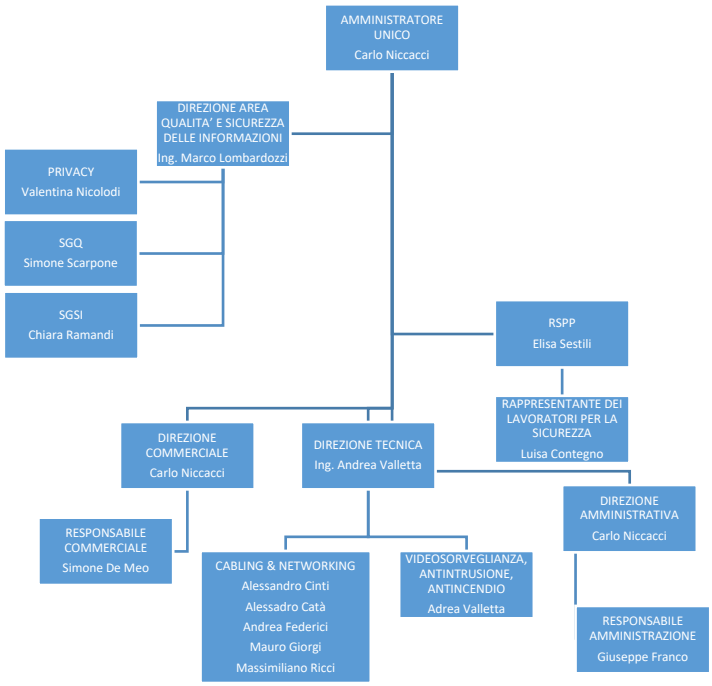
Modello di Organizzazione, gestione e controllo ai sensi del D.lgs. 231/2001 e successive modifiche e integrazioni

Classificazione: pubblico

Data	Revisione	Descrizione	Redatto	Approvato
Ott 2020	0.1	Emissione	RSI	AU
Febb 2021	0.2	Aggiornamento template nuova compagnia		
Febb 2022	0.3	Aggiornamento reati presupposti	RSI	AU

Sommario

L'ORGANIGRAMMA



GLI ORGANI DI GOVERNO

Amministratore unico: Carlo Niccacci

GLI ORGANI DI CONTROLLO

Sono organi di controllo di Stone Security S.r.l. sono i seguenti:

1) **Controllo qualità e sicurezza delle informazioni: Marco Lombardozzi;**
2) **Manutenzione e implementazione: Marco Lombardozzi;**
3) **Verifiche interne (internal audit): Simone Scarpone;**
4) Il **Responsabile del Servizio Prevenzione e Protezione (RSPP)** di cui al d.lgs 81/2008 per la sicurezza dell'ambiente di lavoro: **Elisa Sestili**;
5) L'**Organismo di Vigilanza (organo esterno): Simone Faiella.**

PRINCIPALI DEFINIZIONI ED ABBREVIAZIONI:

- **Attività Sensibili:** attività della società nel cui ambito sussiste il rischio di commissione dei reati di cui al Decreto o rilevanti per la gestione delle risorse finanziarie;
- **CCNL:** Contratto Collettivo Nazionale di Lavoro applicabile ai Dipendenti;
- **Consulenti e Collaboratori:** coloro che agiscono in nome e/o per conto della società sulla base di apposito mandato o di altro vincolo contrattuale di consulenza o collaborazione;
- **Decreto:** Decreto legislativo 8 giugno 2001, n. 231, (di seguito, il "d.lgs. 231/2001" od, alternativamente, il "Decreto") dal titolo "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle assicurazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300*", (con successive modifiche e integrazioni);
- **Destinatari/Esponenti:** Soggetti ai quali è destinato il Modello: Membri degli Organi di governo e controllo, Amministratore unico, Personale amministrativo (Dipendenti e Collaboratori), Consulenti, Partners, Fornitori, terzi in genere;
- **Dipendenti:** tutti i lavoratori subordinati, parasubordinati della società compresi eventuali Dirigenti;
- **Ente:** Stone Security S.r.l. ;
- **Fornitori:** i soggetti, persone fisiche o giuridiche, che, in virtù di specifici contratti, erogano all'Ente servizi o prestazioni;

- **Linee Guida:** le Linee guida redatte da Confindustria per la costruzione dei Modelli di organizzazione, gestione e controllo secondo il Decreto;

- **Modello:** Complesso di principi e di Procedure comportamentali finalizzato a prevenire il rischio della commissione di reati all'interno della società, così come previsto dagli art. 6 e 7 del Decreto, ad integrazione degli strumenti organizzativi e di controllo operanti nella stessa (Atti dell'Amministratore unico, Disposizioni Operative, Ordini di Servizio, Organigramma, Procure, Deleghe, Compendio generale delle informazioni documentate SGI vigente). Il Modello prevede inoltre l'assetto dell'Organismo di Vigilanza e la definizione generale del sistema sanzionatorio-disciplinare;

- **Organismo di Vigilanza:** L'Organismo di vigilanza (di seguito, l' "O.d.V.") previsto dall'art. 6 del Decreto, preposto al controllo del funzionamento e dell'osservanza del Modello e del suo aggiornamento.

Ai sensi citato articolo, una delle condizioni necessarie affinché l'ente non risponda dei reati commessi dai cd. *apicali* o dai cd. *eterodiretti* è l'aver affidato il compito di vigilare sull'effettiva operatività, sul funzionamento, sull'efficacia, sull'osservanza e sull'aggiornamento del Modello a un apposito Organismo dotato di autonomi poteri di iniziativa e di controllo (l'Organismo di Vigilanza, appunto).

- **P.A.:** qualsiasi pubblica amministrazione, inclusi i relativi esponenti nella loro veste di pubblici ufficiali o incaricati di pubblico servizio anche di fatto;

- **Processi Sensibili:** insieme di processi della società nel cui ambito ricorre il rischio di commissione di reati;

- **Protocollo:** insieme delle procedure e delle attività di controllo poste in essere per ciascuna attività sensibile al fine di ridurre a livello "accettabile" il rischio di commissione di reati ai sensi del Decreto;

- **Reati:** i reati rilevanti a norma del d. lgs 231/2001(cosiddetti *reati presupposto*).

PARTE GENERALE

1. II Decreto

Il Decreto Legislativo 8 giugno 2001, n. 231 (di seguito, il "d.lgs. 231/2001" od, alternativamente, il "Decreto") dal titolo "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300*" (in *G.U.* n. 140 del 19 giugno 2001), entrato in vigore il 4 luglio 2001, ha introdotto in Italia un nuovo modello di responsabilità per prevenire la commissione di reati all'interno degli enti collettivi e delle persone giuridiche introducendo la cosiddetta *responsabilità amministrativa* degli enti forniti di personalità giuridica e delle associazioni anche prive di personalità giuridica per i reati commessi dai loro organi o dai loro sottoposti. Tale forma di responsabilità si applica agli enti forniti di personalità giuridica e dunque anche all'Stone Security S.r.l. .

Il d.lgs. 231/2001 è stato successivamente integrato, da ulteriori provvedimenti legislativi: art. 6 della Legge 23 novembre 2001 n. 409 recante "*Disposizioni urgenti in vista dell'introduzione dell'euro*" [art 25-*bis*]; art. 3 del d.lgs. 11 aprile 2002 n. 61 "*Disciplina degli illeciti penali e amministrativi riguardanti le Società commerciali, a norma dell'art. 11 della legge 3 ottobre 2001, n. 366*"[art. 25-*ter*]; art. 3 della Legge 14 aprile 2003 n. 7 "*Ratifica ed esecuzione della Convenzione internazionale per la repressione del terrorismo, fatta a New York il 9 dicembre 1999, e norme di adeguamento dell'ordinamento interno*" [art. 25-*quater*]; art. 5 della Legge 11 agosto 2003 n. 228 "*Misure contro la tratta di persone*"[art 25- *quinquies*]; art. 9 della Legge 18 aprile 2005, n. 62 "*Abusi di mercato*" [art. 25-*sexies*] etc.; *"Reati tributari"* [art. 25-*quinquiesdecies*].

Il complesso delle novelle legislative intervenute sulla base di successive valutazioni politico-criminali ha progressivamente esteso il novero tassativo delle fattispecie di reato dalla cui commissione scaturisce la responsabilità amministrativa degli "Enti". La responsabilità degli enti, difatti, non ha portata generale, ma è circoscritta alle figure di reato espressamente previste dal d.lgs. 231/2001 (cosiddetti *reati presupposto*).

Alcuni punti essenziali del Decreto:

a) Il Decreto prevede un sistema amministrativo-punitivo degli illeciti d'impresa (Enti dotati di personalità giuridica, nonché Società e Associazioni anche prive di personalità giuridica) che va ad aggiungersi al diritto penale delle persone fisiche. La scelta di qualificare come "amministrativa", anziché come "penale", la nuova forma di responsabilità, è frutto della necessità di allentare le consistenti tensioni del mondo imprenditoriale molto preoccupato delle ricadute economiche di tale riforma.

La disciplina è normativamente articolata in modo tale da suscitare l'impressione che il legislatore abbia voluto formalmente definire "amministrativa" una responsabilità che, nella sostanza, assume un volto tutto penalistico: la responsabilità dell'Ente è, difatti, strettamente connessa alla commissione di un fatto di reato espressamente contemplato dal d.lgs. 231/2001, e la sede in cui essa viene accertata è pur sempre il processo penale. Non è un caso se la Corte di Cassazione abbia statuito che ad onta del *nomen iuris*, la nuova responsabilità nominalmente amministrativa, dissimula la sua natura sostanzialmente penale (così Cass., 30 gennaio 2006, in *Dir. e giust.*, 2006).

b) Il giudice penale competente a giudicare l'autore-persona fisica del fatto-reato è anche competente a giudicare l'Ente e ad applicargli la sanzione amministrativa (art. 36).

c) L'Ente collettivo è responsabile ai sensi del Decreto ove il reato sia commesso nel suo interesse o a suo vantaggio, da parte di un soggetto che rivesta un ruolo apicale o subordinato all'interno dell'Ente stesso (art. 5, comma 1). E' esclusa la responsabilità dell'Ente se l'autore del reato agisce nell'interesse esclusivo proprio o di terzi (art. 5, comma 2).

d) Gli articoli 6 e 7 prevedono per l'Ente una forma specifica di esonero dalla responsabilità, qualora esso dimostri di aver adottato ed efficacemente attuato Modelli di Organizzazione, di Gestione e di Controllo idonei a prevenire i reati presupposti, della medesima specie di quello in concreto verificatosi.

e) L'onere probatorio per l'accusa è diverso a seconda che il reato sia commesso da soggetti in posizione apicale o in posizione subordinata: nel primo caso è l'Ente che deve dimostrare l'assenza di colpa per l'organizzazione (in considerazione del fatto che i soggetti apicali esprimono la politica gestionale

dell'Ente); nel secondo caso si ha responsabilità soltanto qualora l'accusa dimostri che la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza posti a carico dell'Ente.

f) Il Modello deve comprendere un sistema di controlli preventivi e di Procedure diretti a programmare la formazione e l'attuazione delle decisioni nell'ambito delle aree e dei processi interni alla società includenti fattori di rischio-reato.

