alle norme in tema di trasparenza;
- garantire l'attuazione del principio di segregazione dei compiti e delle funzioni anche attraverso la predisposizione di specifiche procedure;
- garantire la tracciabilità e la documentabilità di tutte le operazioni effettuate, prevedendo specifici obblighi di archiviazione;
- garantire che le attività a rischio prevedano i necessari controlli gerarchici, che devono essere tracciati/documentati;

- garantire la piena collaborazione agli organi di controllo interni a GETOPEN, oltre che nell'ambito di eventuali indagini/accertamenti da parte di organi esterni;
- garantire la corretta applicazione del Sistema disciplinare, in caso di mancato rispetto dei principi e dei protocolli contenuti nel Modello;

In generale, è fatto divieto ai Destinatari del Modello di porre in essere comportamenti che possano rientrare, anche potenzialmente, nelle fattispecie di reato richiamate dall'art. 24-ter del d.lgs. 231/2001, ovvero di collaborare o dare causa alla relativa realizzazione.

DUNQUE, NELL'AMBITO DEI CITATI COMPORTAMENTI È IN PARTICOLARE FATTO OBBLIGO DI:

- astenersi dal porre in essere azioni dilatorie od ostruzionistiche (espressa opposizione, rifiuti pretestuosi, ritardi nella messa a disposizione dei documenti) al fine di ostacolare, rallentare o fuorviare le attività di vigilanza e controllo svolte dai soggetti a ciò preposti;
- fornire la massima collaborazione nello svolgimento di eventuali indagini e iniziative da parte degli Organi sociali, o, più in generale, da qualsiasi organo/ente ispettivo, finalizzate a rilevare e combattere condotte illecite in relazione alle ipotesi del reato associativo considerato;
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali in generale ed, in particolare, in materia di selezione dei fornitori, di tenuta della contabilità aziendale e di redazione del bilancio di esercizio;
- qualunque sia la procedura applicata ai fini delle acquisizioni di beni e servizi o esecuzione di lavori, a costo GETOPEN o a rimborso, basare la scelta dei fornitori sempre su criteri di massima oggettività e trasparenza;
- non sottostare a richieste di qualsiasi tipo, e da chiunque provenienti, che siano contrarie alla legge, impegnandosi a darne tempestiva informazione al proprio superiore gerarchico (o al soggetto al medesimo sovraordinato

qualora la richiesta provenga dal superiore gerarchico) e all'OdV anche attraverso il sistema di whistleblowing;

- informare immediatamente le Autorità di Polizia qualora si verifichino attentati ai beni aziendali o siano rivolte minacce, fornendo tutte le informazioni necessarie per la ricostruzione del fatto denunciato;
- operare con soggetti terzi solo dopo aver accuratamente verificato la sussistenza dei requisiti di onorabilità e professionalità, in ottemperanza alle norme di legge vigenti e nel rispetto del Sistema antiriciclaggio adottato dalla Società;
- rispettare le regole del Codice Etico adottato dalla Società e le procedure o modalità operative aziendali.
- Garantire il rispetto dello Statuto e delle norme di legge applicabili nelle operazioni societarie;
- Interdire l'ingresso nella compagine societaria di soggetti (sia essi persone fisiche che giuridiche) dei quali sia conosciuta o sospetta l'appartenenza ad operazioni criminali o comunque operanti al di fuori della liceità quali, a titolo meramente esemplificativo ma non esaustivo, persone legate alla camorra, alla mafia, al traffico di sostanze stupefacenti, all'usura, al riciclaggio ecc.;
- Non utilizzare strumenti e conti anonimi o contanti per il compimento di operazioni di trasferimento di importi rilevanti;
- Rispettare tutti i requisiti relativi alla selezione dei fornitori, con particolare attenzione all'incensuratezza degli stessi e alla valutazione preventiva in ordine congruità dei prezzi richiesti rispetto ai valori di mercato;
- Divieto di prestare qualsivoglia forma di collaborazione o anche solo semplice contatto con soggetti colpiti o indiziati da provvedimenti giudiziari legati alla criminalità organizzata;
- Divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti effettivi e/o potenziali che possano, in maniera diretta ed indiretta, favorire le condizioni per reati di criminalità organizzata;

- Divieto di porre in essere qualsiasi situazione e/o tenere qualsiasi comportamento in conflitto di interessi con la Pubblica Sicurezza;

IN PARTICOLARE È FATTO DIVIETO DI:

- Promuovere, costituire, organizzare, dirigere partecipare ovvero finanziare in alcuna forma le associazioni di cui agli artt. 416 e 416 bis c.p.;
- Effettuare donazioni o altra forma di erogazione di fondi, anche indirette, nei confronti di simili associazioni;
- Fornire supporto logistico e/o qualsivoglia altro tipo a persone che partecipano alle predette associazioni;
- Stipulare qualsiasi tipo di contratto o avere rapporti commerciali, di collaborazione o di diverso tipo con controparti che abbiano precedenti penali o carichi pendenti noti alla Società in materia di reati di criminalità organizzata, ovvero dei quali si presume il vincolo associativo e la finalità criminale, anche se non si ha la certezza tanto del vincolo quanto dello scopo illecito, purchè si disponga di elementi sufficienti a farne desumere l'esistenza e ciononostante non si desista dall'instaurazione dei predetti rapporti.

8 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO

I Destinatari devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposto su apposita piattaforma informatica – tutta la documentazione necessaria.

I COMPITI DELL'ORGANISMO DI VIGILANZA IN RELAZIONE ALL'OSSERVANZA DEL MODELLO PER QUANTO CONCERNE I REATI DELLA PRESENTE PARTE SPECIALE SONO:

▪ proporre aggiornamenti alle istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle Aree a rischio;

▪ verificare il rispetto delle procedure contenute nel Modello;

▪ esaminare le eventuali segnalazioni di presunte violazioni del Modello ed operare gli accertamenti ritenuti necessari od opportuni.

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui alla presente Parte Speciale. Tali controlli sono diretti a verificare la corretta applicazione dei principi e delle regole generali di comportamento del presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

INOLTRE, I COMPITI DELL'ORGANISMO DI VIGILANZA IN RELAZIONE ALL'OSSERVANZA DEL MODELLO PER QUANTO CONCERNE I REATI DI CUI ALLA PRESENTE PARTE SPECIALE SONO:

▪proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati contemplati nella presente Parte Speciale;

▪ monitorare sul rispetto delle procedure interne per la prevenzione dei suddetti reati;

▪ esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

GETOPEN SRL
Energy Saving Company
Via Cesare Vivante 9 – 95123 CATANIA
Part. IVA 05012480876 – R.E.A. N. 336696

ALLEGATO

ELENCO ALLEGATI

ALLEGATO 1: Codice Etico

ALLEGATO 2: Clausola contrattuale

ALLEGATO 3: Elenco reati sanzionati dal Decreto

ALLEGATO 4: Composizione dell'Organismo di Vigilanza

ALLEGATO 5: Costituzione, compensi, cause di (in)eleggibilità, decadenza e sospensione dei componenti dell'Organismo di Vigilanza

ALLEGATO 6: Procedura WHISTLEBLOWING

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

GETOPEN SRL
Energy Saving Company
Via Cesare Vivante 9 – 95123 CATANIA
Part. IVA 05012480876 – R.E.A. N. 336696

ALLEGATO - 1 -

CODICE ETICO

Approvato con determina dell'Amministratore Unico del 20.03.2024

SOMMARIO

PREMESSA

GetOpen S.r.l. (in seguito "Società") è una azienda che si occupa: **1)** dello svolgimento di studi, ricerche, indagini e fornitura di servizi reali, finalizzati alla progettazione di nuove tecnologie e sistemi integrati per lo sviluppo sostenibile, la mitigazione dell'impatto dei cambiamenti climatici, la riduzione ed il contenimento dei consumi energetici e delle emissioni di inquinanti; **2)** dell'offerta di servizi energetici integrati per la realizzazione e gestione di iniziative di sviluppo sostenibile.

GetOpen S.r.l. assicura e promuove i principi di responsabilità sociale d'impresa, inspirandosi, nello svolgimento delle proprie attività economiche, al principio di sostenibilità sociale, in virtù del quale le esigenze di efficienza economica e di legittimo profitto devono essere coerenti con la tutela ambientale, con lo sviluppo sociale e con il bene comune.

La Società adotta il presente Codice Etico (in seguito il "Codice") al fine di formalizzare e diffondere i propri principi, valori ed impegni aziendali, sui quali si fonda ogni scelta ed azione posta in essere dalla Società.

Invero, mediante il presente Codice, la Società mira ad orientare comportamenti coerenti con i più alti standard etici internazionali e nazionali nello svolgimento delle sue attività e nella gestione d'impresa. Il Codice include e riconosce come fondamentali anche i principi di sostenibilità per orientare la strategia aziendale ed avere un impatto positivo sul futuro del pianeta, nella consapevolezza che la considerazione delle istanze sociali e ambientali contribuiscono anche a minimizzare l'esposizione ai rischi ed a rafforzare la reputazione della medesima Società.

Ambito di applicazione e soggetti destinatari del Codice Etico

La Società è impegnata a diffondere i valori ed i principi non solo a tutto il personale dipendente, ma anche a tutti i collaboratori ed a qualunque terza parte interessata da rapporti contrattuali, anche occasionali o soltanto temporanei. Tali soggetti vengono identificati come "Soggetti Destinatari" del Codice Etico e sono considerati tali, quando operano nell'interesse, per conto ed in favore di GetOpen sia in Italia che all'Estero. Ai soggetti Destinatari, la Società richiede di conoscere e rispettare i principi ed i contenuti del Codice e di applicarli nell'espletamento delle attività poste in essere.

LA VISION DI GETOPEN S.R.L.

GetOpen è consapevole che l'autorevolezza di un'azienda si riconosca, oltre che dalla competenza e professionalità dei propri dipendenti e collaboratori, anche dalla qualità dei servizi resi ai clienti, nonchè dall'attenzione che la Società pone alle esigenze dell'intera collettività.

I principi che ispirano il lavoro di GetOpen vengono, infatti, indicati nel presente Codice Etico, nella convinzione che l'affidabilità di una società si fonda sul rispetto delle norme vigenti, nonché sull'esperienza, la competenza e la professionalità del proprio personale e dei collaboratori che operano nell'interesse della Società.

Il Codice Etico di GetOpen rappresenta, quindi, un elemento distintivo ed identificativo nei confronti del mercato e dei terzi, la cui conoscenza e condivisione è richiesta a tutti coloro che operano nella Società o che con essa collaborano.

Infatti, il Codice Etico è la carta dei diritti e dei doveri fondamentali attraverso i quali la GetOpen S.r.l. chiarisce le proprie responsabilità etiche e sociali sia verso l'interno che verso l'esterno. Esso risponde all'esigenza di chiarire su quali criteri la Società intende bilanciare gli interessi degli stakeholder interni ed esterni. Invero, il presente Codice Etico offre la possibilità a tutti gli interessati di poter verificare se le loro aspettative e le loro legittime pretese sono state considerate secondo equità, ponendo le basi per un accordo morale di cooperazione vantaggiosa per tutti.

1. PRINCIPI GENERALI

GetOpen presta la propria attività nel rispetto delle norme nazionali e sovranazionali, improntando la propria condotta al rispetto dei principi di legalità, imparzialità, correttezza, non discriminazione, riservatezza, valore delle risorse umane, rispetto delle

informazioni riservate, concorrenza leale, diligenza e correttezza, lealtà e salvaguardia dell'ambiente.

Tutti i Destinatari sono tenuti a conoscere il presente Codice Etico, segnalare eventuali criticità e contribuire alla sua effettiva e concreta applicazione.

1.1. LEGALITÀ

GetOpen S.r.l. opera nell'assoluto rispetto della legge, dei regolamenti, delle procedure interne e dei principi sanciti nel presente Codice Etico.

Tutti i Destinatari sono, pertanto, tenuti ad osservare ogni normativa applicabile e ad aggiornarsi costantemente sulle evoluzioni legislative, anche avvalendosi delle opportunità formative offerte da GetOpen S.r.l.

1.2 CORRETTEZZA

La correttezza e l'integrità morale sono un dovere indefettibile per tutti i Destinatari del presente Codice Etico.

I Destinatari sono tenuti a non instaurare alcun rapporto privilegiato con terzi, che sia frutto di sollecitazioni esterne finalizzate ad ottenere vantaggi impropri.