L'efficacia del Modello di Organizzazione, Gestione e Controllo va garantita attraverso: 1) la verifica costante della sua corretta applicazione; 2) l'adozione di un adeguato sistema sanzionatorio-disciplinare. A tale fine, è prevista l'istituzione negli Enti di un Organismo di Vigilanza (O.d.v.), dotato di autonomi poteri di iniziativa, vigilanza e controllo. L'O.d.V. verifica il funzionamento, l'attuazione e la efficacia del Modello nel tempo.

g) Il sistema delle sanzioni è caratterizzato dall'applicazione all'Ente (sempre) di una sanzione pecuniaria, comminata per quote (art. 10, comma 1). Il giudice determina il numero delle quote in relazione alla gravità dell'illecito, al grado di responsabilità dell'Ente, nonché all'attività svolta per l'attenuazione delle conseguenze del reato e in fase di prevenzione della recidiva, e assegna a ogni singola quota un valore economico compreso tra un minimo e un massimo (art. 10, comma 2- art. 11). Nei casi più gravi, oltre alla sanzione pecuniaria, possono essere applicate all'Ente sanzioni interdittive, quali: l'interdizione dall'esercizio dell'attività, la sospensione o la revoca delle autorizzazioni, licenze o concessioni, il divieto di contrattare con la pubblica amministrazione, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi, il divieto di pubblicizzare beni o servizi (art. 13). Tali sanzioni possono essere applicate, su richiesta del Pubblico Ministero, anche in via cautelare, cioè a indagini in corso (art. 45).

Il sistema sanzionatorio include, infine, la confisca del prezzo o del profitto del reato (art. 19) e, nel caso si applichi una sanzione interdittiva, la pubblicazione della sentenza di condanna (art. 18). Al verificarsi di specifiche condizioni, il giudice, in sede di applicazione di una sanzione interdittiva che determini l'interruzione dell'attività dell'Ente, ha la facoltà di nominare un commissario che vigili sulla prosecuzione dell'attività d'impresa, per un periodo che corrisponde alla durata della pena interdittiva applicata.

h) L'Ente non va esente da responsabilità anche quando l'autore del fatto criminoso non sia identificato o non sia imputabile e anche qualora il reato si estingua per una causa diversa dall'amnistia (art. 8).

i) In caso di illecito commesso all'estero, gli Enti che hanno la sede principale nel territorio dello Stato italiano sono comunque perseguibili, sempre che lo Stato del luogo ove il reato è stato commesso non decida di procedere nei loro confronti (art. 4).

l) Nel caso di trasformazione dell'Ente, resta ferma la responsabilità per i reati commessi prima della data in cui la trasformazione ha avuto effetto (art. 28); in caso di fusione, il nuovo Ente risponde dei reati di cui erano responsabili gli Enti partecipanti alla fusione (art. 29); nel caso di scissione parziale resta ferma la responsabilità dell'Ente scisso per i reati commessi prima della data in cui la scissione ha avuto effetto (art. 30 comma 1), gli Enti beneficiari della scissione, sia totale che parziale, sono solidalmente obbligati al pagamento delle sanzioni pecuniarie dovute dall'Ente scisso per i reati commessi anteriormente alla data dalla quale la scissione ha avuto effetto; nel caso di cessione, il cessionario è solidalmente obbligato, fatta salva la preventiva escussione dell'Ente cedente, al pagamento della sanzione pecuniaria (art. 33).

2. Adozione del Modello di Organizzazione, Gestione e Controllo.

Con l'adozione del Modello, la società intende dotarsi di un nucleo essenziale di principi etici e di Procedure che, a integrazione del sistema e degli altri strumenti organizzativi e di controllo interni già esistenti, risponda alle finalità e alle prescrizioni del Decreto in fase di prevenzione dei reati, di controllo dell'attuazione del Modello e dell'eventuale irrogazione di sanzioni disciplinari per inosservanza delle regole ivi previste.

I Destinatari, ovvero gli esponenti della società, sono tenuti al rispetto delle regole di comportamento previste dal Modello, nell'esercizio delle loro funzioni e/o dei loro incarichi nell'ambito delle aree e dei processi considerati a rischio (v. le Parti speciali del Modello).

Il Modello completa gli strumenti organizzativi e di controllo già operanti.

In particolare esso include, mediante anche quanto stabilito nel Codice Etico, principi di carattere giuridico ed etico informativi della filosofia di STONE SECURITY S.R.L. ispiratrice delle scelte e delle condotte di tutti coloro che, a vario titolo e livello, agiscono per conto e nell'interesse della società. Tutti i destinatari del presente documento devono attenervisi, anche nel rispetto delle leggi nazionali e sopranazionali, tenuto conto che tali principi sovraintendono al regolare svolgimento dell'attività aziendale, all'affidabilità della gestione, contribuendo a salvaguardarne l'immagine.

L'adozione del Modello è stata preceduta dall'analisi dei rischi correlati alle attività ritenute a rischio di commissione-reati. L'analisi è stata svolta privilegiando i colloqui con i referenti delle singole funzioni. Nell'elaborazione del Modello si è infine tenuto conto delle Linee Guida elaborate dalle principali associazioni di categoria.

Il Modello si compone di una parte generale illustrativa dei principi, delle finalità che la società si prefigge con la sua adozione, delle strutture generali dell'organizzazione preventiva e di una Parte Speciale illustrativa di alcune delle specifiche tipologie di reati previste dal Decreto in riferimento alle specifiche aree considerate a rischio sulla base dell'analisi effettuata.

Successive modifiche o integrazioni del Modello eventualmente necessarie, tra cui l'adozione di ulteriori parti speciali per nuove tipologie di reato rilevanti per la società, sono di competenza del l'Amministratore unico. L'Amministratore unico ha anche competenza, su impulso dell'O.d.V. e sentiti i Responsabili o referenti interessati, di adottare modifiche progressive del sistema organizzativo per renderlo sempre più conforme al Modello. A tal fine, verranno effettuate verifiche periodiche della

funzionalità del sistema, area per area, rispetto all'osservanza dei principi e delle norme di condotta costitutivi la *policy* della società.

3. Destinatari

Il Modello è destinato a tutti coloro che operano per e con STONE SECURITY S.R.L. , nei limiti di quanto indicato nell'art. 5 del Decreto, quale che sia il rapporto che li lega alla stessa, e in particolare il Modello è destinato ai soggetti preposti alle fasi dei processi a rischio siano essi Membri degli Organi di governo e controllo, dell'Amministratore unico, Personale tecnico amministrativo (Dipendenti e Collaboratori), Consulenti, Partners, Fornitori, terzi in genere.

4. Diffusione, Comunicazione e Formazione

Stone Security S.r.l. provvede ad informare i Destinatari dell'esistenza e del contenuto del Modello, attraverso la collocazione nel sito Web, mediante apposite affissioni nella bacheca (collocata in zona mensa e nel corridoio dei locali di cui al piano rialzato), mettendo a disposizione del Personale amministrativo copie su supporto cartaceo custodite nei propri uffici. La conoscenza effettiva dei contenuti del Modello da parte delle risorse presenti ed operanti nella società e di tutti i soggetti che hanno rapporti con essa è condizione necessaria per assicurare l'efficacia e la corretta funzionalità del Modello stesso oltre che requisito formale richiesto ai fini dell'efficacia esimente. Il personale, ad ogni livello, deve essere quindi consapevole delle possibili ripercussioni dei propri comportamenti e delle proprie azioni rispetto alle regole prescritte dal Modello.

Stone Security S.r.l. provvede, altresì, alla organizzazione di corsi (seminari/ corsi formativi) finalizzati alla divulgazione del Modello e dei principi del Codice etico, nonché a favorire la comprensione delle procedure ed alla formazione del personale amministrativo operante all'interno della società. La formazione potrà essere, altresì, differenziata nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari, dell'esistenza e della tipologia del rischio nell'area in cui operano, della titolarità o meno di poteri di rappresentanza. Al fine di documentare l'efficacia degli interventi formativi sarà

conservato, a cura della società, il registro delle presenze, i supporti didattici erogati nonché saranno somministrati appositi questionari ai partecipanti.

Stone Security S.r.l. , coinvolgendo le singole funzioni interne alla società e l'O.d.V., assicura di predisporre e di svolgere un programma di iniziative per la diffusione, la formazione e la conoscenza del Modello, anche con riferimento agli aggiornamenti e alle integrazioni successive (incontri anche con esperti, distribuzione copie, diffusione e pubblicazione).

La partecipazione ai programmi di formazione sul Modello è obbligatoria ed il controllo sull'effettività della formazione e sui contenuti del programma è demandato all'Organismo di Vigilanza, che svolge altresì un controllo circa la validità e la completezza dei piani formativi previsti ai fini di un'appropriata diffusione, di un'adeguata cultura dei controlli interni e di una chiara consapevolezza dei ruoli e responsabilità delle varie funzioni interne.

Al personale amministrativo verrà richiesto di sottoscrivere una specifica dichiarazione di adesione al Modello ed al Codice Etico, di cui sarà contestualmente consegnata copia, e la stessa procedura dovrà essere seguita in caso di eventuali modifiche e aggiornamenti del Modello.

Anche i membri degli Organi di governo e controllo, all'atto dell'accettazione della loro nomina ovvero all'atto di entrata in vigore del Modello adottato, così come in caso di aggiornamento dello stesso, dovranno sottoscrivere la dichiarazione di impegno all'osservanza e di collaborazione all'applicazione del Codice Etico e del Modello.

5. Organismo di Vigilanza (O.d.V.)

In forza del presente Modello organizzativo, agli organi di controllo precedentemente menzionati, si aggiunge a completare il sistema dei controlli interni, l'**Organismo di Vigilanza** che garantirà un costante scambio di flussi informativi con gli altri organi di controllo.

In attuazione di quanto previsto dal Decreto e tenuto conto del proprio assetto organizzativo, STONE SECURITY S.R.L. si è dotata di un Organismo di Vigilanza monocratico composto da un professionista, iscritto all'Albo degli Avvocati, esperti in Diritto penale dell'impresa, con comprovate pregresse esperienze in materia di responsabilità amministrativa degli enti *ex* d.lgs. 231/2001.

L'Amministratore unico nomina l'O.d.V. che rimane in carica, anche al fine di garantire il predetto requisito della continuità d'azione previsto dalla norma, per la durata di **tre esercizi consecutivi ed è rieleggibile.**

All'O.d.V. sono attribuite le responsabilità di cui al d.lgs. 231/2001, e per questo **gli sono conferiti tutti i poteri necessari alla vigilanza sull'efficace funzionamento e sull'osservanza del Modello**.

All'O.d.V. è anche affidato il potere di proporre all'Amministratore unico modifiche volte ad implementare l'efficacia del Modello stesso.

5.1. I requisiti

Costituisce causa di ineleggibilità a Membro dell'O.d.V. e di incompatibilità alla permanenza in carica: la condanna con sentenza anche di primo grado, o di patteggiamento, per aver commesso un reato non colposo.

Nello specifico, deve possedere i requisiti di:

- **autonomia ed indipendenza:** l'O.d.V. deve trovarsi in una posizione gerarchica indipendente, ossia senza attribuzione di compiti operativi, e deve disporre di autonomi poteri di spesa, nell'ambito di una dotazione finanziaria fissata annualmente dall'organo di Amministrazione, tenuto conto degli equilibri economico – finanziari della società. È inoltre esclusa la possibilità di nominare membro dell'Organismo di Vigilanza colui che si trova in situazione di:

  - conflitto di interessi anche potenziale con l'Ente;

- relazioni di parentela, coniugio o affinità entro il IV grado con gli Organi di governo e controllo e/o con il Direttore Amministrativo;

In caso di nomina di un membro interno, la maggioranza dell'O.d.V. e la Presidenza dello stesso dovrà comunque essere rappresentata da membri esterni al fine di garantire la necessaria autonomia e indipendenza.