L'intrinseca convinzione di agire nell'interesse della Società non esonera i Destinatari dall'obbligo di osservare, puntualmente, le regole ed i principi del presente Codice Etico.

1.3 NON DISCRIMINAZIONE

Nei rapporti con i Collaboratori ed in particolare nella selezione e gestione del personale, nell'organizzazione lavorativa, nella scelta, selezione e gestione dei fornitori, nonché nei rapporti con gli Enti e le Istituzioni, GetOpen S.r.l. non pone in essere alcuna discriminazione concernente l'età, il sesso, la razza, gli orientamenti sessuali, lo stato di salute, le opinioni politiche e sindacali, la religione, la cultura e la nazionalità.

1.4 RISERVATEZZA

GetOpen S.r.l. si impegna ad assicurare la protezione e la riservatezza dei dati personali dei Dipendenti, Destinatari e dei Collaboratori, nel rispetto della normativa applicabile in materia di protezione dei dati personali.

Infatti, GetOpen S.r.l. tratta tutti i dati personali e sensibili dei Dipendenti, Destinatari e dei Collaboratori nel pieno del GDPR 2016/679.

I Dipendenti, i Destinatari e i Collaboratori sono previamente informati in ordine alla possibilità che la società può trattare i propri dati personali per ragioni strettamente connesse all'espletamento dell'attività lavorativa.

1.5 INFORMAZIONI DI PROPRIETÀ ESCLUSIVA

Preliminarmente, si precisa che i Dipendenti, i Collaborati e tutti i Destinatari del presente Codice Etico sono tenuti a non utilizzare informazioni riservate, apprese in ragione della propria attività lavorativa, per scopi estranei all'esercizio di tale attività e, comunque, ad agire sempre nel rispetto degli obblighi di riservatezza assunti da GetOpen S.r.l. nei confronti di tutti i terzi.

Per "informazioni di proprietà esclusiva" si intendono quelle di proprietà della GetOpen S.r.l..

Non tutte le "informazioni di proprietà esclusiva" della GetOpen S.r.l. sono informazioni riservate e potrebbero essere coperte da brevetti o altri diritti di proprietà intellettuale.

Tali informazioni comprendono piani gestionali, finanziari, commerciali e di assistenza connessa ai servizi e prodotti offerti; sono inoltre compresi i dati relativi al personale e alle retribuzioni.

Le informazioni di proprietà esclusiva comprendono anche i progetti, *Know-how* e processi tecnici e di produzione, piani commerciali e di produzione con i fornitori esterni e società partecipate e numerosi software e *data base* interni, oltre a tutto il materiale protetto da diritti d'autore di terzi (copyright).

1.6 DILIGENZA

Il rapporto tra GetOpen S.r.l. ed i propri Dipendenti e Collaboratori è fondato sulla reciproca fiducia.

Pertanto, i Dipendenti ed i Collaboratori sono tenuti ad operare per favorire gli interessi dell'azienda, nel rispetto dei valori di cui al presente Codice Etico.

I Destinatari devono astenersi da qualsiasi attività che possa confliggere con gli interessi di GetOpen S.r.l. rinunciando al perseguimento di interessi personali incompatibili con i legittimi interessi della Società.

Nei casi in cui si possa raffigurare la possibilità di sussistenza di un conflitto di interessi, i Destinatari sono tenuti a comunicarlo, senza alcun ritardo, al datore di lavoro, affinchè l'azienda possa valutare, ed eventualmente autorizzare, la predetta attività.

Nei casi di violazione, la Società adotterà ogni misura idonea a far cessare il conflitto di interessi, riservandosi di agire a propria tutela.

GetOpen S.r.l. potrà, altresì, adottare i provvedimenti disciplinari di cui al CCNL di riferimento, nonchè quelli di cui al proprio regolamento disciplinare, ciò nel caso in cui i comportamenti posti in essere siano in contrasto con l'etica aziendale puntualmente descritta nel presente Codice Etico e nelle procedure interne.

1.7 LEALTÀ

GetOpen S.r.l. ed i Destinatari si impegnano a realizzare una concorrenza leale, nel rispetto della normativa nazionale e comunitaria, nella consapevolezza che una concorrenza virtuosa costituisce un sano incentivo ai processi di innovazione e sviluppo, tutelando, allo stesso tempo, gli interessi dei consumatori e della collettività.

1.8 SALVAGUARDIA DELL'AMBIENTE

La tutela dell'ambiente è una delle dimensioni chiave dell'impegno di responsabilità assunto da GetOpen nell'esercizio della propria attività d'impresa.

GetOpen crede fermamente che possa esercitare un significativo impatto in termini di sostenibilità ambientale, in particolare nel contesto sociale e ambientale in cui è presente con la sua attività d'impresa, sia nel breve sia nel lungo periodo. Tale impatto è riconducibile sia al consumo di risorse e alla generazione di emissioni e rifiuti direttamente legati alla propria attività (impatti diretti), sia ad attività e comportamenti che non controlla direttamente, in quanto posti in essere da soggetti terzi con i quali si relaziona, ad esempio clienti e fornitori (impatti indiretti).

IN TALE OTTICA, GETOPEN ASSICURA:

- il pieno e sostanziale rispetto delle prescrizioni legislative in materia ambientale;
- la ricerca continua di soluzioni innovative ed efficaci in campo ambientale, anche tramite l'offerta di prodotti e servizi specifici alla clientela e di soluzioni per i propri fornitori;
- la diffusione di buone pratiche di responsabilità ambientale anche attraverso il puntuale rispetto dei principi internazionali in materia;
- l'apertura al dialogo e al confronto con tutti quegli interlocutori che rappresentano la "voce" dell'ambiente;
- l'utilizzo responsabile ed efficiente delle risorse;
- il consumo consapevole delle risorse necessarie per svolgere la propria attività, anche attraverso l'implementazione di un sistema di gestione ambientale e il progressivo miglioramento dell'efficienza energetica delle nostre attività;
- un monitoraggio dei dati ambientali e la sensibilizzazione delle persone che lavorano nella Società per assicurare un miglioramento continuo del comportamento assunto nei confronti dell'ambiente.

GetOpen S.r.l. si impegna, altresì, in ogni fase del suo agire: **1)** ad applicare criteri di cautela – il "Principio di Precauzione"– e un approccio preventivo nei riguardi dell'ambiente e della sua biodiversità; **2)** a promuovere iniziative per una maggiore responsabilità ambientale aziendale; **3)** a sviluppare l'impiego di mezzi e di tecnologie che

non solo non danneggino l'ambiente ma che migliorino la sostenibilità ambientale degli impianti nei quali GetOpen S.r.l. interviene con la propria attività di progettazione.
L'impegno di GetOpen S.r.l. rivolto a salvaguardare il pianeta ed il benessere delle generazioni presenti e future include anche il benessere degli animali.

2 RAPPORTI CON I DIPENDENTI E CON I COLLABORATORI

2.1 SELEZIONE DEL PERSONALE

La valutazione e la selezione del personale sono effettuati secondo correttezza e trasparenza, rispettando le pari opportunità, al fine di coniugare le esigenze di GetOpen, con i profili professionali, le ambizioni e le aspettative dei candidati.
Il personale assunto, anche mediante l'attuazione del presente Codice Etico, riceve un'informazione chiara e corretta circa ruoli, responsabilità, diritti e doveri delle parti.
Per GetOpen S.r.l. il rispetto dell'individualità e della dignità di ciascuna persona è il fondamento per lo sviluppo di un ambiente di lavoro stimolante e inclusivo.

PER LE CITATE RAGIONI, GETOPEN SI IMPEGNA A:

– adottare modalità di reclutamento e gestione fondate su equità e coerenza, allo scopo di prevenire favoritismi, abusi, molestie e discriminazioni di ogni tipo, garantendo processi di valutazione fondati sull'equità e sul merito, valorizzando la motivazione e lo sviluppo di carriera delle persone, nel rispetto delle diversità;
– garantire pari opportunità di sviluppo e di crescita professionale, di accesso ai percorsi formativi e alle iniziative di aggiornamento e di attribuzione dei ruoli, sin dalla fase di selezione delle candidature.

2.2 GESTIONE DEL PERSONALE

Il successo di GetOpen S.r.l. è il risultato del contributo professionale e umano delle persone che operano all'interno della Società. Per questo GetOpen promuove il rispetto delle persone e ne riconosce l'importanza, perseguendo la massima valorizzazione dell'individualità, del merito, del talento, delle competenze e della managerialità.
GetOpen si impegna, quotidianamente, a promuovere una cultura interna basata sul rispetto della dignità individuale, tutelare i diritti delle lavoratrici e dei lavoratori contrastare ogni forma – anche indiretta – di lavoro forzato o minorile e proteggere l'integrità fisica e morale di tutte le proprie persone, attraverso una gestione improntata al rispetto della personalità e professionalità di ciascuno, in un quadro di lealtà e fiducia reciproca.

PER QUESTO GETOPEN S.R.L. MIRA A:

– adottare iniziative atte a prevenire e contrastare qualsivoglia comportamento, espresso in forma fisica, verbale o non verbale, che offenda, prevarichi e leda la dignità umana, garantendo, laddove necessario, opportuna assistenza, supporto e massima riservatezza;

– garantire le libertà sindacali e il diritto di associazione in organismi rappresentativi delle persone di GetOpen S.r.l.;

– adottare misure di protezione complementari (come, ad esempio, la previdenza complementare);

– riconoscere a tutte le persone la possibilità di esprimere la propria individualità e creatività nel lavoro, valorizzando la diversità e le specificità di ogni individuo, come spinta all'innovazione e contributo essenziale alla crescita di GetOpen;

– porre la massima attenzione nella definizione degli obiettivi, favorendone la comprensione e la condivisione, al fine di promuovere comportamenti corretti e trasparenti nella relazione con gli stakeholder;

– presidiare sistemi incentivanti oggettivi e trasparenti, prevedendo obiettivi possibili e raggiungibili;

– valutare la prestazione di coloro che hanno ruoli di responsabilità tenendo conto anche del rispetto dei principi etici su cui si fonda la relazione con le persone;

– rendere più agevole il lavoro semplificando prodotti, procedure e forme di comunicazione;

– assicurare il diritto alla privacy e il rispetto dei dati personali e sensibili;

– promuovere la mobilità sostenibile favorendo, ove possibile, il ricorso a soluzioni di trasporto a minore impatto ambientale;

– promuovere politiche che agevolino l'equilibrio fra vita personale e professionale, favorendo forme di flessibilità e realizzando iniziative per conciliare impegni lavorativi e privati, nella consapevolezza che tale equilibrio è fondamentale nella ricerca del benessere di ogni persona.

2.3 TUTELA DELLA SALUTE E SICUREZZA

Le persone rappresentano la risorsa più importante per GetOpen S.r.l. e su questo principio si fonda la politica di salute e sicurezza posta in essere dalla società al fine di assicurare il benessere fisico e mentale del personale dipendente sul luogo di lavoro.

Per questo, in costante aderenza alle disposizioni di legge e tenuto conto dei migliori standard e linee guida internazionali per la gestione dei sistemi di prevenzione e promozione della salute, GetOpen S.r.l. si impegna a:

– sviluppare metodiche qualificate di analisi e valutazione volte a identificare e controllare le situazioni di rischio per la salute e la sicurezza nei luoghi di lavoro, sia in condizioni ordinarie sia a fronte di situazioni di crisi;
– adottare misure di prevenzione e protezione finalizzate al miglioramento del benessere delle persone, monitorandone nel tempo l'effettività ed efficacia;
– gestire i rischi residui attraverso la predisposizione di piani di emergenza e di intervento;
- porre in essere una puntuale attività di informazione e formazione di tutto il personale dipendente relativamente ai rischi presenti e alle misure di prevenzione e protezione da adottare.

2.4 VALORIZZAZIONE E PERCORSI FORMATIVI

GetOpen S.r.l. riconosce il ruolo strategico rivestito dal complesso delle competenze relazionali, intellettuali, organizzative e tecniche di ogni persona e ritiene quindi essenziale la valorizzazione e la motivazione come driver nelle relazioni.