- **onorabilità:** non possono essere eletti a componenti dell'O.d.V. coloro i quali:

- si trovano nelle condizioni previste dall'art. 2382 c.c. (*interdizione, inabilitazione, ecc.*)

- siano stati condannati con sentenza irrevocabile o con sentenza non definitiva, anche se a pena condizionalmente sospesa, fatti salvi gli effetti della riabilitazione, per uno dei reati tra quelli cui è applicabile il d. lgs. n. 231/2001 ovvero per altro delitto non colposo per il quale sia stato punti con la pena della reclusione superiore a 5 anni. Per sentenza di condanna si intende anche la sentenza resa ex art. 444 c.p.p.;

- siano stati ritenuti personalmente responsabili per "*omessa e/o insufficiente vigilanza*", all'esito di un procedimento giudiziario svolto in contraddittorio con gli stessi, in relazione all'attività dai medesimi svolta quali componenti dell'Organismo di Vigilanza in seno a enti nei cui confronti siano state applicate le sanzioni previste dall'art. 9 del Decreto per illeciti commessi durante la loro carica;

- abbiano subito l'applicazione delle sanzioni amministrative accessorie previste dall'art. 187 quater del d. lgs. n. 58/1998;

- **professionalità:** l'O.d.V. deve possedere le competenze, tra cui conoscenze di tipo ispettivo ed organizzativo sui sistemi di controllo (organizzazione aziendale, analisi di procedure, ecc.) nonché di tipo giuridico, specie in disciplina penale d'impresa.

- **continuità d'azione:** l'O.d.V. deve garantire un'attività costante e continuativa di vigilanza sul Modello, fornendo pareri consultivi sulla costruzione ed aggiornamento dello stesso. L'O.d.V., a supporto della propria azione e tenuto conto dei contenuti professionali richiesti per l'espletamento dell'attività di controllo, potrà avvalersi, nell'ambito delle disponibilità approvate separatamente nel *budget*, della collaborazione di consulenti esterni, ove richiesta. Nello svolgimento dei compiti assegnati, l'Organismo di Vigilanza ha accesso senza limitazioni alle informazioni per le attività di indagine, analisi e controllo e potrà giovarsi, sotto la sua diretta sorveglianza e responsabilità, della collaborazione delle diverse funzioni e strutture dell'ente ovvero di collaboratori esterni, avvalendosi delle rispettive

competenze e professionalità. A tal fine l'O.d.V. potrà nominare un Segretario dell'Organismo che svolga funzioni di supporto, segreteria e verbalizzazione. All'O.d.V. è inoltre garantito l'utilizzo di idonei locali per le riunioni, audizioni ed altre attività al fine di garantire che le funzioni ad esso affidate siano svolte con assoluta riservatezza.

E' in ogni caso assicurata all'O.d.V. la collaborazione da parte di tutte le strutture appartenenti a Stone Security S.r.l.

In caso di temporaneo impedimento dell'O.d.V., di durata superiore a due mesi, l'Amministratore unico provvede alla nomina di un supplente. Il supplente cessa dalla carica quando viene meno l'impedimento che ha determinato la nomina.

L'O.d.V. ha, inoltre, la responsabilità di disciplinare gli aspetti e le modalità concrete dell'esercizio della propria azione, ivi incluso ciò che attiene ai propri poteri e al relativo sistema organizzativo e di funzionamento.

Nel caso in cui nel corso del mandato dell'O.d.V. venga a scadenza ovvero a cessare per qualsivoglia motivo il mandato dell'Amministratore Unico che l'ha nominato, l'O.d.V. resterà comunque carica fino alla scadenza naturale del triennio, così da garantire la continuità dei controlli.

L'O.d.V. resta in carica fino alla scadenza del mandato, ed esso è rinnovabile da parte dell'Amministratore unico, previa valutazione dell'esatto adempimento di tutti gli obblighi da parte dell'Organismo sopra detto. L'Organismo di Vigilanza cessa per scadenza del termine pur continuando a svolgere, *ad interim*, le proprie funzioni fino all'insediamento del nuovo Organismo di Vigilanza che sarà all'uopo nominato, onde consentire la continuità dei controlli e delle procedure di vigilanza.

5.2. Attività di Vigilanza e di Controllo dell'O.d.V.

Il compito di vigilanza si esplica in via generale nell'esercizio dei poteri di controllo e di ispezione.

All'O.d.V. spetta il compito di vigilare sull'effettiva applicazione del Modello e verificare l'efficienza, l'efficacia e l'adeguatezza del Modello adottato nel prevenire e contrastare la commissione degli illeciti.

All'O.d.V. compete, inoltre, assicurare, con opportune tecniche di monitoraggio, di analisi e di valutazione dei rischi, la rilevazione di eventuali difetti di funzionamento dello stesso, attraverso l'individuazione di elementi indicativi della concreta e/o potenziale commissione di reati all'interno della realtà aziendale. In particolare, l'attività ispettiva e di controllo deve tendere all'individuazione di eventuali punti di debolezza del sistema che potrebbero essere potenzialmente idonei a favorire la commissione dei reati o semplicemente a riscontrare un significativo scostamento tra i comportamenti effettivamente accertati rispetto a quelli codificati.

L'O.d.V. può in qualsiasi momento, anche a sorpresa, in completa autonomia e discrezionalità, procedere a interventi di controllo e verifica in merito all'efficace applicazione del Modello da parte delle singole funzioni e unità operative.

L'O.d.V. potrà richiedere di consultare la documentazione inerente l'attività svolta dalle singole unità e/o funzioni organizzative e dai soggetti preposti alle fasi dei processi a rischio oggetto di controllo o ispezione; potrà inoltre estrarre copia dei documenti rilevanti, effettuare colloqui e richiedere relazioni scritte. Nell'esecuzione di tali operazioni dovrà tenere informato e richiedere la collaborazione del referente della funzione interessata.

L'O.d.V., coordinandosi con i Responsabili delle funzioni interessate dal controllo, deve verificare periodicamente l'idoneità del Modello a prevenire la commissione dei reati di cui alla Parte Speciale.

Sono previste verifiche su singoli atti: periodicamente l'O.d.V. procederà a una verifica a campione di atti nei processi ritenuti a rischio. Sono altresì previste verifiche dei processi della società: periodicamente l'O.d.V. procederà a verificare l'efficacia delle procedure interne e degli altri strumenti organizzativi, specialmente mediante un riesame delle situazioni monitorate; una verifica dello standard di conoscenza del Modello da parte del Personale; un esame delle richieste o segnalazioni pervenute.

Le verifiche ispettive periodiche saranno svolte, ordinariamente, con il supporto del referente della singola funzione interessata.

L'O.d.V., a seguito delle verifiche effettuate, ove emergano all'interno della società nuove situazioni di criticità in ordine al rischio di commissione-reati, proporrà all'Amministratore unico gli adeguamenti del Modello che ritenga necessari od opportuni. Uguale potere di impulso compete all'O.d.V. nell'ipotesi di cambiamenti normativi in materia.

Alla procedura decisionale partecipano anche, in veste consultiva, l'Amministratore unico e i referenti delle funzioni interessate.

L'O.d.V. provvederà ad informare l'Amministratore circa le violazioni accertate che possono comportare una responsabilità dell'Ente ed avviare il relativo procedimento per le eventuali sanzioni disciplinari.

Dovrà l'O.d.V., inoltre, verificare l'idoneità del sistema disciplinare, ai sensi e per gli effetti del d.lgs. 231/2001, e monitorare l'applicazione delle sanzioni in caso di accertata violazione del Modello.

5.3. Reporting dell'O.d.V.

L'O.d.V., in seguito alle ispezioni realizzate nonché al verificarsi di eventuali segnalazioni e/o all'emersione di eventuali criticità, riferisce con diverse linee di *reporting*:

- la prima, su base *continuativa*, direttamente verso l'Amministratore unico o l'eventuale Amministratore munito di specifica delega al fine di informarli tempestivamente, anche per le vie brevi, su eventuali segnalazioni relative a violazioni del Modello, ad innovazioni normative in materia di responsabilità amministrativa degli enti, ovvero alla necessità od opportunità di modificare/aggiornare il Modello;

- la seconda, *annuale*, nei confronti dell'Amministratore Unico al fine di informarlo, mediante relazione scritta, circa l'attività svolta, con particolare riferimento al funzionamento del Modello, alle verifiche effettuate e al piano delle attività, nonché con riferimento ai principali accadimenti rilevanti ai fini 231, dando evidenza di tutte le infrazioni rilevate;

Tali report sono archiviati unitamente a tutte le carte di lavoro dell'O.d.V. a cura dello stesso Organismo di Vigilanza nella figura del suo Presidente e vengono messi a disposizione degli Organi di governo e controllo a loro richiesta.

L'O.d.V. ha inoltre la facoltà di richiedere, per motivi urgenti, la convocazione degli Organi di governo e controllo che, a loro volta, possono convocare l'O.d.V. in qualsiasi momento, salvo adeguato preavviso.

5.4. Rapporti tra Destinatari e Organismo di Vigilanza

L'O.d.V. riferisce, periodicamente o all'occorrenza, all'Amministratore unico, agli Amministratori (salvo i casi di criticità che riguardino proprio quest'ultimo) in ordine all'effettiva attuazione del Modello o in ordine a specifiche situazioni di rischio che si siano eventualmente palesate.

I Destinatari sono tenuti a informare e comunicare all'O.d.V. ogni dato rilevante ai fini dell'assolvimento dei suoi compiti di prevenzione e controllo.

In presenza di problematiche interpretative o di quesiti sul Modello, i Destinatari devono rivolgersi, in via privilegiata, all'O.d.V. per i chiarimenti necessari od opportuni.

L'O.d.V., eventualmente avvalendosi di esperto, è competente a risolvere i conflitti interpretativi concernenti la portata di principi e contenuti afferenti alle procedure di gestione già esistenti e quelli afferenti al Modello.

All'O.d.V. devono essere trasmesse a cura dei referenti delle funzioni coinvolte le informazioni relative ai procedimenti, agli accertamenti e alle verifiche aventi per oggetto le condotte previste nelle Parti speciali del Modello, nonché di tutti quegli eventi che siano in qualsiasi modo attinenti ai reati ivi contemplati.

All'O.d.V. devono essere trasmessi altresì, nel rispetto delle norme sulla segretezza delle indagini, provvedimenti e/o notizie provenienti da autorità di Polizia, dall'Autorità giudiziaria o da altra Autorità, dai quali si evinca lo svolgimento di attività giudiziaria o di indagine, anche contro ignoti, in relazione alla commissione di uno o più dei reati presupposti dal Decreto che possano mostrare collegamenti con Stone Security S.r.l. .

L'O.d.V. deve essere tempestivamente informato di ogni cambiamento significativo avente ad oggetto sia la concreta operatività del Modello che la struttura della Stone Security S.r.l. .

L'O.d.V. di concerto con i referenti delle funzioni interessate, potrà adottare proprie disposizioni operative che stabiliscano modalità e termini per la gestione e la diffusione di notizie, dati e altri elementi utili allo svolgimento dell'attività di vigilanza e di controllo dell'organismo stesso.

5.5. Segnalazioni verso l'O.d.V.

Deve essere garantito l'afflusso di eventuali **segnalazioni e notizie di reato all'O.d.V.**, incluse segnalazioni di natura ufficiosa, da parte di tutti gli esponenti della società, in merito ad eventi che potrebbero ingenerare responsabilità dell'Ente ai sensi del Decreto ovvero che comunque configurino una violazione delle **procedure**, degli obblighi e/o dei divieti fissati dallo stesso **Modello** o del **Codice Etico**.

L'O.d.V. valuterà le segnalazioni ricevute e gli eventuali provvedimenti da assumere. A tal fine, a sua discrezione valuterà l'autore la segnalazione della violazione, motivando in forma scritta eventuali rifiuti di procedere a indagine interna, dandone comunicazione all'Amministratore unico (salvo il caso di un suo conflitto di interessi nella situazione specifica).

La procedura di segnalazione sarà organizzata in modo da tenere indenni i segnalanti da ogni forma di ritorsione, discriminazione o penalizzazione, assicurando la riservatezza della loro identità, fatti salvi peraltro gli obblighi di legge e la tutela della Stone Security S.r.l. e delle persone accusate erroneamente o in mala fede.