PER QUESTO GETOPEN SI IMPEGNA A:

– presidiare l'evoluzione di percorsi formativi a supporto delle esigenze individuali orientati all'innovazione e al miglioramento costante del livello di competenza, per creare le condizioni ottimali affinché ciascuna persona sia in grado di interpretare al meglio il proprio ruolo e sviluppare la capacità di lavorare in squadra per contribuire al raggiungimento degli obiettivi d'impresa;
– perseguire l'eccellenza dei risultati sotto il profilo sia quantitativo sia qualitativo, attraverso azioni commerciali e politiche di budget indirizzate, pianificate e monitorate in coerenza con i principi etici del presente Codice e nel rispetto della professionalità e della dignità di ciascuna persona, nonché delle specificità del contesto territoriale in cui opera;
– adottare politiche gestionali e premianti in grado di riconoscere e valorizzare il contributo individuale e di gruppo al raggiungimento degli obiettivi;
– promuovere la partecipazione responsabile delle persone, supportandole sempre, anche in occasione di lunghe assenze e richiedendo loro di impegnarsi costantemente in modo attivo affinché si sentano coinvolte nel progetto di crescita di GetOpen S.r.l., attraverso il quale raggiungere anche la propria realizzazione professionale.

3 RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

Le Risorse umane di GetOpen S.r.l. devono conoscere e rispettare, ove applicabile, le linee guida emanate dalla Società con riferimento ai rapporti e agli adempimenti con la Pubblica Amministrazione, nonché le linee guida in materia di omaggi e liberalità. Tali linee guida devono essere applicate in tutti gli ambiti di attività di GetOpen ove ci si relazioni con Pubbliche Amministrazioni e loro rappresentanti.

IN PARTICOLARE:

- nelle richieste indirizzate alla Pubblica Amministrazione per l'ottenimento di provvedimenti relativi alle attività svolte dalle Società;
- in tutte le occasioni di contatto con incaricati di effettuare verifiche ispettive e sopralluoghi presso la sede di GetOpen, finalizzate alla verifica del rispetto di prescrizioni e/o di adempimenti di legge;
- in tutte le occasioni di contatto con Pubbliche Amministrazioni per ragioni istituzionali, commerciali o di fornitura;
- nell'adempiere ad obblighi o prescrizioni date dalla Pubblica Amministrazione.

GetOpen S.r.l. si comporta correttamente e con trasparenza nello svolgimento di trattative e rapporti negoziali con la Pubblica Amministrazione, così come nell'esecuzione di qualsiasi adempimento di legge
o prescrizione dettata dalla stessa.

I rapporti di GetOpen S.r.l. con i pubblici ufficiali (ivi inclusi gli impiegati pubblici - a prescindere se siano incaricati di pubblico servizio o meno - e concessionari di pubblico servizio) si basano sulla trasparenza, sulla lealtà e sulla correttezza.

GetOpen S.r.l. condanna ogni comportamento che possa costituire atto di corruzione anche nei confronti di soggetti privati. Qualunque tentativo di estorsione, concussione o induzione a dare utilità indebite da parte di un pubblico ufficiale o un incaricato di pubblico servizio deve essere segnalato senza indugio.

I Destinatari del Codice Etico devono comunicare i rapporti di affari o le attività economiche intraprese a titolo personale con pubblici ufficiali.

Alla luce di quanto sopra, nessun Destinatario può:

- cercare di influenzare impropriamente le decisioni delle Amministrazioni interessate, in particolare dei funzionari che trattano o decidono per conto delle stesse;
- offrire, promettere o concedere denaro, beni in natura, facilitazioni o altre utilità non dovuti, sotto qualsiasi forma e anche in modo indiretto, a qualunque soggetto (sia esso dirigente, funzionario o dipendente della Pubblica Amministrazione o soggetto privato incaricato di pubblico servizio, o a soggetti loro congiunti, affini, conviventi e soggetti ad

essi in qualche modo collegati), in vista del compimento di un atto d'ufficio o per influenzarne illecitamente una decisione che sia volta a promuovere o favorire gli interessi della Società, anche a seguito di illecite pressioni o di sollecitazione da parte del medesimo beneficiario. Alle Risorse umane è consentito offrire omaggi e cortesie di uso commerciale di modesto valore secondo quanto previsto dalla procedura "Omaggi e liberalità";

- inviare documenti falsi o artatamente formulati, attestare requisiti inesistenti o dare garanzie non rispondenti al vero;
- procurare indebitamente qualsiasi altro tipo di profitto (licenze, autorizzazioni, sgravi di oneri anche previdenziali ecc.) con mezzi che costituiscano artifici o raggiri (ad esempio: l'invio di documenti falsi o attestanti cose non vere);
- intraprendere attività economiche, conferire incarichi professionali, dare o promettere doni, denaro, o altri vantaggi, a pubblici ufficiali o impiegati pubblici coinvolti in procedimenti amministrativi che possono comportare vantaggi per GetOpen S.r.l.;
- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico della Pubblica Amministrazione o di terzi o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi, contenuti in uno dei suddetti sistemi;
- ricevere indebitamente contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo in qualunque modo denominate, concessi o erogati da parte delle Pubblica Amministrazione, tramite l'utilizzo o la presentazione di documenti falsi o mendaci, o mediante l'omissione di informazioni dovute;
- utilizzare contributi, sovvenzioni o finanziamenti destinati alla realizzazione di opere pubbliche o allo

svolgimento di attività di pubblico interesse, per scopi diversi da quelli per cui sono concessi;

- scambiare illegittimamente informazioni sulle offerte con i partecipanti ad eventuali gare o procedure ad evidenza pubblica.

Costituisce violazione della politica istituzionale di GetOpen S.r.l. adottare condotte che configurano il reato di corruzione anche nei Paesi esteri in cui tali condotte non fossero punite o altrimenti vietate.

In linea generale, i rapporti con la Pubblica Amministrazione per conto di GetOpen devono essere gestiti da soggetti delegati o comunque autorizzati.

GetOpen S.r.l. agisce nel rispetto della legge e favorisce, nei limiti delle proprie competenze, la corretta amministrazione della giustizia.

Nello svolgimento della propria attività, GetOpen opera in modo lecito e corretto collaborando con l'autorità giudiziaria, le forze dell'ordine e qualunque pubblico ufficiale che abbia poteri ispettivi e svolga indagini nei suoi confronti.

In previsione di un procedimento giudiziario, di un'indagine o di un'ispezione da parte della Pubblica Amministrazione o delle Autorità di Vigilanza, nessuno deve distruggere o alterare registrazioni, verbali,

scritture contabili e qualsiasi tipo di documento, mentire o fare dichiarazioni false alle autorità competenti.

Nessuno deve tentare di persuadere altri a fornire informazioni false o ingannevoli alle Autorità competenti.

Nessuno può intraprendere attività economiche, conferire incarichi professionali, dare o promettere doni, danaro o altri vantaggi a chi effettua gli accertamenti e le ispezioni, ovvero alle Autorità competenti.

4 RAPPORTI CON FORNITORI, CLIENTI, PARTNER E ALTRE CONTROPARTI CONTRATTUALI

GetOpen S.r.l. imposta i rapporti con Fornitori, Clienti e Partner esclusivamente sulla base di criteri di fiducia, qualità, competitività, professionalità e rispetto delle dinamiche di mercato.

In particolare, GetOpen S.r.l. si adopera per selezionare i Fornitori ed i Clienti sulla base di criteri di valutazione che includano, oltre alla qualità ed economicità dell'offerta, aspetti quali reputazione, affidabilità, professionalità, efficienza e sostenibilità, tali da permettere di impostare un solido e duraturo rapporto fiduciario. GetOpen evita accordi con fornitori di dubbia reputazione che possano non rispecchiare i valori espressi nel presente Codice Etico in linea con i principi del Global Compact promosso dall'ONU, quali il rispetto dell'ambiente, delle condizioni di lavoro, dei diritti umani e i principi di legalità, rispetto della concorrenza e lotta alla corruzione.

I medesimi principi sono adottati nella valutazione dei Partner, cui si richiede la condivisione dei valori del presente Codice Etico.

GetOpen S.r.l.si aspetta che i Fornitori, i Clienti e i Partner non ricevano alcuna indebita pressione ad effettuare prestazioni non previste contrattualmente.

Nel richiedere l'adesione al presente Codice Etico per quanto a loro applicabile, GetOpen S.r.l. si aspetta da Fornitori, Clienti, Partner e altri soggetti comportamenti conformi ai principi ivi contenuti. Comportamenti contrastanti possono essere considerati grave

inadempimento ai doveri di correttezza e buona fede nell'esecuzione del contratto con GetOpen, motivo di lesione del rapporto fiduciario e giusta causa di risoluzione del contratto stesso.

Nessun Destinatario del presente Codice Etico può promettere o concedere denaro, beni in natura, facilitazioni o altre utilità, direttamente o indirettamente e sotto qualunque forma, a qualsiasi individuo che rappresenti una controparte per GetOpen S.r.l. allo scopo di orientarne una decisione o di influenzare il compimento di atti o la conclusione di accordi commerciali o, in generale, per promuovere o favorire illecitamente gli interessi di GetOpen oppure per danneggiare scorrettamente un concorrente. Sono consentiti omaggi e cortesie di uso commerciale di modesto valore secondo quanto stabilito dalla procedura "Omaggi e liberalità".

5 GESTIONE DELL'IMPRESA

5.1 CONTROLLI INTERNI

È politica di GetOpen diffondere a tutti i livelli una cultura orientata all'esercizio del controllo, caratterizzata dalla consapevolezza dell'esistenza dei controlli interni e dalla coscienza del contributo positivo che questi danno al miglioramento dell'efficienza.

Per controlli interni si intendono tutti gli strumenti necessari o utili a indirizzare, gestire e verificare le attività della Società con l'obiettivo di assicurare l'attendibilità, l'accuratezza, l'affidabilità e la tempestività delle informazioni fornite agli organi sociali e al mercato, la salvaguardia del patrimonio aziendale, l'efficacia dei processi aziendali, il rispetto delle leggi e dei regolamenti nonché dello statuto e procedure interne.

La responsabilità di realizzare un sistema di controllo interno e di gestione dei rischi efficace riguarda, a

vario titolo, ogni livello della struttura organizzativa; conseguentemente gli amministratori, i componenti degli organi di controllo e tutte le Risorse umane, ciascuno nell'ambito della propria funzione, deve contribuire alla definizione, funzionamento e monitoraggio del sistema di controllo interno e di gestione dei rischi.

Nell'ambito delle loro competenze, i responsabili di unità organizzative sono tenuti a essere partecipi del sistema di controllo interno e gestione dei rischi aziendale e a farne partecipi i propri collaboratori.

Il rispetto delle prescrizioni del presente Codice Etico è affidato alla prudente, ragionevole ed attenta sorveglianza di ciascuno dei Destinatari, nell'ambito dei rispettivi ruoli e funzioni all'interno dell'azienda.

Tutti i Destinatari sono invitati a riportare ai loro diretti superiori i fatti e le circostanze potenzialmente in contrasto con i principi e le prescrizioni del presente Codice.

Il management di GetOpen S.r.l. e gli organi all'uopo preposti adottano ogni necessaria misura per porre fine alle violazioni, potendo ricorrere a qualsiasi provvedimento disciplinare nel rispetto della legge e dei diritti dei lavoratori, ivi inclusi i diritti sindacali.

5.2 COMUNICAZIONE E DIFFUSIONE DEL CODICE ETICO

GetOpen S.r.l. si impegna a favorire e garantire adeguata conoscenza del Codice Etico divulgandolo presso i Dipendenti, i Collaboratori e tutti i Destinatari, mediante apposite ed adeguate attività di comunicazione.

Affinché chiunque possa uniformare i suoi comportamenti a quelli qui descritti, GetOpen S.r.l. assicurerà un adeguato programma di formazione e una continua sensibilizzazione dei valori e delle norme etiche contenuti nel Codice Etico.

5.3 BENI DI GETOPEN S.R.L.

I locali, le attrezzature, i sistemi, le vetture aziendali e tutti gli altri beni di GetOpen S.r.l. possono essere utilizzati, esclusivamente, per lo svolgimento delle attività aziendali o per scopi autorizzati dalla società.

5.4 PROTEZIONE DEL PATRIMONIO DI GETOPEN S.R.L.

Il patrimonio di GetOpen S.r.l. è costituito da beni materiali mobili e immateriali (ovvero informazioni e prodotti di proprietà esclusiva, che possono rappresentare oggetto di tutela di proprietà intellettuale) per il mantenimento della sua competitività nel mercato in cui opera.

Tra i predetti beni vi sono dati riservati ai dipendenti per l'espletamento della propria attività lavorativa. La perdita, il furto o l'uso improprio dei predetti beni potrebbe pregiudicare la Società e per questa ragione ogni Dipendente e Collaboratore è responsabile della protezione del patrimonio aziendale in generale. A questo scopo, si richiede il rispetto e la conoscenza delle procedure di sicurezza oltre la diligenza necessaria ad evitare ogni tipo di pregiudizio.

Infatti, ogni Dipendente e Collaboratore deve prestare attenzione a qualsiasi situazione che possa condurre alla perdita, al furto o all'uso improprio dei beni della GetOpen S.r.l. e denunciare ai responsabili della Sicurezza o al proprio superiore non appena ne venga a conoscenza.

Il patrimonio sociale di GetOpen S.r.l. deve essere gestito in modo efficiente ed onesto e, pertanto, tutti i soggetti obbligati al rispetto di questo Codice Etico concorrono a preservarne l'integrità ed il valore, a tutela dei soci, dei creditori e degli investitori.
Tutte le Risorse umane hanno la responsabilità della conservazione e della protezione dei beni e degli strumenti che sono loro affidati da GetOpen S.r.l. e devono contribuire a garantire la salvaguardia dell'intero patrimonio aziendale, rispettando le procedure operative e di sicurezza stabilite dalla Società.

6. COMUNICAZIONE AZIENDALE E RISERVATEZZA DELLE INFORMAZIONI

La comunicazione, all'interno ed all'esterno della Società, deve essere chiara, precisa e veritiera, onde evitare la diffusione di notizie e informazioni erronee ovvero il determinarsi di situazioni comportanti responsabilità di qualsiasi natura per la Società.
A tutela della reputazione della Società e della riservatezza delle informazioni non devono essere comunicate all'esterno, anche attraverso i digital e social media, informazioni riservate relative a GetOpen S.r.l. non già rese pubbliche (quale a titolo di esempio, contratti, procedimenti disciplinari e giudiziari, elementi retributivi, ecc); è altresì vietato diffondere contenuti, immagini, documenti scritti o audio-video di proprietà di GetOpen, senza autorizzazione.
Ai Destinatari è richiesto di non pubblicare informazioni non veritiere, diffamatorie, lesive dell'immagine di GetOpen o lesive della dignità di qualunque altro soggetto esterno, in qualche modo associate o associabili alla Società.
Le informazioni ed i documenti riservati, i progetti di lavoro, il know-how vanno custoditi e protetti in maniera adeguata e continua sia rispetto ai terzi che rispetto ai colleghi che agli stessi non sono direttamente interessati. I soggetti che, per ragioni di lavoro, vi hanno accesso devono, comunque, trattarli secondo le istruzioni e le procedure fissate dalla Società.
Qualora terze persone, deliberatamente e/o fraudolentemente, cercassero di ottenere informazioni riservate ad un Destinatario del presente Codice Etico, quest'ultimo deve darne tempestiva comunicazione ai propri referenti nell'ambito dell'organizzazione.

6.1 PROTEZIONE DEI DATI PERSONALI

GetOpen adotta misure organizzative e di sicurezza per il corretto trattamento dei dati personali di cui sia in possesso, nel rispetto della normativa europea e nazionale applicabile.

I dati personali vanno trattati in proporzione al consenso ricevuto e alle finalità del trattamento e non possono essere divulgati all'esterno senza consenso. I soggetti che, per ragioni di lavoro, vi hanno accesso devono seguire le istruzioni e le procedure fissate dalla Società.

6.2 ABUSO DI INFORMAZIONI PRIVILEGIATE

Per "informazioni privilegiate" si intendono le informazioni di carattere preciso – ai sensi dell'art. 181 comma 3 d.lgs. n. 58 del 1998 (TUF) – non pubbliche, concernenti direttamente o indirettamente la Società o uno o più strumenti finanziari emessi dalla Società e che, se rese pubbliche, potrebbero influire in modo sensibile sui prezzi degli strumenti finanziari quotati.

E' vietato utilizzare o comunicare ad altri, senza giustificato motivo, informazioni privilegiate.

I Destinatari del Codice Etico, se in possesso di informazioni privilegiate, ne devono dare immediato avviso alla Società perché provveda a gestirle nei termini e con le modalità indicate dalla legge e secondo la relativa procedura adottata dall'Amministratore Unico.

7 LINEE GUIDA DEL SISTEMA SANZIONATORIO

L'impegno della Società è focalizzato al raggiungimento delle *best practice* relativamente alle sue responsabilità di *business*, etiche e sociali verso i suoi soci, il suo capitale umano e gli altri stakeholder, Il Codice Etico definisce le aspettative della Società nei confronti dei Destinatari e la responsabilità di cui questi devono farsi carico per trasformare tali politiche in azioni concrete.

Le violazioni del Codice Etico sono passibili di sanzione, proporzionata alla gravità e declinata in base al tipo di rapporto che il Destinatario interessato intrattiene con GetOpen. I provvedimenti includono anche la cessazione del rapporto fiduciario con la Società con le conseguenze contrattuali previste e consentite dalle norme vigenti.

Infatti, la violazione dei principi fissati nel Codice Etico e nelle procedure indicate nei controlli interni compromette il rapporto fiduciario tra la Società ed i propri amministratori, dipendenti, consulenti, collaboratori a vario titolo, clienti, fornitori, partners commerciali e finanziari.

Tali violazioni saranno quindi immediatamente perseguite da GetOpen S.r.l. in maniera incisiva e tempestiva, mediante l'adozione di provvedimenti disciplinari adeguati e proporzionati.

Gli effetti delle violazioni del Codice Etico e dei protocolli interni devono essere tenuti in considerazione da tutti coloro che, a qualsiasi titolo, intrattengono rapporti con GetOpen S.r.l. A seconda della gravità della condotta posta in essere dal soggetto coinvolto in una delle attività illecite previste dal Codice Etico, GetOpen S.r.l. provvederà senza indugio ad adottare i provvedimenti opportuni, indipendentemente dall'eventuale esercizio dell'azione penale da parte dell'autorità giudiziaria.

FERMO QUANTO SOPRA ESPOSTO, I COMPORTAMENTI IN VIOLAZIONE DEL CODICE ETICO COSTITUISCONO:

- o grave inadempimento per i dipendenti (operai, impiegati, quadri e dirigenti), con le sanzioni, applicate a seconda della gravità, previste dal CCNL di categoria (rimprovero verbale, rimprovero scritto, multa non superiore a tre ore di retribuzione, sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni lavorativi, licenziamento per giusta causa o giustificato motivo); nel caso di pendenza dell'azione penale ovvero di esecuzione di un provvedimento restrittivo della libertà personale assunto nei confronti del dipendente, prima di adottare il provvedimento disciplinare, potrà essere adottata la sanzione della sospensione dal servizio e dalla retribuzione, per la durata corrispondente all'esito dell'azione penale ovvero fino al termine della durata del provvedimento restrittivo della libertà personale;
- o giusta causa per revoca del mandato agli amministratori;
- o causa di risoluzione immediata del rapporto, nei casi più gravi, per i collaboratori esterni e parasubordinati;
- o causa di risoluzione immediata del rapporto, nei casi più gravi, per i fornitori, appaltatori e subappaltatori.

L'individuazione e l'applicazione delle sanzioni terrà sempre conto dei principi generali di proporzionalità e di adeguatezza rispetto alla violazione contestata.

In tutte le suddette ipotesi, GetOpen S.r.l. si riserva altresì il diritto di esercitare tutte le azioni che riterrà opportune per il risarcimento del danno subito in conseguenza del comportamento in violazione del Codice Etico.

7.1 SEGNALAZIONI IN CASO DI VIOLAZIONI DELLE DISPOSIZIONI DEL CODICE ETICO

Eventuali situazioni di sospetta violazione delle disposizioni di cui al presente Codice Etico, da parte di uno o più Destinatari, possono essere segnalate, senza indugio, da qualunque Destinatario, purché la segnalazione sia in buona fede e circostanziata, ovvero fondata su elementi di fatto precisi e concordanti.

I seguenti canali di comunicazione sono alternativamente utilizzabili per la raccolta delle segnalazioni:

a) a mezzo e-mail, alla casella di posta elettronica: getopen@pec.getopen.it;

b) a mezzo posta ordinaria, in busta chiusa all'attenzione dell'Amministratore Unico e/o dell'Organismo di Vigilanza, inviata presso la sede legale della Società.

Le segnalazioni saranno gestite tempestivamente e attraverso un processo predefinito.

GetOpen richiede che le segnalazioni vengano fatte in forma nominativa, impegnandosi a mantenere riservata l'identità del Segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti di GetOpen o delle persone accusate erroneamente e/o in mala fede.

GetOpen tutela il Segnalante in buona fede contro ogni forma di ritorsione, discriminazione e/o di penalizzazione: ove tali atteggiamenti fossero riscontrati, GetOpen agirà di conseguenza.

Ugualmente GetOpen potrà reagire ai sensi della normativa applicabile verso chi, consapevolmente, dovesse effettuare segnalazioni false, infondate o pretestuose.

8. APPENDICE DI DETTAGLIO AI FINI DEL D.LGS. 231/2001

Il Codice Etico costituisce un elemento del Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/01.

Il Decreto Legislativo 8 giugno 2001, n. 231, prevede che la Società possa essere ritenuta responsabile per i reati commessi nel suo interesse o vantaggio. Il Decreto stabilisce all'art. 6 che la Società non risponde del reato commesso qualora dimostri (tra l'altro) di aver adottato ed efficacemente attuato Modelli di organizzazione, gestione e controllo idonei a prevenire i reati della specie di quello verificatosi.

Scopo del Modello Organizzativo, come per il Codice Etico, è quello di essere ragionevolmente idoneo ad individuare e prevenire le condotte penalmente rilevanti poste in essere nell'interesse o a vantaggio della Società, da soggetti "apicali" o sottoposti alla loro direzione e/o vigilanza.

Le norme del Codice Etico costituiscono parte essenziale delle obbligazioni contrattuali del personale disciplinate dalle disposizioni del codice civile.

Qualsiasi comportamento posto in essere dai Dipendenti, dai Collaboratori e da tutti i Destinatari che intrattengono rapporti con la Società in contrasto con le regole previste nel seguente Codice Etico, lede il rapporto di fiducia instaurato con l'azienda e può determinare, come previsto da specifiche clausole contrattuali, azioni disciplinari e di

risarcimento del danno, fermo restando, per i lavoratori dipendenti, il rispetto delle procedure previste dai contratti collettivi di lavoro e dal Sistema disciplinare adottato dalla Società.

GetOpen S.r.l. è consapevole del fatto che l'integrità e i valori etici sono elementi essenziali dell'ambiente di controllo della propria organizzazione e che essi incidono significativamente sulla progettazione, sull'amministrazione e sull'operatività quotidiana del proprio business.

Invero, affinché non vi siano incertezze o fraintendimenti su ciò che GetOpen S.r.l. richiede a tutti i Destinatari dello stesso, il presente Codice Etico e il modo in cui esso è inserito nella struttura di controllo dell'organizzazione saranno oggetto di frequenti azioni di formazione e comunicazione, al fine di consentire che il medesimo diventi patrimonio comune e condiviso a tutti i livelli.

8.1 TUTELA DEL CAPITALE SOCIALE, DEI CREDITORI E DEL MERCATO

Uno degli aspetti centrali che qualificano la condotta di GetOpen S.r.l. è rappresentato dal rispetto dei princìpi di comportamento intesi a garantire l'integrità del capitale sociale, la tutela dei creditori e dei terzi che instaurano rapporti con la Società.

I suddetti principi sono tutelati, anche, da norme penali e ai sensi del D.Lgs. 231/01 la violazione di tali disposizioni può costituire fonte di responsabilità per GetOpen S.r.l. ove le fattispecie di reato sia realizzata nell'interesse della Società stessa.

Pertanto, è posto l'espresso divieto a carico dei dipendenti, dei Collaboratori e di tutti i Destinatari del presente Codice Etico di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato previste dall'art. 25 ter del D.Lgs. 231/01 e porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo, ovvero comportamenti che possano favorire la commissione dei predetti reati.