Pertanto, chiunque intenda segnalare una violazione (o presunta violazione) del Modello o del Codice Etico deve comunicarla all'O.d.V., tramite i mezzi sotto specificati, anche in forma anonima.

L'indirizzo cui inoltrare le segnalazioni è il seguente:

o.d.v.@ml2net.com.

Le segnalazioni pervenute sono conservate a cura dell'O.d.V. che le valuta e, in caso di accertata violazione, provvede a proporre gli eventuali provvedimenti in conformità a quanto previsto alla successiva sezione dedicata al Sistema disciplinare.

L'O.d.V., nel corso dell'attività di indagine che segue la segnalazione, deve agire in modo da garantire che i segnalanti e i soggetti coinvolti in genere non siano fatti oggetto di ritorsioni, discriminazioni o comunque penalizzazioni, assicurando, quindi, la riservatezza del soggetto che effettua la segnalazione (salvo la ricorrenza di eventuali obblighi di legge che impongano diversamente).

Inoltre, per agevolare l'attività di controllo e di pianificazione degli *audit* dell'O.d.V., tutti i soggetti destinatari del presente Modello, devono immediatamente trasmettere allo stesso le informazioni rilevanti concernenti l'attività della società, incluse:

- qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la P.A. con nota scritta;
- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca che sono in corso indagini, anche nei confronti di ignoti, per reati che possano coinvolgere, direttamente o indirettamente l'Ente;
- richieste di assistenza legale inoltrate da dipendenti in caso di avvio a loro carico di procedimenti per reati, salvo espresso divieto dell'autorità procedente;
- notizie e documenti relativi all'instaurazione ed all'esito di procedimenti disciplinari.

Inoltre è fatto specifico obbligo ai referenti di ogni servizio/funzione di trasmettere all'O.d.V., con cadenza semestrale, una "Attestazione ai fini del D.lgs. 231/2001" con la quale riportano all'O.d.V. eventuali infrazioni al Modello ed alle procedure operative delle quali siano venuti a conoscenza, ovvero attestano la piena conformità delle condotte proprie dei soggetti sottoposti alla loro supervisione alle procedure operative e al Modello, qualora nel periodo di riferimento non siano venuti a conoscenza di alcuna infrazione al Modello ed alle procedure operative vigenti.

Ogni informazione, segnalazione, documentazione attestante i controlli svolti, report, verbali di riunioni previsti nel Modello sono conservati dall'O.d.V. in formato elettronico per un periodo di 10 anni.

L'accesso al database e alla documentazione cartacea è consentito - oltre che ai membri dell'O.d.V., anche successivamente alla cessazione della loro carica - esclusivamente agli Organi di governo e controllo, previa loro richiesta.

6. - Sistema disciplinare

L'art. 6, comma 2, lett. *e)* e l'art. 7, comma 4, lett. *b)* del Decreto stabiliscono espressamente (con riferimento sia ai soggetti in posizione apicale sia ai soggetti sottoposti ad altrui direzione) che l'esonero da responsabilità dell'Ente è subordinato, tra l'altro, alla prova dell'avvenuta introduzione di "*un* ***sistema disciplinare*** *idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*". La predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello è quindi condizione essenziale per assicurare l'effettività del Modello stesso.

Stone Security S.r.l. , pertanto, ha predisposto un sistema di sanzioni disciplinari per le eventuali violazioni delle disposizioni del Modello (in conformità all'art. 6 comma 2 lett. *e)*, e all'art. 7 comma 4 lett. *b)* del Decreto).

Le violazioni del Modello ledono il rapporto di fiducia, trasparenza, correttezza, lealtà, integrità e credibilità che deve intercorrere tra Stone Security S.r.l. e i suoi appartenenti.

Tali violazioni possono determinare, come conseguenza, azioni disciplinari a carico dei soggetti interessati, anche a prescindere dall'instaurazione di un giudizio penale nel caso in cui il comportamento integri una fattispecie di reato. La valutazione disciplinare può inoltre non coincidere con l'eventuale giudizio espresso in sede penale, potendo tale valutazione riguardare anche comportamenti che semplicemente infrangano le regole procedimentali e d'azione previste dal Modello e tuttavia non ancora costituenti reato.

Il tipo e l'entità delle sanzioni verranno applicate, in concreto, in proporzione alla gravità delle mancanze, in base ai seguenti criteri generali di valutazione di maggiore o minore gravità del fatto e della colpevolezza individuali:

a. dolo o colpa della condotta inosservante;

b. rilevanza degli obblighi violati;

e. livello ricoperto di responsabilità gerarchica e/o tecnica;

d. responsabilità esclusiva o con altri che abbiano concorso nel determinare la violazione;

e. professionalità e personalità del soggetto, precedenti disciplinari, circostanze in cui è stato commesso il fatto illecito.

L'irrogazione della sanzione disciplinare sarà ispirata ai principi di autonomia (rispetto all'eventuale processo penale), tempestività, immediatezza, proporzionalità ed equità.

6.1.- Comportamenti sanzionabili

Fermi restando gli obblighi nascenti dalla legge 30 maggio 1970, n. 300 (c.d. "Statuto dei lavoratori") e dalle altre norme di legge applicabili, i comportamenti sanzionabili che costituiscono violazione del Modello sono, a titolo esemplificativo, elencati di seguito in ordine di gravità crescente:

A. violazione di regole o di procedure interne adottate in attuazione del Modello o ivi contenute (ad es., omissione di comunicazioni o false comunicazioni all'O.d.V., ostacolo all'attività dell'O.d.V., omissione di controlli, ecc.);

B. violazione di prescrizioni del Codice Etico;

C. comportamenti diretti al compimento di uno o più reati o comunque idonei ad esporre l'ente alle conseguenze della commissione di reati.

Le sanzioni vengono commisurate al livello di responsabilità ed autonomia operativa del dipendente, all'eventuale esistenza di precedenti disciplinari a carico dello stesso, all'intenzionalità e gravità del suo comportamento (misurabile in relazione al livello di rischio cui la società è esposta).

La violazione delle procedure, dei sistemi di controllo, del Codice Etico e del Modello da parte dei dipendenti costituisce sempre illecito disciplinare. Pertanto: (i) ogni notizia di violazione determinerà l'avvio di un procedimento disciplinare; (ii) all'autore della violazione, debitamente accertata, verrà prescritta una sanzione disciplinare; (iii) tale sanzione sarà proporzionata alla gravità dell'infrazione.

I provvedimenti disciplinari irrogabili nei riguardi dei dipendenti, nel rispetto delle procedure previste dall'articolo 7 dello Statuto dei lavoratori e di altre norme eventualmente applicabili, sono previsti dal CCNL applicabile.

6.2. Ambito di applicazione

Le sanzioni disciplinari potranno essere applicate nei confronti del Personale della Stone Security S.r.l. , che ponga in essere illeciti corrispondenti ai seguenti criteri generali:

1) mancato rispetto delle disposizioni previste dal Modello;

2) mancata o non veritiera evidenza dell'attività svolta relativamente alle modalità di documentazione, di conservazione e controllo degli atti previsti dalle procedure interne in modo da impedire la trasparenza e verificabilità dell'attività stessa;

3) omessa vigilanza dei superiori gerarchici sul comportamento dei propri sottoposti al fine di verificare la corretta ed effettiva applicazione delle disposizioni del Modello;

4) violazione degli obblighi di formazione, aggiornamento o comunicazione al personale in ordine alle procedure e ai contenuti del Modello;

5) violazione e/o elusione del sistema di controllo, poste in essere mediante sottrazione, distruzione o alterazione della documentazione prevista dalle procedure interne ovvero impedendo il controllo o l'accesso alle informazioni ed alla documentazione ai soggetti preposti, incluso l'O.d.V..

6.3. Sanzioni per i lavoratori dipendenti. Criteri specifici.

Le disposizioni del Modello sono parte integrante delle obbligazioni contrattuali assunte dal Personale dipendente (impiegati e quadri).

La violazione di tali disposizioni potrà costituire inadempimento delle obbligazioni contrattuali, con ogni conseguenza di legge, anche in ordine all'eventuale risarcimento del danno, nel rispetto, in particolare, degli articoli 2103, 2106 e 2118 del Codice Civile, dell'art. 7 della legge n 300/1970 ("Statuti dei Lavoratori"), della Legge n. 604/1996 e successive modifiche ed integrazioni sui licenziamenti individuali

nonché dei contratti collettivi di lavoro, compresa l'applicabilità dell'art. 2119 del Codice civile che dispone la possibilità di licenziamento.

In caso di violazione del Modello da parte di personale dipendente non dirigente l'Organo Amministrativo può applicare le sanzioni di seguito elencate, secondo il criterio della proporzionalità:

- rimprovero scritto, multa o sospensione qualora il lavoratore violi le procedure interne previste dal presente Modello o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso, dovendosi ravvisare in tali comportamenti una "non esecuzione degli ordini impartiti dalla società sia in forma scritta che verbale";

- licenziamento con preavviso qualora il lavoratore adotti, nell'espletamento delle attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del presente Modello e diretto al compimento di un reato sanzionato dal Decreto dovendosi ravvisare in tale comportamento un "atto tale da far venire meno radicalmente la fiducia della società nei confronti del lavoratore";

- licenziamento senza preavviso qualora il lavoratore adotti, nell'espletamento delle attività nelle aree a rischio, un comportamento palesemente in violazione delle prescrizioni del presente Modello, tale da determinare il rischio di applicazione a carico della società di misure previste dal Decreto, dovendosi ravvisare nel suddetto comportamento, una condotta tale da provocare "alla società grave nocumento morale e/o materiale" nonché da costituire "delitto a termine di legge".

In caso, invece, di violazione del Modello da parte di personale dirigente, l'Amministratore unico può applicare:

- una sanzione monetaria adeguata rispetto alla violazione;
- nei casi più gravi, ricorrere al licenziamento del dirigente medesimo con o senza preavviso, da prescrivere ai sensi delle disposizioni di legge e del contratto collettivo nazionale applicato.

In ogni caso, nella procedura di irrogazione delle sanzioni è assicurato al dipendente il contraddittorio e il diritto di difesa secondo le disposizioni vigenti.

6.4. Sanzioni per i Dirigenti

Il mancato rispetto delle disposizioni del Modello da parte dei Dirigenti, a seconda della gravità della infrazione e tenuto conto della natura fiduciaria del rapporto di lavoro, potrà comportare nei loro confronti l'adozione di misure sanzionatorie, compresa la risoluzione del rapporto lavorativo nel caso venga leso l'elemento fiduciario, in conformità a quanto previsto dal C.C.N.L. applicabile.

6.5. Misure nei confronti dei Vertici

In caso di violazione delle disposizioni del Modello da parte dei vertici della società, l'O.d.V. informerà l'Amministratore unico, il quale assumerà le opportune iniziative previste dalla normativa vigente. Nei casi più gravi si potrà procedere anche alla revoca della carica su delibera dell'Amministratore Unico.

6.6. Misure nei confronti di Collaboratori, Consulenti e Fornitori

Nei confronti di coloro che operano con Stone Security S.r.l. in qualità di collaboratori, consulenti e fornitori, si potrà procedere al recesso per giusta causa o alla risoluzione del contratto ai sensi dell'art. 1454 e ss. Codice civile, nell'ipotesi in cui i medesimi abbiano posto in essere comportamenti in contrasto con le disposizioni previste dal Modello, tali da comportare l'interruzione del rapporto di fiducia. In caso di mancata osservanza del Modello o del Codice Etico da parte di Consulenti, Collaboratori e Fornitori, l'Amministratore unico dovrà, infatti, contestare agli stessi la violazione rilevata e potrà decidere per l'applicazione di penali e/o per la risoluzione del contratto. Ciò può essere esercitato anche qualora le condotte in violazione del Modello configurino ipotesi di reato e come tali vengano contestate dall'Autorità Giudiziaria, con riserva di richiedere il risarcimento qualora dal comportamento tenuto derivino danni concreti alla società.