I Dipendenti, i Collaboratori e tutti i Destinatari del presente Codice Etico, nell'ambito delle funzioni e attività svolte, sono responsabili della definizione e del corretto funzionamento del sistema di controllo e sono tenuti a comunicare in forma scritta alla Società o al proprio superiore le eventuali omissioni, falsificazioni o irregolarità contabili delle quali fossero venuti a conoscenza.

8.2 PUBBLICA AMMINISTRAZIONE

L'assunzione di impegni con le Istituzioni Pubbliche Locali, Statali, Comunitarie e Internazionali è riservata esclusivamente alle funzioni preposte e autorizzate. Per questo

motivo è opportuno che venga raccolta e conservata la documentazione che riassume le modalità attraverso le quali GetOpen S.r.l. è entrata in contatto con le Istituzioni.

È fatto assoluto divieto di:

- ai Dipendenti, ai Collaboratori esterni e ai consulenti delle Società e a tutti i Destinatari del presente Codice Etico di:
- falsificare e/o alterare i rendiconti al fine di ottenere un indebito vantaggio o qualsiasi altro beneficio per la Società;
- falsificare e/o alterare i dati documentali al fine di ottenere il favore o l'approvazione di un progetto non conforme alle normative vigenti in materia;
- destinare fondi pubblici a finalità diverse da quelle per cui si sono ottenuti.

8.3 CONFLITTO D'INTERESSI

Per garantire la massima trasparenza, GetOpen S.r.l. ed i propri dipendenti si impegnano a non trovarsi in situazioni di conflitto di interessi con dipendenti di qualsiasi Authority e loro familiari. Ciascun Dipendente, Collaboratore e Destinatario del presente Codice Etico che ritenga di trovarsi in una situazione di conflitto tra il proprio interesse personale, per suo conto o per conto di terzi, e gli interessi della Società, deve darne comunicazione immediata secondo l'opportunità, al proprio superiore gerarchico e all'Amministratore Unico, restando valide le norme specifiche previste dal Codice Civile.

8.4 SISTEMA DI WHISTLEBLOWING

Il sistema di whistleblowing di GetOpen è a disposizione dei suoi dipendenti e di terze parti in caso di dubbi sul fatto che una legge, un regolamento, uno dei principi enunciati nel presente Codice Etico sia stato o stia per essere violato, in caso di minaccia o grave pregiudizio per l'interesse generale della Società, come in caso di corruzione in seno a GetOpen. Ulteriori informazioni sul sistema di whistleblowing, sulla protezione specifica dei whistleblower, sulla riservatezza, sulla protezione dei dati e sulle modalità di segnalazione sono riportate nella sezione principale del Codice Etico di GetOpen, nonché nel Modello di Organizzazione gestione e controllo ai sensi del d.lgs. 231/01.

GetOpen sanziona severamente ogni condotta di corruzione e, pertanto, nel caso in cui da un'indagine interna emergano casi di corruzione o di traffico di influenze illecite, possono essere intraprese sanzioni disciplinari nei confronti dei dipendenti, incluso il licenziamento, in conformità con le politiche disciplinari stabilite nelle norme interne, ove applicabile, e con la legge locale. In caso di individuazione di casi di corruzione, GetOpen può riservarsi di interrompere i rapporti di affari con partner commerciali e altre terze parti.

9 ENTRATA IN VIGORE E DIFFUSIONE

Il presente Codice Etico e di Condotta entra in vigore a partire dalla sua approvazione da parte dell'Amministratore Unico e viene attuato insieme al Modello di organizzazione, gestione e controllo predisposto ai sensi del D.Lgs. 231/2001. Ogni variazione o integrazione successiva è approvata dall'Amministratore Unico e diffusa secondo quanto previsto del Modello.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

GETOPEN SRL
Energy Saving Company
Via Cesare Vivante 9 – 95123 CATANIA
Part. IVA 05012480876 – R.E.A. N. 336696

ALLEGATO - 2 -

Clausola contrattuale

GetOpen intende inserire, tra le condizioni generali di contratto, la seguente clausola, al fine di assicurare l'osservanza e divulgazione del proprio Modello Organizzativo di cui al D.Lgs. 231/2001.

1) CLAUSOLA CONTRATTUALE PER CONTROPARTE

"*La parte X dichiara di conoscere le norme comportamentali adottate da GETOPEN nel Modello D.Lgs. 231/01 e nel proprio Codice Etico, entrambi pubblicati nel sito internet aziendale www.getopen.it e, conseguentemente, dichiara e riconosce di essere consapevole delle conseguenze che comportamenti contrari, ai sopra citati documenti e alla normativa D.Lgs 231/2001, possono avere con riguardo al rapporto contrattuale, potendo configurare inadempimento contrattuale e, dunque, causa di risarcimento del danno e di risoluzione del contratto*".

GETOPEN SRL
Energy Saving Company
Via Cesare Vivante 9 – 95123 CATANIA
Part. IVA 05012480876 – R.E.A. N. 336696

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

ALLEGATO - 3 -

ELENCO REATI SANZIONATI DAL DECRETO

Aggiornato con la Legge n.90 del 28 giugno 2024 e con il D.Lgs n.87 del 14 giugno 2024

1. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE (ARTT. 24 E 25, D.LGS. N. 231/2001)

[articolo modificato dalla Legge n. 90 del 28 giugno 2024]

- Peculato (art. 314 c.p.);
- Peculato mediante profitto dell'errore altrui (art. 316 c.p.);
- Malversazione di erogazioni pubbliche (art. 316 bis c.p.);
- Indebita percezione di erogazioni pubbliche (art. 316 ter c.p.);
- Concussione (art. 317 c.p.);
- Corruzione per l'esercizio della funzione (art. 318 c.p.);
- Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.);
- Corruzione in atti giudiziari (art. 319 ter c.p.);
- Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.);
- Istigazione alla corruzione (art. 322 c.p.);
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione, abuso d'ufficio di membri delle Corti internazionali o degli organi delle comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.);
- Abuso d'ufficio (art. 323 c.p.);
- Traffico di influenze illecite (art. 346 bis c.p.);
- Turbata libertà degli incanti (art. 353 c.p.);
- Inadempimento di contratti di pubbliche forniture (art. 355 c.p.);
- Frode nelle pubbliche forniture (art. 356 c.p.);
- Truffa in danno dello Stato o di altro Ente pubblico (art. 640, comma 2 n. 1 c.p.);
- Truffa (art. 640);
- Truffa (art. 640 quater Applicabilità dell'art. 322 -ter);

- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.);
- Frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640 ter c.p.).

2. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (ART. 24 BIS D.LGS. N. 231/2001)

[articolo interamente modificato, anche il testo, con l'inserimento del comma 1-bis e la modifica dei commi esistenti dalla Legge n. 90 del 28 giugno 2024]

- Falsità in documenti informatici pubblici aventi efficacia probatoria (art. 491 bis c.p., in relazione agli artt. 476, 477, 478, 479, 480, 481, 482, 483, 484, 487, 488, 489, 490 492 c.p. 493 c.p.);
- Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.); [abrogato];
- Art. 617-bis (Detenzione, diffusione e installazione abusiva di apparecchiature e di altri etc.);
- Estorsione (art. 629 c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- Art. 635-quater.1 (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi, etc.);
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 «quinquies c.p.).

- Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105).

3. DELITTI DI CRIMINALITÀ ORGANIZZATA (ART. 24 TER D.LGS. N. 231/2001)

- Associazione per delinquere (art. 416 c.p.);
- Associazione per delinquere diretta alla commissione dei delitti di riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.), tratta di persone (art. 601 c.p.), traffico di organi prelevati da persona vivente (art. 6()1 bis c.p.), acquisto e alienazione di schiavi (art. 602 c.p.), tratta o trasporto di stranieri in violazione delle diposizioni del Testo Unico in materia di Immigrazione ex art. 12 comma 3 bis, D.Lgs. n. 286/1998 (art. 416 comma 6 c.p., in relazione agli artt. 600, 601, 601 bis e 602 c.p., nonché in relazione all'art. 12 comma 3 bis D.Lgs. n. 286/1998);
- Associazione per delinquere diretta alla commissione dei delitti di prostituzione minorile (art. 600 bis c.p.), pornografia minorile (art. 600 ter c.p.), detenzione di materiale pedopornografico (art. 600 quater c.p.), pornografia virtuale (art. 600 quater. 1 c.p.), iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 quinquies c.p.), violenza sessuale (art. 609 bis c.p.), atti sessuali con minorenne (art. 609 quater c.p.), corruzione di minorenne (art. 609 quinquies c.p.), violenza sessuale di gruppo (609 octies c.p.), adescamento di minorenni (art. 609 undecies c.p.) (art. 416 comma 7, in relazione agli artt. 600 bis, 600 ter, 600 quater, 600 quater. l, 600 quinquies, 609 bis, 609 quater, 609 quinquies, 609 octies, 609 undecies c.p.);
- Associazione per delinquere diretta alla commissione dei delitti di cui all'art. 407 comma 2 lett. a) n. 5 c.p.p.;
- Associazioni di tipo mafioso anche straniere (art. 416 bis c.p.);
- Delitti commessi avvalendosi delle condizioni previste dal predetto art. 416 bis c.p. ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo;
- Delitti previsti dall'art. 74 D.P.R. n. 309/1990;
- Sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.).

4. FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO (ART. 25 BIS D.LGS. N. 231/2001)

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);

- Alterazione di monete (art. 454 c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.);
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

5. DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO (ART. 25 BIS.L D.LGS. N. 231/2001)

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513 bis c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517 ter c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517 quater c.p.).

6. REATI SOCIETARI (ART. 25 TER D.LGS. N. 231/2001)

- False comunicazioni sociali (artt. 2621 e 2621 bis c.c.);
- False comunicazioni sociali delle società quotate (art. 2622 c.c.);
- Falso in prospetto (art. 2623 c.c.);
- Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624 c.c.);
- Impedito controllo (art. 2625 c.c.);
- Indebita restituzione dei conferimenti (art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);

- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Omessa comunicazione del conflitto di interessi (art. 2629 bis c.c., in relazione all'art. 2391 c.c.);
- Formazione fittizia del capitale (art. 2632 c.c.);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- Corruzione tra privati (art. 2635 comma 3 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis comma 1 c.c.);
- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Aggiotaggio (art. 2637 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità di pubblica vigilanza (art. 2638, comma I e 2 c.c.);
- False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D. Lgs. 19/2023).

7. DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO (ART. 25 QUATER D.LGS. N. 231/2001)

- Associazioni sovversive (art. 270 c.p.);
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270 bis c.p.);
- Assistenza agli associati (art. 270 ter c.p.);
- Arruolamento con finalità di terrorismo anche internazionale (art. 270 quater c.p.);
- Organizzazione di trasferimenti per finalità di terrorismo (art. 270 quater.l c.p.);
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270 quinquies c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270 quinquies. / c.p.);
- Sottrazione di beni o denaro sottoposti a sequestro (art. 270 quinquies.2 c.p.);
- Condotte con finalità di terrorismo (art. 270 sexies c.p.);
- Attentato per finalità terroristiche o di eversione (art. 280 c.p.);
- Atto di terrorismo con ordigni micidiali o esplosivi (art. 280 bis c.p.);
- Atti di terrorismo nucleare (art. 280 ter c.p.);
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289 bis c.p.);
- Sequestro a scopo di coazione (art. 289 ter c.p.);
- Istigazione a commettere alcuno dei delitti con finalità di terrorismo o dell'ordine democratico (art. 302 c.p.);

- Cospirazione politica mediante accordo (art. 304 c.p.);
- Cospirazione politica mediante associazione (art. 305 c.p.);
- Banda armata: formazione e partecipazione (art. 306 c.p.);
- Assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.);
- Impossessamento, dirottamento e distruzione di un aereo (L. 342/1976, art. 1);
- Danneggiamento delle installazioni a terra (L. 342/1976, art. 2);
- Violazione dell'art. 2 della Convenzione Internazionale per la repressone del finanziamento del terrorismo di New York del 9 dicembre 1999.

8. PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI (ART. 25 QUATER.L D.LGS. N. 231/2001)

- Pratiche di mutilazione degli organi genitali femminili (art. 583 bis c.p.).

9. DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE (ART. 25 QUINQUIES D.LGS. N. 231/2001)

- Riduzione o mantenimento in schiavitù o ln servitù (art. 600 c.p.);
- Prostituzione minorile (art. 600 bis c.p.);
- Pornografia minorile (art. 600 ter c.p.);
- Detenzione o accesso a materiale pornografico (art. 600 quater c.p.);
- Pornografia virtuale (art. 600 quater I c.p.);
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 quinquies c.p.);
- Tratta di persone (art. 601 c.p.);
- Acquisto e alienazione di schiavi (art. 602 c.p.);
- Intermediazione illecita e sfruttamento del lavoro (art. 603 bis c.p.);
- Adescamento di minorenni (art. 609 undecies c.p.).

10. ABUSI DI MERCATO (ART. 25 SEXIES D.LGS. N. 231/2001)

- Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (art. 184 D.Lgs. n. 58/1998);
- Manipolazione di mercato (art. 185 D.Lgs. n. 58/1998).

11. OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E DELLA SICUREZZA SUL LAVORO (ART. 25 SEPTIES D.LGS. N. 231/2001)

- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose (art. 590 comma 3 c.p.).

12. RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENE O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO (ART. 25 OCTIES D.LGS N. 231/2001)

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648 bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.);
- Autoriciclaggio (art. 648 ter.l c.p.).

13. DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART. 25 OCTIES D.LGS N. 231/2001)

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493- ter c.p.);
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 quater c.p.);
- Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640 ter c.p.);
- Trasferimento fraudolento di valori (art. 512 bis c.p.)
- Violazione delle disposizioni di cui al Capo I, II, III e IV del Titolo VII del c.p. relativo ai delitti contro la fede pubblica;
- Violazione delle disposizioni di cui al Capo I e II del Titolo XIII del c.p., relativo ai delitti contro il patrimonio.

14. DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (ART. 25 NOVIES D.LGS N. 231/2001)

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171 comma 1 lett. A bis, L. n. 633/1941);
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione, qualora ne risulti offeso l'onore o la reputazione (art. 171 comma 3, L. n. 633/1941);
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla S.I.A.E.; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171 bis comma I, L. n. 633/1941);

- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171 bis comma 2, L. n. 633/1941);
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di Immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171 ter, L. n. 633/1941);
- Mancata comunicazione alla S.I.A.E. dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171 septies, L. n. 633/1941);
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171 octies, L. n. 633/1941).

15. INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 25 DECIES D.LGS N. 231/2001)

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 377 bis c.p.).

16. REATI AMBIENTALI (ART. 25 UNDECIES D.LGS N. 231/2001)

- Inquinamento ambientale (art. 452 bis c.p.);
- Disastro ambientale (art. 452 quater c.p.);
- Delitti colposi contro l'ambiente (art. 452 quinquies c.p.);
- Traffico e abbandono di materiali ad alta radioattività (art. 452 sexies c.p.);
- Associazione per delinquere, anche di tipo mafioso, diretta alla commissione di delitti contro l'ambiente di cui agli artt. 452 bis ss. c.p. (art. 452 octies c.p.);

- Attività organizzate per il traffico illecito di rifiuti (art. 452 quaterdecies c.p.);
- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727 bis c.p.);
- Reati relativi alla violazione delle norme che regolamentano il commercio internazionale delle specie animali e vegetali in via di estinzione (L. 7 febbraio 1992, n. 150);
- Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733 bis c.p.);
- Reati relativi alla violazione della disciplina in materia di tutela delle acque (art. 137 commi 2, 3, 5, 11 e 13, D.Lgs. n. 152/2006);
- Attività di gestione di rifiuti non autorizzata (art. 256 commi 1, 3, 5, 6, D.Lgs. n. 152/2006);
- Bonifica dei siti (art. 257 D.Lgs. n. 152/2006);
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 comma 4, D.Lgs. n. 152/2006);
- Traffico illecito di rifiuti (art. 259 comma 1 D.Lgs. n. 152/2006);
- Sistema informatico di controllo della tracciabilità dei rifiuti (art. 260 bis commi 6, 7, 8, D.Lgs n. 152/2006);
- Reati relativi alla violazione della disciplina in materia di tutela dell'aria (art. 279 comma 5, D.Lgs. n. 152/2006);
- Reati relativi alla violazione delle misure poste a tutela dell'ozono stratosferico e dell'ambiente (L. 28 dicembre 1993, n. 549);
- Reati relativi alla violazione della disciplina volta a ridurre l'inquinamento

17. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (ART. 25 DUODECIES D.LGS N. 231/2001)

- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22 comma 12 bis, D.Lgs. n. 286/1998; art. 12 commi 3, 3 bis, 3 ter, 5, D.Lgs. n. 286/1998).

18. RAZZISMO E XENOFOBIA (ART. 25 TERDECIES D.LGS N. 231/2001)

- Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa (art. 604 bis c.p.).

19. FRODE IN COMPETIZIONI SPORTIVE, ESERCIZIO ABUSIVO DI GIOCO O DI SCOMMESSA E GIOCHI D'AZZARDO ESERCITATI A MEZZO DI APPARECCHI VIETATI (ART. 25 QUATERDECIES D.LGS N. 231/2001)

- Reati di frode in competizioni sportive, di esercizio abusivo di gioco o di scommessa e di

giochi d'azzardo esercitati a mezzo di apparecchi vietati (artt. 1 e 4, Legge 13 dicembre 1989, n. 401).

20. Reati Tributari (Art. 25-quinquesdecies, D.Lgs. n. 231/2001) [modificato dal D.Lgs n.87 del 14 Giugno 2024 ed in particolare, all'Art.10-quater "Indebita compensazione" è stato aggiunto il comma 2-bis che tratta della eventuale esclusione della punibilità dell'agente in merito a spettanze del credito.]

- Disposizioni comuni alle sanzioni amministrative e penali aggiunta dei commi g-quater "crediti inesistenti", g-quinquies "crediti non spettanti" (Art. 1 D.Lgs. n. 74/2000);

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000)
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000)
- Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]
- Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000)
- Omesso versamento di ritenute certificate (art. 10 D.Lgs. n. 74/2000, sostituito integralmente)
- Omesso versamento di IVA (Art. 10-ter D.Lgs. n. 74/2000, sostituito integralmente)
- Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000)
- Sequestro e confisca (Art. 12-bis D.Lgs. n. 74/2000)
- Cause di non punibilità. Pagamento del debito tributario (Art. 13 D.Lgs. n. 74/2000)
- Circostanze del reato (Art. 13-bis D.Lgs. n. 74/2000)
- Principio di specialità (Art. 19 D.Lgs. n. 74/2000)
- Rapporti tra procedimento penale e processo tributario (Art. 20 D.Lgs. n. 74/2000)
- Sanzioni amministrative per le violazioni ritenute penalmente rilevanti (Art. 21 D.Lgs. n. 74/2000)
- Efficacia delle sentenze penali nel processo tributario e nel processo di Cassazione (Art. 21-bis D.Lgs. n. 74/2000)
- Applicazione ed esecuzione delle sanzioni penali e amministrative (Art. 21-ter D.Lgs. n. 74/2000)

21. CONTRABBANDO (Art. 25 sexiesdecies D.Lgs n. 231/2001)

- Contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali (art. 282 DPR n. 43/1973);

- Contrabbando nel movimento delle merci nei laghi di confine (art. 283 DPR n. 43/1973);

- Contrabbando nel movimento marittimo delle merci (art. 284 DPR n. 43/1973);

- Contrabbando nel movimento delle merci per via aerea (art. 285 DPR n. 43/1973);

- Contrabbando nelle zone extra-doganali (art. 286 DPR n. 43/1973);

- Contrabbando per indebito uso di merci importate con agevolazioni doganali (art. 287 DPR n. 43/1973);
- Contrabbando nei depositi doganali (art. 288 DPR n. 43/1973);
- Contrabbando nel cabotaggio e nella circolazione (art. 289 DPR n. 43/1973);
- Contrabbando nell'esportazione di merci ammesse a restituzione di diritti (art. 290 DPR n. 43/1973);
- Contrabbando nell'importazione od esportazione temporanea (art. 291 DPR n. 43/1973);
- Contrabbando di tabacchi lavorati esteri (art. 291 bis DPR n. 43/1973);
- Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati esteri (art. 291 ter DPR n. 43/1973);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291 quater DPR n. 43/1973);
- Altri casi di contrabbando (art. 292 DPR n. 43/1973);
- aggravanti del contrabbando (art. 295 n.43 /1973).

22. DELITTI CONTRO IL PATRIMONIO CULTURALE (ART. 25 SEPTIESDECIES D.LGS N. 231/2001)

- Furto di beni culturali (art. 518 bis c.p.);
- Appropriazione indebita di beni culturali (art. 518 ter c.p.);
- Ricettazione di beni culturali (art. 518 quater c.p.);
- Falsificazione in scrittura privata relativa a beni culturali (art. 518 oclies c.p.);
- Violazioni in materia di alienazione di beni culturali (art. 518 novies c.p.);
- Importazione illecita di beni culturali (art. 518 decies c.p.);
- Uscita o esportazione illecite di beni culturali (art. 518 undecies c.p.);
- Distruzione, dispersione, deterioramento, deturpamento, Imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518 duodecies c.p.);
- Contraffazione di opere d'arte (art. 518 quaterdecies c.p.).

23. RICICLAGGIO DL BENI CULTURALI E DEVASTAZIONE E SACCHEGGIO DL BENI CULTURALI E PAESAGGISTICI (ART. 25 DUODEVICIES D.LGS N. 231/2001)

- Riciclaggio di beni culturali (art. 518 sexies c.p.);
- Devastazione e saccheggio di beni culturali e paesaggistici (art. 518 terdecies c.p.).

24. REATI TRANSNAZIONALI (L. 146/2006)

- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al D.P.R. 9 ottobre 1990, n. 309);
- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3 bis, 3 ter e 5, del testo unico di cui al D. Lgs. 25 luglio 1998, n. 286);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291quater del testo unico di cui al D.P.R. 23 gennaio 1973, n. 43);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.);
- Favoreggiamento personale (art. 378 c.p.);
- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso (art. 416 bis c.p.).

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

GETOPEN SRL
Energy Saving Company
Via Cesare Vivante 9 – 95123 CATANIA
Part. IVA 05012480876 – R.E.A. N. 336696

ALLEGATO - 4 -

COMPOSIZIONE ORGANISMO DI VIGILANZA

In ottemperanza all'art. 6 del D. Lgs. 231/2001, GetOpen affida all'Organismo di Vigilanza il compito di vigilare sull'efficace attuazione, sul funzionamento, sull'osservanza del Modello e di proporne l'aggiornamento al fine di migliorarne l'efficacia nella prevenzione dei reati e degli illeciti.

GetOpen affida le funzioni di Organismo di Vigilanza ad un organismo monocratico, esterno a GETOPEN S.r.l., in possesso dei requisiti di autonomia, indipendenza, professionalità e onorabilità richiesti per l'esercizio delle proprie funzioni.

L'Organismo di Vigilanza si occupa esclusivamente, ai sensi del D. Lgs. 231/2001, della vigilanza sull'attuazione e sull'osservanza del Modello da parte dei soggetti allo stesso sottoposti e formula proposte di modifica ed aggiornamento con lo scopo preciso di migliorarne l'efficacia di prevenzione dei reati compresi nel catalogo contenuto nel D. Lgs. 231/2001.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

GETOPEN SRL
Energy Saving Company
Via Cesare Vivante 9 – 95123 CATANIA
Part. IVA 05012480876 – R.E.A. N. 336696

ALLEGATO - 5 -

COSTITUZIONE, COMPENSI, CAUSE DI (IN) ELEGGIBILITÀ, DECADENZA E SOSPENSIONE DEI COMPONENTI DELL'ORGANISMO DI VIGILANZA

COMPENSI

GETOPEN stabilisce il compenso annuo spettante al componente monocratico dell'Organismo di Vigilanza, riconoscendo, altresì, il rimborso delle spese vive e documentate sostenute per l'espletamento dell'incarico conferito.

INELEGGIBILITÀ

Il componente monocratico dell'Organismo di Vigilanza deve essere in possesso dei requisiti di onorabilità di cui all'art. 109 del D.Lgs. 1 settembre 1993, n. 385.