A tale scopo, la società prevede un'apposita clausola risolutiva espressa nelle lettere di incarico/contratti stipulati con i collaboratori, i consulenti e/o i fornitori. La società si riserva comunque la facoltà di attendere l'esito del procedimento penale prima di comunicare la risoluzione ai collaboratori consulenti e/o fornitori interessati.

Riguardo alle regole disciplinari applicabili ai lavoratori dipendenti di STONE SECURITY S.R.L. , nel rispetto delle procedure di cui all'art. 7 L. n. 300/1970 (e di eventuali normative speciali applicabili), si farà riferimento - per le violazioni del Modello - agli apparati disciplinari e ai "criteri di correlazione per le mancanze dei lavoratori e i provvedimenti disciplinari" richiamati nelle Contrattazioni collettive di lavoro.

In questo quadro, sono previste le seguenti **sanzioni "progressive"**:

a) rimprovero verbale o scritto, per il lavoratore che violi le procedure interne previste dal Modello, o adotti, nell'espletare attività a rischio-reato, un comportamento non conforme alle prescrizioni del Modello medesimo;

b) multa, per il lavoratore che violi più volte le procedure interne previste dal Modello o adotti, nell'espletamento di attività a rischio, un comportamento più volte non conforme alle prescrizioni del Modello stesso, anche prima che tali mancanze siano state singolarmente accertate e contestate;

c) sospensione dal servizio e dalla retribuzione, per il lavoratore che nel violare le procedure preventive o nell'adottare, nelle attività a rischio, un comportamento difforme dal Modello, arrechi danno alla società;

d) trasferimento per punizione o licenziamento con indennità sostitutiva del preavviso e con trattamento di fine rapporto, per il lavoratore che adotti, nell'espletamento di attività a rischio, un

comportamento non conforme alle prescrizioni del Modello, idoneo e diretto in modo univoco al compimento di un reato;

e) licenziamento senza preavviso e con trattamento di fine rapporto, per il lavoratore che adotti, nell'espletare attività a rischio, un comportamento inosservante della legge penale, manifestamente contrario alle prescrizioni del Modello, e tale da determinare il pericolo di concreta applicazione a carico della società delle sanzioni amministrative previste dal Decreto di riferimento.

L'accertamento delle infrazioni disciplinari e l'irrogazione delle sanzioni sono rimessi agli organismi competenti in virtù delle procedure stabilite, nonché dei poteri e delle attribuzioni loro conferiti dallo Statuto o dal corpo dei regolamenti interni della società.

Il sistema disciplinare viene costantemente monitorato dall'O.d.V. in coordinamento con il referente del Personale. Ogni violazione del Modello, da chiunque commessa, deve essere tempestivamente comunicata per iscritto all'O.d.V., ferme restando le prerogative e le competenze del titolare del potere disciplinare.

L'O.d.V. deve essere altresì informato con tempestività di ogni sanzione disciplinare applicata per violazione delle prescrizioni del Modello.

7. Il Codice etico

Il Codice Etico, che costituisce parte integrante del Modello ai sensi dell'art. 6, comma 3, del d. lgs.231/2001, prevede i criteri generali di comportamento ai quali devono attenersi tutti coloro che, direttamente o indirettamente, temporaneamente o stabilmente, instaurano rapporti con Stone Security S.r.l. . Esso, pertanto, contempla i principi etici essenziali in riferimento al sistema di controllo preventivo rispetto ai reati contemplati nel Decreto.

La sua osservanza si estende a tutto il personale operante all'interno di Stone Security S.r.l. .

Stone Security S.r.l. contestualmente all'opera di rivisitazione/implementazione del Modello ha provveduto alla adozione del proprio Codice Etico, assicurando la piena armonia dei principi in esso consacrati con il Modello aggiornato.

7.1. La relazione tra Modello Organizzativo e Codice Etico

Un elemento essenziale del sistema di controllo preventivo è rappresentato dall'adozione, attuazione e rispetto dei principi etici rilevanti ai fini della prevenzione dei reati previsti dal d. lgs. 231/2001.

Il Codice Etico è quindi parte integrante del Modello di Organizzazione, Gestione e Controllo e ha lo scopo di esprimere il complesso di principi deontologici che l'Istituto pone a fondamento della propria *mission*.

Il Modello e il Codice Etico sono strettamente correlati e devono intendersi quale espressione di un unico corpo di norme, adottate dalla società per promuovere gli alti principi morali di correttezza, onestà e trasparenza in cui crede e a cui uniforma la propria attività. Pur a fronte della diversa funzione assolta dal Modello rispetto al Codice Etico, essi sono redatti secondo principi e procedure comuni, al fine di creare un insieme di regole interne coerenti ed efficaci finalizzate a trovare massima diffusione tra i dipendenti della società.

Nel Codice Etico, a cui si rinvia per esigenza di sintesi, sono quindi illustrati i principi etici fondamentali della società e le norme di condotta di carattere generale.

8. Soggetti esposti e reati presupposto

Il decreto legislativo 8 giugno 2001 n. 231, in vigore dal 4 luglio 2001, ha introdotto –come chiarito- la disciplina della "*responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*", estendendo, per la prima volta nel nostro ordinamento, la responsabilità in sede penale degli enti che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito. L'ampliamento della responsabilità consente pertanto di colpire direttamente il patrimonio degli Enti che abbiano coltivato un proprio interesse o tratto un vantaggio dalla commissione di determinati reati da parte delle persone fisiche – autori materiali dell'illecito penalmente rilevante – che "impersonano" l'ente o che operano, comunque, nell'interesse di quest'ultimo. Il primo comma dell'art. 5 d.lgs. 231/2001 circoscrive però la responsabilità amministrativa dell'Ente ai soli reati commessi "*nel suo interesse o a suo vantaggio*".

Sulla base di quanto disposto dal decreto in oggetto, l'Ente, in quanto persona giuridica, può quindi essere ritenuto responsabile in relazione a taluni reati commessi o tentati nell'interesse e/o vantaggio dell'ente stesso da:

- **persone fisiche che rivestono posizioni "apicali"** (art. 5, comma 1, lett. a) di rappresentanza, amministrazione, direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione ed il controllo dell'Ente stesso;

- **persone sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione "apicale", cd. "eterodiretti"** (art. 5, comma 1, lett. b).

Una delle particolarità della normativa in esame risiede, pertanto, nel binomio "responsabilità penale" di chi materialmente si rende colpevole del reato e "responsabilità amministrativa" (o come più propriamente è stata definita "parapenale") in capo agli Enti.

Per poter imputare all'Ente la responsabilità da reato devono essere però presenti contemporaneamente **due presupposti**: uno di tipo *oggettivo*, l'altro *soggettivo*. Tale norma introduce quindi un primo presupposto "oggettivo" di connessione tra un fatto di reato, commesso dalla persona fisica, e la

persona giuridica. Il secondo presupposto, di carattere "soggettivo", è destinato a creare una particolare connessione tra l'Ente e il terzo autore del reato, rendendo "presunta" la responsabilità del primo, nel caso in cui a commettere un reato siano i soggetti in posizione apicale, a norma dell'art. 6 del d.lgs. 231/2001.

Pertanto, l'addebito di colpevolezza dell'Ente deriva dal fatto che tale categoria di soggetti è legittimata ad esprimere la volontà dello stesso nei rapporti instaurati con i terzi, fino al punto da "personificare" lo stesso Ente giuridico. In questo caso, sarà in capo all'Ente l'onere della prova, dovendo dimostrare che il comportamento del reo non sia stato tenuto nell'interesse o a vantaggio dell'Ente stesso e che il Modello, ancorché idoneo, sia stato eluso fraudolentemente.

Per quanto riguarda invece la responsabilità dei soggetti sottoposti all'altrui direzione, ai sensi dell'art 7 d.lgs. 231/2001, viene presunto, al contrario, il rispetto degli obblighi di direzione e vigilanza da parte dei vertici, attribuendo l'onere della prova alla pubblica accusa. Tra essi si devono ricomprendere i dipendenti, ossia coloro i quali siano legati da un rapporto di lavoro subordinato, ai sensi degli artt. 2094 e 2095 c. c., ma anche coloro i quali, non avendo un rapporto di dipendenza, siano comunque in posizione di subalternità alla direzione e al controllo del vertice dell'Ente, come, ad esempio, i collaboratori coordinati e continuativi.

Come già descritto nel paragrafo precedente, la responsabilità dell'Ente è circoscritta alla commissione, da parte dei soggetti apicali e/o dei sottoposti, di specifiche ipotesi di reato (i cosiddetti ***reati presupposto***) in base alla fattispecie organizzativa ed al settore in cui l'Ente si trova ad operare, sono state analiticamente esaminate nella Parte Speciale del presente Modello di Organizzazione, Gestione e Controllo.

9. Mappatura dei rischi

Stone Security S.r.l. , al fine di dotarsi di un efficace Modello di Organizzazione, Gestione e Controllo, ha attuato una serie di attività preliminari, articolate in diverse fasi, dirette alla costruzione di un sistema di prevenzione e gestione dei rischi conforme con le disposizioni del Decreto e le linee guida di riferimento.

Il processo di analisi si è articolato secondo i seguenti *step* operativi:

- Mappatura dei processi sensibili;
- Definizione e analisi dei rischi di reato potenziali per singolo processo;
- Analisi, valutazione e azione di miglioramento del sistema di controllo preventivo (c.d. Procedure).

9.1. Mappatura dei processi/attività sensibili

In tale fase è stata effettuata un'analisi del contesto organizzativo ed operativo dell'Ente al fine di censire le aree interessate alle potenziali casistiche di reato ed individuare i soggetti interessati all'attività di controllo e monitoraggio. Al fine di analizzare il contesto di riferimento in cui STONE SECURITY S.R.L. opera, l'attività di identificazione dei processi sensibili è iniziata con l'esaminare la documentazione organizzativa della società quale lo statuto, l'organigramma, le procedure, il bilancio annuale e tutta la documentazione ritenuta rilevante.

Si è quindi proceduto da un lato alla somministrazione, ai principali "*KeyOfficer*" di riferimento, di un questionario autovalutativo (*Control risk self assessment*), al fine di ottenere una visione completa delle attività svolte all'interno della società e del grado di proceduralizzazione esistente e percepito, il livello di percezione del rischio oltre che per individuare eventuali *gap* nel sistema di controllo interno. Il lavoro è stato completato dall'effettuazione di alcune interviste ai "*KeyOfficer*", durante le quali sono state esaminate le eventuali deleghe e/o poteri conferiti (sistema delle deleghe) e dettagliati i processi o attività sensibili gestiti e più esposti alla possibile commissione dei reati presupposto di cui al d.lgs. 231/01, sia riferibili direttamente al soggetto interessato, che all'area di competenza.

Attraverso le informazioni fornite dagli intervistati è stato pertanto possibile:

a. individuare le principali attività di competenza dei singoli uffici e le relative criticità potenziali;

b. descrivere le relative modalità di esecuzione, pianificazione e controllo;

c. individuare gli eventuali controlli, istruzioni o presidi attualmente in vigore, atti a mitigare i rischi.

Dalla combinazione delle informazioni rilevate dall'analisi critica della documentazione, dai questionari compilati e dalle interviste è stata elaborata la mappatura dei processi e sono state identificate le aree sensibili a rischio di commissione di reati.