Mentre, non può essere nominato componente dell'Organismo di Vigilanza colui che si trovi nelle condizioni previste dall'art. 2399 c.c. e, salvi gli effetti della riabilitazione, colui il quale è stato condannato con sentenza divenuta definitiva, anche se emessa ex artt. 444 e ss. c.p.p. ed anche se con pena condizionalmente sospesa:

1) alla reclusione per un tempo non inferiore ad un anno per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267;

2) alla pena detentiva per un tempo non inferiore ad un anno per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;

3) alla reclusione per un tempo non inferiore ad un anno per un delitto contro la pubblica amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, per un delitto in materia tributaria;

4) per un qualunque delitto non colposo alla pena della reclusione per un tempo non inferiore a due anni;

5) per uno dei reati previsti dal titolo XI del libro V del codice civile così come riformulato del D.Lgs. 61/02;

6) per un reato che importi e abbia importato la condanna ad una pena da cui derivi l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;

7) per uno o più reati tra quelli tassativamente previsti dal Decreto anche se con condanne a pene inferiori a quelle indicate ai punti precedenti;

8) coloro che hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate le sanzioni previste dall'art. 9 del Decreto;

9) coloro nei cui confronti sia stata applicata in via definitiva una delle misure di prevenzione previste dall'art. 10, comma 3, della legge 31 maggio 1965, n. 575, come sostituito dall'articolo 3 della legge 19 marzo 1990, n. 55 e successive modificazioni;

10) coloro nei cui confronti siano state applicate le sanzioni amministrative accessorie previste dall'art. 187 quater Decreto Legislativo n. 58/1998.

L'Amministratore Unico di GetOpen può revocare il componente monocratico dell'Organismo di Vigilanza nei casi in cui si verifichino: **a)** rilevanti inadempimenti rispetto al mandato conferito, in ordine ai compiti indicati nel regolamento; **b)** per ipotesi di violazione degli obblighi di riservatezza; **c)** quando si manifestino cause di ineleggibilità di cui sopra, anteriori alla nomina a componente dell'OdV; **d)** quando intervengano le cause di decadenza di seguito specificate.

DECADENZA

Il componente monocratico dell'Organismo di Vigilanza decade dalla carica nel momento in cui venga a trovarsi, successivamente alla sua nomina:

• in una delle situazioni contemplate nell'art. 2399 c.c.;

• condannato con sentenza definitiva (intendendosi per sentenza di condanna anche quella pronunciata ex art. 444 c.p.p.) per uno dei reati indicati ai numeri 1, 2, 3, 4, 5, 6 e 7 delle condizioni di ineleggibilità innanzi indicate;

• nella situazione in cui, dopo la nomina, si accerti aver rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate le sanzioni previste dall'art. 9 del Decreto in relazione a illeciti amministrativi commessi durante la loro carica.

SOSPENSIONE

Costituiscono cause di sospensione dalla funzione di componente monocratico dell'Organismo di Vigilanza:

• la condanna con sentenza non definitiva per uno dei reati dei numeri da 1 a 7 delle condizioni di ineleggibilità innanzi indicate;

• l'applicazione su richiesta delle parti di una delle pene di cui ai numeri da 1 a 7 delle condizioni di ineleggibilità innanzi indicate;

• l'applicazione di una misura cautelare personale;

• l'applicazione provvisoria di una delle misure di prevenzione previste dall'art. 10, comma 3, della legge 31 maggio 1965, n. 575, come sostituito dall'articolo 3 della legge 19 marzo 1990, n. 55 e successive modificazioni.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

GETOPEN SRL
Energy Saving Company
Via Cesare Vivante 9 – 95123 CATANIA
Part. IVA 05012480876 – R.E.A. N. 336696

ALLEGATO - 6 -

Procedura Wistleblowing

SOMMARIO

1. PREMESSA

La presente procedura ha lo scopo di disciplinare il processo di trasmissione, ricezione, analisi e gestione delle Segnalazioni (cd. Whistleblowing) su informazioni, adeguatamente circostanziate, riferibili al Personale di GETOPEN e/o Terzi relative a violazioni di leggi e regolamenti, del Codice Etico e del Modello Organizzativo 231.

La procedura è anche finalizzata a dare attuazione al Decreto Legislativo 10 marzo 2023 n. 24, pubblicato in G.U. in data 15.03.2023, recante il recepimento della Direttiva (UE) 2019/1937 riguardante "*la protezione delle persone che segnalano violazioni del diritto dell'Unione (cd. disciplina Whistleblowing*)" e, per quanto non espressamente indicato dalla stessa, resta integralmente applicabile quanto previsto dal suddetto Decreto Legislativo.

LA PREDETTA NORMATIVA PREVEDE, IN SINTESI:

- un regime di tutela verso specifiche categorie di soggetti che segnalano informazioni, acquisite nel contesto lavorativo, relative a violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'ente;
- misure di protezione, tra cui il divieto di ritorsioni, a tutela del Segnalante, dei colleghi e dei parenti del segnalante e dei soggetti giuridici collegati al Segnalante;
- l'istituzione di canali di segnalazione interni all'ente per la trasmissione di Segnalazioni che garantiscano la tutela della riservatezza dell'identità del Segnalante, della Persona coinvolta e/o comunque menzionata nella Segnalazione, del contenuto della Segnalazione e della relativa documentazione;
- oltre alla facoltà di sporgere denuncia all'autorità giudiziaria o contabile, la possibilità (qualora ricorra una delle condizioni previste all'art. 6, comma 1, del d.lgs. n. 24/2023) di effettuare Segnalazioni esterne tramite il canale gestito dall'Autorità Nazionale Anticorruzione (di seguito ANAC), nonché di effettuare Divulgazioni pubbliche (al ricorrere di una delle condizioni previste all'art. 15, comma 1, del d.lgs. n. 24/2023), tramite la stampa o mezzi elettronici o di diffusione in grado di raggiungere un numero elevato di persone;
- provvedimenti disciplinari nonché sanzioni amministrative pecuniarie irrogate da ANAC nei casi previsti dagli artt. 16 e 21 del d.lgs. n. 24/2023.

2. I DESTINATARI

DESTINATARI DELLA PROCEDURA SONO:

- i Vertici aziendali, i componenti degli organi sociali e l'Organismo di Vigilanza di GETOPEN;
- i dipendenti, gli ex dipendenti e i candidati a posizioni lavorative, i soci, i clienti di GETOPEN nonché - a titolo non esaustivo - i partner, i fornitori (anche in regime di appalto/subappalto), i consulenti, i collaboratori nello svolgimento della propria attività

lavorativa presso GETOPEN che sono in possesso di Informazioni su violazioni come definite nella presente Procedura.
Rientrano, altresì, tra i Destinatari, i soggetti fisici e giuridici, non ricompresi nelle precedenti categorie ma ai quali si applicano le misure di protezione previste dalla presente Procedura.
Quanto previsto nel presente documento si applica anche alle Segnalazioni anonime, purché adeguatamente circostanziate, come definite nella presente Procedura.

3. SCOPO E CAMPO DI APPLICAZIONE

La Procedura ha lo scopo di disciplinare il processo di trasmissione, ricezione, analisi e gestione delle Segnalazioni, compresa l'archiviazione e la successiva cancellazione sia delle Segnalazioni sia della documentazione ad esse correlata, con le modalità indicate nel presente documento.
La Procedura si applica a GETOPEN che ne garantisce la corretta e costante applicazione, nonché la massima diffusione interna ed esterna.
Sono escluse dal perimetro di applicazione della Procedura le Segnalazioni inerenti a:
- contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale del Segnalante, che attengono esclusivamente alla disciplina del rapporto di lavoro o ai rapporti con le figure gerarchicamente sovraordinate, salvo che siano collegate o riferibili alla violazione di norme o di regole/procedure interne;
- violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato dell'Unione Europea;
- violazioni disciplinate in via obbligatoria da atti dell'Unione Europea o nazionali, come indicati nell'art. 1, co. 2, lett. b), del d.lgs. n. 24/2023 (in materia di servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente);
- fatti o circostanze rientranti nell'applicazione di disposizioni nazionali o dell'Unione Europea in materia di informazioni classificate, segreto forense o medico e di segretezza delle deliberazioni degli organi giurisdizionali, ovvero rientranti nell'applicazione di disposizioni nazionali in materia di procedura penale, di autonomia e indipendenza della magistratura, delle disposizioni sulle funzioni e attribuzioni del Consiglio Superiore della Magistratura, in materia di difesa nazionale e di ordine e sicurezza pubblica, nonché in materia di esercizio e tutela del diritto dei lavoratori di consultare i propri rappresentanti

o i sindacati, di protezioni contro le condotte o gli atti illeciti posti in essere in ragione di tali consultazioni, di autonomia delle parti sociali e del loro diritto di stipulare accordi collettivi, nonché di repressione delle condotte antisindacali;

- richieste di esercizio dei diritti in materia di protezione dei dati personali nei confronti di GETOPEN (c.d. diritti privacy), ai sensi del Regolamento (UE) n. 2016/679 (Regolamento Generale sulla Protezione dei Dati - GDPR) e dei d.lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) e d.lgs. 10 agosto 2018, n. 101 e successive modifiche e integrazioni.

Qualora dette circostanze siano rilevanti anche ai sensi del Modello Organizzativo 231 dovranno essere oggetto di Segnalazione, come previsto dalla presente Procedura.

Le Segnalazioni rientranti nelle predette tipologie verranno inoltrate alle competenti strutture aziendali per monitorare gli esiti al fine di rilevare eventuali debolezze del sistema di controllo interno e di gestione dei rischi o impatti su processi sensibili 231.

4. RIFERIMENTI NORMATIVI ESTERNI

- Decreto Legislativo 8 giugno 2001 n. 231 ("Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300");
- Regolamento (UE) n. 2016/679 (Regolamento Generale sulla Protezione dei Dati - GDPR);
- Decreto Legislativo 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) e successive modifiche ed integrazioni, tra cui il Decreto Legislativo 10 agosto 2018, n. 101, nonché le collegate disposizioni legislative;
- Direttiva (UE) 2019/1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (cd. Whistleblowing);
- Decreto Legislativo 10 marzo 2023 n. 24, pubblicato in G.U. in data 15.03.2023, recante il recepimento della Direttiva (UE) 2019/1937;
- Decreto-legge 15 marzo 2012, n. 21, convertito in Legge 11 maggio 2012, n. 56 ("Norme in materia di poteri speciali sugli assetti societari nei settori della Difesa e della Sicurezza Nazionale, nonché per le attività di rilevanza strategica nei settori dell'Energia, dei Trasporti e delle Comunicazioni");
- Decreto-legge 11 luglio 2019 n. 64 ("Golden Power - Norme in materia di poteri speciali sugli assetti societari");

- DPCM 1 agosto 2022 n. 133 ("Nuovo Regolamento di procedura per l'esercizio dei poteri speciali").

5. RIFERIMENTI NORMARTIVI INTERNI

- Modello Organizzativo 231 di GETOPEN S.R.L.;

- Codice Etico di GETOPEN S.R.L.;

- Gestione del procedimento disciplinare personale dipendente.

6. DESCRIZIONE DELPROCESSO E RESPONSABILITA'

6.1 Scopo e descrizione del processo

Per le Segnalazioni riguardanti GETOPEN, il Responsabile del processo di gestione è l'Organismo di Vigilanza della Società.

Al fine di dare seguito alle Segnalazioni, l'Organismo di Vigilanza di GETOPEN si avvale del supporto delle Funzione Aziendali competenti.

Le Funzioni Aziendali competenti, nell'ambito delle attività di supporto all'Organismo di Vigilanza, svolgono, altresì, gli approfondimenti istruttori richiesti da ANAC sulle Segnalazioni esterne ovvero sulle Divulgazioni pubbliche riguardanti GETOPEN dandone informativa all'Organismo di Vigilanza di riferimento.

6.2 La trasmissione della Segnalazione

I Destinatari della presente Procedura che vengono a conoscenza di Informazioni su eventuali violazioni sono tenuti ad effettuare una Segnalazione attraverso i canali di segnalazione interni di seguito descritti.

Chiunque riceve una Segnalazione, in qualsiasi forma (orale o scritta), deve trasmetterla tempestivamente, e comunque entro 7 giorni dal suo ricevimento, all'Organismo di Vigilanza, attraverso i canali di segnalazione interni di seguito descritti, dando contestuale notizia della trasmissione al Segnalante se noto. Il Segnalante non può trattenere copia dell'originale e deve eliminare eventuali copie in formato digitale, astenendosi dall'intraprendere qualsiasi iniziativa autonoma di analisi e/o approfondimento. Lo stesso è tenuto alla riservatezza dell'identità del Segnalante, delle Persone coinvolte e/o comunque menzionate nella Segnalazione, del contenuto della Segnalazione e della relativa documentazione.

La mancata comunicazione di una Segnalazione ricevuta nonché la violazione dell'obbligo di riservatezza costituiscono una violazione della Procedura e potranno comportare l'adozione di provvedimenti disciplinari.

LE SEGNALAZIONI POSSONO ESSERE TRASMESSE:

- a mezzo posta ordinaria, indirizzata all'Organismo di Vigilanza 231 di GETOPEN e/o presso la sede legale della società.

Il Segnalante può inoltre chiedere di effettuare una Segnalazione orale mediante un incontro diretto con l'Organismo di Vigilanza di GETOPEN. In tal caso, previo consenso del Segnalante, il colloquio è documentato a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale, che il Segnalante può verificare, rettificare e confermare mediante sottoscrizione.

6.3 Classificazione e analisi preliminare della Segnalazione

L'Organismo di Vigilanza, dopo avere analizzato le Segnalazioni ricevute, valuta:

- l'avvio della fase di istruttoria;
- la chiusura delle Segnalazioni, in quanto: **i)** generiche o non adeguatamente circostanziate; **ii)** palesemente infondate; **iii)** riferite a fatti e/o circostanze oggetto in passato di specifiche attività istruttorie già concluse, ove dalle preliminari verifiche svolte non emergano nuove informazioni tali da rendere necessari ulteriori approfondimenti; **iv)** "circostanziate verificabili", per le quali, alla luce degli esiti delle preliminari verifiche svolte, non emergono elementi tali da supportare l'avvio della successiva fase di istruttoria; **v)** "circostanziate non verificabili", per le quali, alla luce degli esiti delle preliminari verifiche svolte, non risulta possibile, sulla base degli strumenti di analisi a disposizione, svolgere ulteriori approfondimenti per verificare la fondatezza della Segnalazione.

AL FINE DI ACQUISIRE ELEMENTI INFORMATIVI, L'ORGANISMO DI VIGILANZA HA FACOLTÀ DI:

- svolgere, anche direttamente, nel rispetto di eventuali specifiche normative applicabili, approfondimenti tramite, ad esempio, formale convocazione e audizioni del Segnalante, del Segnalato e/o delle Persone coinvolte nella Segnalazione e/o comunque informate sui fatti, nonché richiedere ai predetti soggetti la produzione di relazioni informative e/o documenti;
- avvalersi, se ritenuto opportuno, di esperti o periti esterni a GETOPEN.

Nel caso in cui la Segnalazione riguardi l'Amministratore Unico o l'Organismo di Vigilanza di GETOPEN, la segnalazione verrà gestita dalla Funzione non segnalata.

6.4 L'esecuzione dell'istruttoria

LA FASE ISTRUTTORIA DELLA SEGNALAZIONE HA L'OBIETTIVO DI:

- procedere ad approfondimenti ed analisi specifiche per verificare la ragionevole fondatezza delle circostanze fattuali segnalate;
- ricostruire i processi gestionali e decisionali seguiti sulla base della documentazione e delle evidenze rese disponibili;
- fornire eventuali indicazioni in merito all'adozione delle necessarie azioni di rimedio volte a correggere possibili carenze di controllo, anomalie o irregolarità rilevate sulle aree e sui processi aziendali esaminati.

Non rientrano nel perimetro di analisi dell'istruttoria, se non nei limiti della manifesta irragionevolezza, le valutazioni di merito o di opportunità, discrezionali o tecnico-discrezionali, degli aspetti decisionali e gestionali di volta in volta operate dalle strutture/posizioni aziendali coinvolte, in quanto di esclusiva competenza di queste ultime.

L'Organismo di Vigilanza, nel corso degli approfondimenti, può richiedere integrazioni o chiarimenti al Segnalante. Inoltre, ove ritenuto utile per gli approfondimenti, può acquisire informazioni dalle Persone coinvolte nella Segnalazione, le quali hanno anche facoltà di chiedere di essere sentite o di produrre osservazioni scritte o documenti. In tali casi, anche al fine di garantire il diritto di difesa, viene dato avviso alla Persona coinvolta dell'esistenza della Segnalazione, pur garantendo la riservatezza sull'identità del Segnalante e delle altre Persone coinvolte e/o menzionate nella Segnalazione.

L'Organismo di Vigilanza cura lo svolgimento dell'istruttoria anche acquisendo dalle Funzioni Aziendali interessate gli elementi informativi necessari, coinvolgendo, come su esposto e se ritenuto opportuno, esperti o periti esterni a GETOPEN.

Le attività istruttorie sono svolte ricorrendo, a titolo non esaustivo, a: **i)** dati/documenti aziendali utili ai fini dell'istruttoria (es. estrazioni da sistemi aziendali e/o altri sistemi specifici utilizzati); **ii)** banche dati esterne (es. info provider/banche dati su informazioni societarie); **iii)** fonti aperte; **iv)** evidenze documentali acquisite presso le strutture aziendali; **v)** ove opportuno, dichiarazioni rese dai soggetti interessati o acquisite nel corso di interviste verbalizzate.

6.5 Reporting

A conclusione di ciascuna attività istruttoria gli esiti degli approfondimenti sono sintetizzati in un report o, per le Segnalazioni "relative a fatti rilevanti" e/o con analisi complesse, in una nota istruttoria, in cui sono riportati:

- un giudizio di ragionevole fondatezza/non fondatezza sui fatti segnalati;
- l'esito delle attività svolte e le risultanze di eventuali precedenti attività istruttorie svolte sui medesimi fatti/soggetti segnalati o su fatti analoghi a quelli oggetto della Segnalazione;
- eventuali indicazioni in merito alle necessarie azioni correttive sulle aree e sui processi aziendali esaminati, adottate dal competente management che viene informato sugli esiti delle analisi.

Inoltre, se all'esito dell'istruttoria emergono:

- possibili fattispecie di rilevanza penale o di responsabilità civile, l'Organismo di Vigilanza può disporre di comunicare le risultanze al Consulente Legale della Società per le valutazioni di competenza; ipotesi di inosservanza di norme/procedure o fatti di possibile rilevanza sotto il profilo disciplinare o giuslavoristico.

Le Segnalazioni chiuse, in quanto palesemente infondate, se non anonime, sono trasmesse all'Amministratore Unico affinché valuti con le altre strutture aziendali competenti se la Segnalazione sia stata effettuata al solo scopo di ledere la reputazione o di danneggiare o comunque di recare pregiudizio alla persona, ai fini dell'attivazione di ogni opportuna iniziativa nei confronti del Segnalante.

Qualora, invece, all'esito della verifica, la segnalazione risulti fondata il responsabile della procedura, in relazione alla natura della violazione, provvederà:

a) a presentare denuncia all'autorità giudiziaria competente;

b) a comunicare l'esito dell'accertamento all'Amministratore Unico, affinchè provveda all'adozione dei provvedimenti gestionali di competenza, incluso se vi sono i presupposti, l'esercizio dell'azione disciplinare;

c) ad adottare gli eventuali ulteriori provvedimenti e/o azioni che, nel caso concreto, si rendano necessari a tutela di GETOPEN.

6.6 Trattamento dei dati personali e conservazione della documentazione

Ogni trattamento dei dati personali è effettuato nel rispetto degli obblighi di riservatezza di cui all'art. 12 del d.lgs. n. 24/2023 ed in conformità alla normativa sulla protezione dei dati personali di cui al Regolamento (UE) 2016/679 (Regolamento Generale sulla

Protezione dei Dati – GDPR), al decreto legislativo 30 giugno 2003 n. 196 e al decreto legislativo 18 maggio 2018 n. 51.

La tutela dei dati personali è assicurata oltre che al Segnalante (per le segnalazioni non anonime) anche alla Persona coinvolta o menzionata nella segnalazione.

Al fine di garantire la gestione e la tracciabilità delle Segnalazioni e delle attività conseguenti, l'Organismo di Vigilanza cura la predisposizione e l'aggiornamento di tutte le informazioni riguardanti le Segnalazioni ed assicura la conservazione di tutta la correlata documentazione di supporto per il tempo strettamente necessario alla loro definizione, e comunque per non più di 5 anni, decorrenti dalla data di comunicazione dell'esito finale.

I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati tempestivamente.

Gli originali delle segnalazioni pervenute in forma cartacea sono conservati in apposito ambiente protetto.

7. GARANZIE E TUTELE

7.1 La tutela dell'identità del Segnalante

Le Segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.

Fatti salvi gli obblighi di legge, l'identità del Segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso dello stesso, a persone diverse da quelle competenti a ricevere o a dare seguito alle Segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli artt. 29 e 32, par. 4, del Regolamento (UE) 2016/679 (Regolamento Generale sulla Protezione dei Dati – GDPR) e dell'art. 2 - *quaterdecies* del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

In particolare, l'identità del Segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità possono essere rivelate solo previo consenso espresso dello stesso:

- nell'ambito del procedimento disciplinare, qualora la contestazione sia fondata, in tutto o in parte, sulla Segnalazione e la conoscenza dell'identità del Segnalante sia indispensabile per la difesa dell'incolpato;

- nell'ambito del procedimento instaurato in seguito a Segnalazioni interne o esterne, se la rivelazione dell'identità del Segnalante o di qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità è indispensabile anche ai fini della difesa della Persona coinvolta. A tal fine, in tali casi è data preventiva comunicazione scritta, al Segnalante delle ragioni della rivelazione dei dati riservati.

Il personale di GETOPEN coinvolto nella gestione delle Segnalazioni è tenuto alla riservatezza dell'identità del Segnalante, delle Persone coinvolte e/o comunque menzionate nella Segnalazione, del contenuto della Segnalazione e della relativa documentazione.

La riservatezza è garantita anche a chi segnala prima dell'inizio o successivamente alla cessazione del rapporto di lavoro, ovvero nel periodo di prova, qualora dette informazioni siano state acquisite nell'ambito del contesto lavorativo oppure nella fase selettiva o precontrattuale.

È, altresì, garantita la riservatezza sull'identità delle Persone coinvolte e/o menzionate nella Segnalazione alla pari di quella che viene assicurata al Segnalante.

La violazione dell'obbligo di riservatezza, fatte salve le eccezioni di cui sopra, può comportare nei confronti dell'interessato l'irrogazione di sanzioni amministrative pecuniarie da parte di ANAC nonché l'adozione di provvedimenti disciplinari da parte della Società, così come previsto dal Modello Organizzativo 231 ("Sistema Disciplinare").

7.2 Misure di protezione

Nei confronti del Segnalante è vietato il compimento di atti ritorsivi, intesi come qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della Segnalazione interna o esterna/Divulgazione pubblica/denuncia, che provoca o può provocare al Segnalante, in via diretta o indiretta, un danno ingiusto.

La protezione è garantita anche al Segnalante anonimo, che ritiene di aver subito ritorsioni ed è stato successivamente identificato.

Le misure di protezione si applicano nei limiti e alle condizioni previste dal capo III del d.lgs. n. 24/2023 e sono estese anche a:

- le categorie di Segnalanti che non rientrano nell'ambito di applicazione oggettivo e/o soggettivo previsto dal d.lgs. n. 24/2023;
- le persone del medesimo contesto lavorativo del Segnalante che sono legate ad esso da uno stabile legame affettivo o di parentela entro il quarto grado, i colleghi di lavoro del

Segnalante che lavorano nel medesimo contesto lavorativo e che hanno con esso un rapporto abituale e corrente;

- gli enti di proprietà del Segnalante o per i quali lo stesso lavora nonché gli enti che operano nel medesimo contesto lavorativo del Segnalante.

Chi ritiene di aver subito una ritorsione in ragione della Segnalazione può comunicarlo ad ANAC.

Gli atti ritorsivi eventualmente assunti in ragione della Segnalazione sono nulli e le persone che sono state licenziate a causa della Segnalazione hanno diritto a essere reintegrate nel posto di lavoro in attuazione della disciplina applicabile al lavoratore.

Ferma restando l'esclusiva competenza di ANAC in merito all'eventuale applicazione delle sanzioni amministrative di cui all'art. 21 del d.lgs. n. 24/2023.

8 DIFFUSIONE E PUBBLICAZIONE DELLA PROCEDURA

La presente procedura è pubblicata sul sito internet della Società www.getopen.it