9.2. Definizione e analisi dei rischi potenziali per singolo processo

Con riferimento alle aree sensibili individuate in precedenza e al contesto operativo dell'Ente di riferimento (Stone Security S.r.l.), sono state identificate anche le possibili criticità e rischiosità di violazioni di norme riconducibili al decalogo dei reati presupposto *ex* d.lgs. 231/01.

Tale attività ha permesso di individuare le specifiche categorie di reato in cui possono incorrere i destinatari del presente Modello. Esse sono state messe in correlazione con le aree, i processi e le attività sensibili definendo la cosiddetta "**matrice dei rischi**", strumento operativo di censimento, monitoraggio e controllo del rischio di commissione di illeciti, all'uopo inserito nel presente Modello.

9.3. Analisi, valutazione e miglioramento del sistema di controllo preventivo

Sulla base della matrice dei rischi rilevati, al fine di individuare tutte le misure preventive idonee a limitare il verificarsi degli stessi, in relazione al singolo processo/attività "sensibile", sono state analizzate le procedure ed i controlli in essere al fine di valutarne l'adeguatezza dei Procedure esistenti, ossia la loro attitudine a prevenire comportamenti illeciti (o comunque a ridurne il rischio ad un livello accettabile) e ad evidenziarne l'eventuale commissione.

In particolare, per ciascun processo sensibile sono stati definiti i seguenti elementi:

1. i rischi di commissione di reato associati;

2. le strutture organizzative coinvolte nel processo;

3. il sistema dei presidi e controlli (Procedure) esistenti;

4. gli eventuali ulteriori presidi ritenuti utili per il rafforzamento dei controlli.

Lo scopo di tale valutazione è stato quello di ridurre ad un livello accettabile il rischio di commissione di reato identificato.

Nella Parte Speciale del presente documento, a cui si rinvia, sono trattati per famiglia di reato i processi/attività sensibili rispetto alle singole fattispecie di reato ritenute maggiormente critiche o rilevanti per l'Ente con l'indicazione delle principali ipotesi delittuose astrattamente perpetrabili nonché dei Procedure di prevenzione previsti nei processi a rischio di reato e dei relativi riferimenti alle specifiche procedure di regolamentazione delle c.d. attività sensibili.

9.4. Criteri di analisi dei rischi adottati

La mappatura dei rischi ha comportato l'analisi di impatto potenziale e di inerenza dei reati in esame, tenuto conto del settore in cui opera STONE SECURITY S.R.L. e della tipologia specifica dei servizi offerti. Sulla base delle tipologie di rischio considerate potenziali ed inerenti, si è valutata l'adeguatezza del livello di presidio del sistema di controllo interno.

Una volta determinato l'elenco dei rischi per processo sensibile, si è proceduto ad una classificazione dei rischi come di seguito esposta in funzione dell'impatto e della probabilità, laddove per impatto si intende il pregiudizio che sopporterebbe l'Ente in caso di commissione del reato in esame (anche in relazione alla

previsione o meno di sanzioni interdittive a fronte dello specifico reato) e per probabilità quella di verificazione dell'evento:

- **<u>Rischio "Basso" o Accettabile (valore numerico corrispondente: 1):</u>** la fattispecie di reato può verificarsi con **probabilità estremamente** ridotta e comunque con danni di bassa entità;

- **<u>Rischio "Medio" o Rilevante (valore numerico corrispondente: 2):</u>** le fattispecie di reato possono verificarsi con **probabilità non elevata, ma tuttavia significativa**, ovvero, nel caso si possa verificare con probabilità estremamente ridotta, i relativi danni sono comunque di entità non trascurabile;

- **<u>Rischio "Alto" o Critico (valore numerico 3):</u>** la fattispecie di reato può verificarsi con **elevata probabilità**, ovvero nel caso si verifichi con probabilità ridotta o anche non elevata, i relativi danni sono di entità significativamente elevata.

La valutazione del rischio di controllo, come già precedentemente descritto, è stata formalizzata attraverso apposita '**matrice dei rischi' mediante la quale è stata rappresentata la correlazione tra processo sensibile e reato censito** con relativa evidenza **del grado di adeguatezza** dei presidi previsti dal sistema di controllo interno e del **grado di rischio** in termini di **probabilità/impatto** (basso = verde, medio = giallo, alto = rosso).

		PROBABILITÀ			
		0 - nulla	1 - bassa	2 - media	3 - alta
IMPATTO	0 - nullo	0	0	0	0
	1 - basso	0	1	2	3
	2 - medio	0	2	4	6
	3 - alto	0	3	6	9

Tale matrice è stata individuata assieme alla *governance* della società al fine di condividere, in un apposito piano, le azioni più opportune da perseguire nel tempo per il contenimento dei rischi emersi, secondo criteri di proporzionalità e di impatto potenziale.

In caso di rischio di controllo "Medio" o "Alto" l'Organismo preposto alla Vigilanza del Modello prevedrà il rafforzamento dei controlli sulle operazioni poste in essere nelle aree interessate.

PARTE SPECIALE

10. CARATTERISTICHE DELLA PARTE SPECIALE

La presente Parte Speciale fornisce una descrizione delle attività della società considerate a rischio di commissione dei reati previsti dal Decreto (c.d. **Attività Sensibili**), con particolare attenzione, in relazione a ciascuna Attività Sensibile, alle fattispecie di reato astrattamente configurabili e alle relative modalità di potenziale commissione.

I Reati potenzialmente configurabili nella realtà STONE SECURITY S.R.L. sono stati suddivisi nelle seguenti tipologie:

- Reati contro la Pubblica Amministrazione (Parte Speciale I);
- Reati societari (Parte Speciale II);
- Reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Parte Speciale III);
- Reati di criminalità informatica e trattamento illecito dei dati (Parte Speciale IV);
- Reati di violazione del diritto d'autore (Parte Speciale V)
- Reati di criminalità organizzata (Parte Speciale VI);
- Reati in tema di salute e sicurezza sul lavoro (Parte Speciale VII);
- Reati ambientali (Parte Speciale VIII);
- Impiego di cittadini stranieri il cui soggiorno è irregolare (Parte Speciale IX);
- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (Parte Speciale X);
- Delitti tributari (Parte Speciale XI);

Ciascuna Parte Speciale è stata suddivisa in due Sezioni.

La prima illustra nel dettaglio:

- le **fattispecie di reato** potenzialmente configurabili nella realtà della società;
- le aree di **attività** ed i **processi maggiormente sensibili** in relazione alle fattispecie di reato indicate al punto n. 1;

Nella seconda Sezione ("**SISTEMI DI PREVENZIONE**") sono riportati:

- i **Procedure preventivi di comportamento e di controllo** che i Destinatari del Modello, coinvolti nella singola Attività Sensibile, sono chiamati a rispettare al fine di prevenire la commissione dei reati sopra descritti (per alcune Attività Sensibili è stata prevista l'unificazione delle prescrizioni specifiche in quanto comunemente applicabili);
- i **principi generali** e **regole di condotta** posti a presidio della singola Attività Sensibile (per alcune Attività Sensibili è stata prevista l'unificazione dei principi di controllo in quanto comunemente applicabili);
- i **controlli** periodicamente effettuati dall'O.d.V. con il supporto delle funzioni coinvolte nel processo gestito.

Per quanto concerne i *criteri di classificazione dei rischi* in funzione dell'impatto e della probabilità di verificazione, si rinvia a quanto esposto nel paragrafo 10 (si veda, la "matrice dei rischi") della Parte Generale del presente Modello.

La valutazione del rischio è stata poi formalizzata attraverso una apposita **tabella** mediante la quale è stata rappresentata la **correlazione tra il processo sensibile, il tipologia di reato considerata e gli organi di governo ed amministrativi** operanti all'interno di STONE SECURITY S.R.L. .

PARTE SPECIALE I

REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

QUALI FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

(Artt. 24, 25 e 25 *decies*)

1. Premessa

- ***Nozione di Pubblica Amministrazione, di Pubblico Ufficiale, e di Incaricato di Pubblico Servizio***

Agli effetti della legge penale, è considerato "Ente della Pubblica Amministrazione" qualsiasi persona giuridica che abbia la cura di interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.

La Pubblica Amministrazione comprende, in relazione ai reati previsti nel codice penale, "*tutte le attività dello Stato e degli altri enti pubblici*".

E' anche opportuno richiamare l'art. 1, comma 2, del d.lgs. 165/2001 in tema di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche che definisce come amministrazioni pubbliche tutte le amministrazioni dello Stato.

Non tutte le persone fisiche che agiscono nella sfera e in relazione ai suddetti enti sono soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie criminose richiamate dal d.lgs. 231/2001.

In particolare le figure che assumono rilevanza a tal fine sono soltanto quelle dei "*pubblici ufficiali*" e degli "*incaricati di pubblico servizio*".

Ai sensi dell'art. 357 c.p., è considerato **pubblico ufficiale** "agli effetti della legge penale" colui che "*esercita una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti 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*". 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".

Nell'ambito dei soggetti che svolgono pubbliche funzioni, la qualifica di pubblico ufficiale è poi riservata a coloro che formano o concorrano a formare la volontà della Pubblica Amministrazione. o che svolgono tale attività per mezzo di poteri autoritativi o certificativi, mentre quella di incaricato di pubblico è assegnata dalla legge in via residuale a coloro che non svolgono pubbliche funzioni ma che non curino neppure mansioni di ordine o non prestino opera semplicemente materiale.

Al fine di individuare se l'attività svolta da un soggetto possa essere qualificata come pubblica, ai sensi e per gli effetti di cui agli art. 357 e 358 c.p., ha rilievo esclusivo la **natura delle funzioni esercitate**, che devono essere inquadrabili tra quelle della P.A. Non rilevano invece la forma giuridica dell'Ente e la sua costituzione secondo le norme del diritto pubblico, né lo svolgimento della sua attività in regime di monopolio, né tanto meno il rapporto di lavoro subordinato dell'agente con l'organismo datore di lavoro.

Al fine di individuare se l'attività svolta da un soggetto possa essere qualificata come pubblica, ai sensi e per gli effetti di cui agli art. 357 e 358 c.p., è necessario inoltre verificare se essa sia, o non, **disciplinata da norme di diritto pubblico**, quale che sia la connotazione soggettiva del suo autore, distinguendosi poi - nell'ambito dell'attività definita pubblica sulla base del detto parametro oggettivo - la pubblica funzione dal pubblico servizio per la presenza (nell'una) o la mancanza (nell'altro) dei poteri tipici della potestà amministrativa, come indicati dal comma 2 dell'art. 357 predetto.

- *Individuazione delle aree e delle operazioni a rischio*

I reati indicati nella presente Parte Speciale presuppongono l'instaurazione di rapporti con la Pubblica Amministrazione.

- *Regole di comportamento e procedure*

I rapporti con la Pubblica Amministrazione devono essere tenuti da ciascun Destinatario, nella misura in cui gli stessi siano coinvolti in attività o in operazioni rientranti nelle aree a rischio-reato sopra delineate, ispirandosi ai **principi di lealtà, veridicità, correttezza e trasparenza**.

I rapporti tra STONE SECURITY S.R.L. e la Pubblica Amministrazione non possono in alcun modo compromettere l'integrità o la reputazione di entrambe le parti.

I Destinatari devono astenersi da qualsiasi situazione di possibile conflitto di interessi nei confronti della Pubblica Amministrazione.

I Destinatari devono evitare di porre in essere comportamenti contrari alla legge, tali in particolare da integrare le fattispecie di reato di cui alla presente Parte Speciale.

A tal fine è fatto espresso divieto di:

- promesse o indebite elargizioni di denaro o di altri benefici di qualsiasi natura a pubblici ufficiali o a incaricati di un pubblico servizio o a persone dagli stessi indicati;
- effettuazione di regali o altri omaggi non di modico valore e, in ogni caso, al di fuori delle consuetudini interne alla società in particolari occasioni dell'anno;
- accettazione di regali, omaggi, pressioni, raccomandazioni o segnalazioni di ogni genere che provengano da pubblici ufficiali o da incaricati di un pubblico servizio;
- effettuare prestazioni in favore dei Consulenti e dei Fornitori che non trovino giustificazione nel contesto del rapporto contrattuale instaurato con gli stessi;
- riconoscere compensi a favore dei Consulenti e dei Fornitori che non trovino giustificazione in relazione al tipo di incarico assunto e alle prassi vigenti in sede locale;
- dichiarazioni mendaci a organismi pubblici locali, nazionali o sopranazionali al fine di conseguire erogazioni pubbliche, finanziamenti agevolati o rimborsi;

- destinazione di somme ricevute da organismi pubblici, a titolo di erogazioni, contributi, o finanziamenti a scopi diversi da quelli legalmente o legittimamente previsti.

I rapporti con la Pubblica Amministrazione, nelle aree a rischio, devono essere gestiti in modo unitario ed omogeneo, procedendo alla nomina o all'individuazione di uno o più **Responsabili interni per ogni operazione o serie di operazioni** (in caso di ripetitività delle stesse): se non diversamente indicato, il Responsabile interno corrisponde al Responsabile della funzione competente alla gestione dell'operazione considerata.

Il Responsabile può chiedere informazioni e chiarimenti a tutte le funzioni, alle unità operative o ai singoli soggetti che si occupano o che si sono occupati dell'operazione.

Il Responsabile interno deve informare mensilmente il Referente della funzione, qualora quest'ultimo non sia il responsabile diretto dell'operazione, di tutti gli aspetti significativi dell'operazione stessa, evidenziandone gli aspetti di maggiore o minore criticità.

Il Referente della funzione deve informare periodicamente l'O.d.V. di tutte le operazioni a rischio-reato che vengano svolte.

Nel rapporto con la Pubblica Amministrazione, il Referente della funzione (e chiunque altro agisca per suo conto) deve:

- individuare all'interno della Pubblica Amministrazione. il funzionario che, in ragione del proprio incarico, è il soggetto a cui rivolgersi;
- documentare, quanto più possibile, in forma scritta i rapporti con il soggetto così individuato;
- redigere in forma scritta tutti i contratti, nonché gli incarichi conferiti ai Collaboratori e ai Consulenti;
- astenersi da ogni tipo di pagamento in contanti o in natura;
- astenersi dall'utilizzo di eventuali percorsi privilegiati o conoscenze specifiche acquisite anche al di fuori della propria realtà professionale;
- informare periodicamente, l'O.d.V. dell'attività svolta.

Qualora il rapporto con la Pubblica Amministrazione venga intrattenuto, in base ad apposita autorizzazione e in via eccezionale, da un soggetto interno alla società privo di poteri o deleghe formali specifiche, a tale soggetto è fatto obbligo di:

- relazionare con tempestività e compiutezza il responsabile della funzione interessata sui singoli avanzamenti del procedimento o della negoziazione;
- comunicare, senza ritardo, al responsabile della funzione eventuali comportamenti della controparte pubblica rivolti a ottenere favori, elargizioni illecite di danaro od altre utilità, anche nei confronti di terzi.

Ogni esponente della società è tenuto a segnalare all'O.d.V. eventuali abusi di potere od ostruzionismi, da parte di funzionari pubblici, tesi a ottenere indebitamente la promessa o la dazione di denaro o altra utilità.

- *Segue: adattamento delle Procedure*

Al fine di centrare l'obiettivo-qualità in termini penali-preventivi, nello **svolgimento delle operazioni a rischio** occorre anche che:

- siano ricostruibili la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- non vi sia identità fra coloro che assumono o attuano le decisioni, coloro che devono darne evidenza contabile e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dal sistema procedurale di controllo interno;
- i documenti riguardanti l'attività della STONE SECURITY S.R.L. siano archiviati e conservati con modalità tali da non permetterne la modificazione successiva, se non con apposita traccia;
- l'accesso ai documenti già archiviati sia sempre motivato e consentito solo ai soggetti autorizzati dalle norme interne all'O.d.V..

Per le **operazioni a rischio concernenti la gestione di risorse finanziarie**, la procedura deve prevedere inoltre che:

- siano stabiliti limiti all'autonomo impiego di risorse finanziarie, mediante la fissazione di soglie quantitative coerenti alle competenze gestionali e alla responsabilità organizzative affidate a singoli soggetti;
- il superamento dei limiti detti possa avvenire soltanto nel rispetto delle procedure di autorizzazione e previa adeguata motivazione;
- le operazioni che comportano utilizzazione o impiego di risorse economiche o finanziarie debbano avere una causale espressa ed essere documentate e registrate in conformità ai principi di correttezza professionale e contabile. Il processo decisionale deve essere verificabile;
- l'impiego di risorse finanziarie sia motivato dal soggetto richiedente, che ne attesta la congruità (con motivazione sintetica per operazioni ordinarie, con motivazione analitica per operazioni diverse dalle ordinarie);
- la procedura di firma congiunta per determinate tipologie di operazioni o per operazioni che superino una determinata soglia quantitativa.

Per le **operazioni di incarico a consulenti esterni** le procedure poste in essere dalla società devono prevedere che:

- la nomina dei consulenti avvenga a cura o su indicazione dei vertici della società ovvero nel rispetto delle direttive, anche di carattere generale, dallo stesso impartite;
- non vi sia identità tra chi richiede la consulenza, chi la autorizza e chi esegue il pagamento;

- il vertice della società determini in via preventiva i requisiti di onorabilità, professionalità e indipendenza dei consulenti a cui conferire l'incarico;
- la richiesta di autorizzazione al conferimento dell'incarico a consulenti esterni sia motivata con specifico riferimento ai requisiti anzidetti.

Deve essere incluso il divieto di affidare incarichi professionali, o di intraprendere attività economica diretta con pubblici ufficiali o con incaricati di pubblico servizio che abbiano personalmente partecipato ad operazioni vantaggiose per l'Ente negli ultimi dodici mesi.

Allo scopo di ottimizzare la trasparenza e la veridicità delle procedure nelle aree di criticità a rischio, si effettueranno **verifiche ispettive interne periodiche**, il cui espletamento è affidato all'O.d.V.; verifiche finalizzate all'accertamento del rispetto delle regole procedurali e sostanziali, previste dal Modello, da parte delle singole funzioni e unità organizzative della società.

I Referenti interni posso attuare deroghe alle procedure previste dal Modello in casi di particolare urgenza nella formazione della decisione, ovvero in situazioni di impossibilità temporanea al rispetto delle procedure. Sono previste un'apposita informativa all'O.d.V. e la ratifica a posteriori da parte della dell'organo di indirizzo.

2. Profili generali delle fattispecie criminose di cui agli artt. 24, 25 e 25 decies

Oggetto di analisi della presente Parte Speciale sono i reati che si configurano sul presupposto che l'Ente abbia instaurato rapporti con una Pubblica Amministrazione.

Per Pubblica Amministrazione, o Ente Pubblico, deve intendersi qualsiasi persona giuridica a cui l'ordinamento attribuisce la cura di interessi pubblici, o che svolga attività di natura legislativa, amministrativa o giudiziaria, in forza di norme di diritto pubblico o atti autoritativi[1].

Ai sensi dell'art. 3 del d.lgs. n. 163/2006, sono equiparati alla categoria in esame gli organismi pubblici istituiti, anche in forma societaria, per soddisfare specifici interessi generali, finanziati dallo Stato, da enti pubblici territoriali o da altri organismi di diritto pubblico, oppure la cui gestione sia soggetta a controllo di questi ultimi, ovvero il cui organo di amministrazione, di direzione o di vigilanza sia costituito da componenti dei quali più della metà sia designata dagli enti suindicati, nonché dotato di personalità giuridica.

Sono, altresì, ricompresi nella suddetta categoria gli organi e le Istituzioni appartenenti alle Comunità Europee.

Il bene giuridico tutelato dalle norme incriminatrici che verranno analizzate nel prosieguo deve essere individuato in riferimento ai principi di cui all'art. 97, comma 2 della Costituzione, il quale stabilisce che l'esercizio della pubblica funzione deve avvenire nel rispetto dei principi di buon andamento e imparzialità dell'amministrazione.

Proprio in ragione di tale esigenza, sono puniti anche quei comportamenti posti in essere da privati che, con atti sollecitatori anche di natura fraudolenta ad opera di un soggetto pubblico, siano idonei a turbare il corretto esercizio della funzione amministrativa e, conseguentemente, produrre un danno, anche di natura economica, in capo alla Pubblica Amministrazione nella sua interezza.

Occorre specificare, altresì, che tali reati hanno natura c.d. propria, poiché al fine di una loro realizzazione è necessaria la partecipazione di un soggetto qualificato - un pubblico ufficiale o un incaricato di pubblico servizio – differenziandosi, sotto questo profilo, dai reati c.d. comuni, ovvero che possono essere commessi da chiunque.

[1] A titolo esemplificativo, ma non esaustivo, ci si riferisce: alle amministrazioni dello Stato (Presidenza del Consiglio, Consob, Banca d'Italia, Agenzia delle Entrate, Autorità per l'Energia Elettrica e Gas); la Comunità Europea e Istituti collegati; ASL; INPS; INAIL; Comuni, Province, Regioni.

Pertanto, visto che molti dei reati considerati nella presente Parte Speciale presuppongono le nozioni di "*pubblico ufficiale*" ed "*incaricato di pubblico servizio*", appare necessario descriverne brevemente gli elementi essenziali.

Ai sensi dell'art. 357, primo comma, c.p., 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*": "*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*".

Con riferimento alla nozione di "*funzione legislativa*" e "*funzione giudiziaria*", vista la facile identificazione del ruolo e dei soggetti, il codice non ha ritenuto opportuno esplicitarne analoga definizione.

L'art. 358 c.p. prevede che "*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".

Perché il "servizio" possa definirsi pubblico, deve essere disciplinato (nelle stesse forme della pubblica funzione) da norme di diritto pubblico e atti autoritativi; ma estrinsecarsi al di fuori di poteri di natura certificativa, autorizzativa e deliberativa (propri, invece, dell'attività del pubblico ufficiale).

Il legislatore ha, inoltre, precisato che non può mai costituire "servizio pubblico" lo svolgimento di "semplici mansioni di ordine", né la "prestazione di opera meramente materiale".

La giurisprudenza ha individuato la categoria degli incaricati di un pubblico servizio, ponendo l'accento sul carattere della strumentalità ed accessorietà delle attività rispetto a quella pubblica in senso stretto. In sostanza, trattasi di soggetti che danno un contributo concreto alla realizzazione delle finalità del pubblico servizio, con connotazione di sussidiarietà e di complementarietà esercitando, di fatto, una funzione pubblica.

Essa ha, quindi, indicato 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:

(a) 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;

(b) la presenza di una convenzione e/o concessione con la Pubblica Amministrazione;

(c) l'apporto finanziario da parte dello Stato;

(d) l'immanenza dell'interesse pubblico in seno all'attività economica.

Trattasi di reati che, sotto il profilo dell'elemento soggettivo, sono caratterizzati dal dolo che può essere definito, in linea generale, come la consapevolezza in capo all'agente del reato da commettere e, conseguentemente, la volontà del suo concretizzarsi nella realtà.

Infine, è necessario premettere che nella presente Parte Speciale sono ricompresi due delitti di cui agli artt. 640, comma II e 640 *bis* c.p., ovvero truffa in danno dello Stato e truffa per conseguire erogazioni dallo Stato, i quali non appartengono alla categoria dei tipici reati contro la Pubblica Amministrazione. di cui al Libro II, Titolo II, Capo I del Codice Penale.

Tuttavia, è sembrato opportuno ricomprendere tale previsione nella presente Parte Speciale in ragione della particolare ipotesi di truffa considerata, la quale presuppone comunque l'interazione tra l'agente e la Pubblica Amministrazione.

3. Reati contro il patrimonio dello Stato, di altro ente pubblico o della Comunità europea di cui all'art. 24 del Decreto

3.1. Malversazione a danno dello Stato (art. 316-bis c.p.)

La norma in esame punisce "*chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro Ente pubblico o dalle Comunità Europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità*".

La condotta materiale oggetto di incriminazione è la distrazione, anche parziale, delle somme ottenute dalla P.A., dallo Stato o dalla Comunità Europea, per soddisfare scopi diversi rispetto alla realizzazione di opere o attività di pubblico interesse per cui sono stati rilasciati.

Potrebbe verificarsi, ad esempio, in caso di mancata destinazione dei contributi o finanziamenti ricevuti dallo Stato o da altro Ente pubblico per la specifica esecuzione delle attività finanziate (ad es. Erasmus, formazione) e conseguente impiego degli stessi in altri investimenti e/o attività per le quali l'Ente nutre interesse.

Trattasi di reato istantaneo, la cui consumazione avviene nel momento in cui si realizza la distrazione delle somme.

3.2. Indebita percezione di erogazioni in danno allo Stato o all'Unione Europea (art. 316-ter c.p.)

Tale disposizione, salvo che il fatto costituisca la specifica ipotesi di truffa aggravata per il conseguimento di erogazioni ex art. 640-*bis* c.p., incrimina "*chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestati cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, 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 punita, quindi, la condotta di chi, al fine di ottenere mutui o finanziamenti dallo Stato (includendo anche enti e organi appartenenti all'Unione Europea), utilizza documenti materialmente alterati, dichiarazioni mendaci, ovvero omette informazioni dovute.

Il reato potrebbe realizzarsi, ad esempio, in caso di alterazione da parte del personale di STONE SECURITY S.R.L. di documenti attestanti l'esistenza di condizioni essenziali per ottenere, a titolo esemplificativo, contributi pubblici per uno specifico progetto oppure, nella fase di rendicontazione dello stesso, attraverso la falsificazione di documenti giustificativi delle spese sostenute con evidente vantaggio per l'Ente.

Diversamente dall'ipotesi di reato considerata nel paragrafo precedente, in tal caso non rileva lo specifico scopo per cui le somme indebitamente percepite vengano utilizzate.

Sotto il profilo penale, infatti, assume rilevanza la sola condotta fraudolenta e sleale impiegata per ottenere i finanziamenti predetti, elemento che, unitamente all'erogazione del finanziamento da parte dello Stato o altro Ente pubblico, consuma il reato in esame.

3.3. Truffa ai danni dello Stato (art. 640, comma II, n. 1 c.p.)

La norma punisce "*chiunque, mediante artifizi e raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno*", prevedendo una pena aggravata quando il fatto è commesso *"a danno dello Stato o di altro ente pubblico o col pretesto di farsi esonerare dal servizio militare."*

Il reato si realizza quando la condotta finalizzata a conseguire un ingiusto profitto consista in qualsiasi alterazione della realtà (artifizi e raggiri) tale da indurre in errore lo Stato (inclusi gli Enti pubblici e L'Unione Europea), il quale, procedendo con un atto di disposizione patrimoniale, subisce un danno di natura economica.

Il delitto è integrato quando, a seguito del comportamento ingannevole, si realizza l'ingiusto profitto dell'agente e il conseguente danno in capo allo Stato.

Il reato in esame potrebbe realizzarsi, ad esempio, nel caso in cui, per un accreditamento o l'ottenimento di un finanziamento pubblico, vengano posti in essere artifizi o raggiri per giustificare l'esistenza di requisiti non sussistenti e obblighi mai adempiuti, con ciò causando un nocumento allo Stato o a un altro ente pubblico o dell'Unione Europea;

Nell'ambito della categoria in esame è stata inserita anche tale ulteriore fattispecie che, ad onta della collocazione codicistica conferita dal legislatore, comunque offende gli interessi del buon andamento della Pubblica amministrazione.

Per le stesse ragioni sono state considerate le fattispecie che seguono.

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

Tale fattispecie sanziona chiunque ponga in essere la tipica condotta di truffa di cui all'art. 640 c.p., al fine di ottenere "*contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità Europee*."

La norma in esame non va confusa con la previsione di cui all'art. 316-*ter* c.p. (cfr. par. 2.3.) in quanto quest'ultima fattispecie trova applicazione in via sussidiaria, ovvero solo ove non sia configurabile il reato di truffa *ex* art. 640-*bis* c.p.

Nello specifico, l'elemento differenziante è da ricercare nel requisito degli artifizi e dei raggiri che "assorbono" la condotta materiale del reato di indebita percezione di erogazioni a danno dello Stato (dichiarazioni mendaci o omesse informazioni dovute) tutte le volte in cui i comportamenti suddetti si inseriscano in un contesto artificioso più ampio, finalizzato a rafforzare la portata ingannatoria della condotta principale ed idoneo a indurre in errore il soggetto passivo.

Il delitto si consuma nel momento in cui, a seguito degli artifizi e dei raggiri, lo Stato o altro Ente pubblico eroga il finanziamento richiesto.

La fattispecie potrebbe essere integrata, ad esempio, in caso di alterazione da parte del personale operante presso STONE SECURITY S.R.L. di documenti attestanti l'esistenza di condizioni essenziali per ottenere, a titolo esemplificativo, contributi pubblici per uno specifico progetto oppure, nella fase di rendicontazione dello stesso, attraverso la falsificazione di documenti giustificativi delle spese sostenute con evidente vantaggio per l'Ente di appartenenza.

3.5. Frode informatica in danno allo Stato o di altro Ente Pubblico (art. 640-ter, comma II, c.p.)

La norma incrimina "*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*", prevedendo, al

secondo comma, una pena aggravata quando ricorre una delle circostanze di cui all'art. 640, comma II n.1 (fatto commesso in danno allo Stato o di altro Ente Pubblico).

Ai sensi del terzo comma della norma in commento (inserito dall'art. 9 del D.L. n. 93/2013, convertito dalla legge n. 119/2013) "*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 reato di frode informatica ha la medesima struttura della truffa, differenziandosi solo in relazione al fatto che il comportamento fraudolento non è esercitato direttamente sul soggetto passivo, bensì su un sistema informatico, telematico o sulle relative pertinenze.

La condotta si perfeziona nel momento in cui l'agente interviene, senza avere titolo, sul sistema informatico, alterandone il funzionamento.

3.6. Trattamento sanzionatorio per le fattispecie di cui all'art. 24 del Decreto.

Con riferimento al profilo sanzionatorio, l'integrazione dei reati suddetti comporta l'applicazione all'Ente della sanzione pecuniaria fino a 500 quote.

Inoltre, nell'ipotesi in cui l'Ente abbia tratto un profitto di rilevante entità o abbia causato un danno di particolare gravità, verrà applicata la sanzione pecuniaria da 200 a 600 quote.

Infine, si applicheranno le sanzioni interdittive di cui all'art. 9, comma II, lett. c), d) ed e) del Decreto.

4. Reati contro il buon andamento e l'imparzialità della Pubblica Amministrazione di cui all'art. 25 del Decreto

4.1. Concussione (art. 317 c.p.)

La norma punisce "*il pubblico ufficiale che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità*".

La condotta penalmente rilevante si compone di due momenti fondamentali.

In primo luogo, occorre che il pubblico ufficiale eserciti il c.d. *metus publicae potestatis*, ovvero paventi un esercizio distorto della propria qualifica o dei propri poteri in danno al soggetto passivo.

Un comportamento siffatto deve, altresì, essere tale da costringere la vittima a dare o promettere denaro o altra utilità.

Il reato di concussione si verifica, pertanto, in caso di abuso di potere da parte di pubblico ufficiale o incaricato di pubblico servizio che, *abusando* della sua qualità o dei suoi poteri, *costringa* taluno a dare o promettere denaro o altra utilità a lui o a un terzo.

Per "*costrizione*" deve intendersi quello stato di coartazione del soggetto passivo, rimasto privo di qualsiasi possibilità di determinare il proprio comportamento in direzione contraria rispetto alla prospettazione del male ingiusto (minaccia) paventato dal pubblico ufficiale mediante l'abuso dei propri poteri o qualità.

Infine, il reato si consuma nel momento della dazione o della promessa: sotto quest'ultimo aspetto, ove alla promessa segua la dazione, il perfezionamento del reato coinciderà con tale evento.

Alla luce della recenti modifiche intervenute sulla disciplina dei reati contro la pubblica amministrazione, considerando che nelle ipotesi in esame è previsto quale soggetto attivo del reato proprio il solo pubblico ufficiale - e non l'incaricato di pubblico servizio - e non è punibile il coartato soggetto passivo del reato - a differenza delle ipotesi di corruzione ed induzione indebita a dare o promettere utilità – sono molto limitate e remote le ipotesi di concretizzazione del rischio reato sostanzialmente riconducibili al concorso, da *extraneus*, con il pubblico ufficiale concussore.

4.2. Corruzione per l'esercizio della funzione (art. 318 c.p.)

La norma[2] incrimina "*il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa.*"

Il reato in esame è strutturato secondo la logica del concorso necessario di persone, per cui il delitto, al fine della sua realizzazione, presuppone il contributo sia del corruttore che del pubblico ufficiale corrotto.

Oggetto materiale della condotta è un atto o un comportamento che rientri nelle competenze del pubblico ufficiale, ovvero in quella sfera di attività a cui lo stesso è preposto dalla norma attributiva della pubblica funzione.

Il reato si consuma, alternativamente, al momento della dazione o della promessa. Ne consegue, che ove alla promessa segua il ricevimento del denaro e dell'utilità, il perfezionamento del reato avverrà in quest'ultimo istante.

Il reato potrebbe realizzarsi, ad esempio, in caso di offerta o promessa di denaro o altre utilità da parte di esponenti della società (appartenenti alla *governance*, dipendenti e non) a pubblici ufficiali o incaricati di pubblico servizio al fine di agevolare e far ottenere all'Ente, a titolo esemplificativo, i vantaggi di cui sopra.

Anche in tal caso, gli esponenti della società possono porre in essere la fattispecie di reato in esame come corruttori (secondo l'esemplificazione sopra riportata). Anche in questo caso, ai fini della configurabilità della responsabilità *ex* d.lgs. 231/01, non potranno prendersi in esame i casi in cui la condotta sia stata posta in essere nell'esclusivo interesse o vantaggio del soggetto agente e quindi sarà necessario che la dazione illecita o la promessa di utilità sia avvenuta ad interesse o vantaggio dell'Ente.

4.3. Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)

[2] L'art. 318 c.p. è stato modificato dalla legge 6 novembre del 2012 n. 190 che ha definitivamente abolito la distinzione della corruzione propria nella forma antecedente e susseguente, circoscrivendo il reato al solo evento corruttivo che investa, in generale, la funzione affidata al pubblico ufficiale.

E' punito "*il pubblico ufficiale che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri d'ufficio, riceve, per sé o per un terzo, denaro o altra utilità, o ne accetta la promessa*".

Diversamente dalla previsione di cui al paragrafo precedente, tale ipotesi di corruzione presuppone che il *pactum sceleris* tra il pubblico ufficiale e il corruttore abbia ad oggetto atti specifici di cui, a seconda che l'esercizio della pubblica funzione intervenga prima o dopo l'accordo criminoso[3], se ne richiede l'omissione, il ritardo o la contrarietà ai doveri imposti al pubblico ufficiale dalla norma attributiva del potere.

Con riferimento al momento consumativo del delitto, valgono le medesime considerazioni esposte nel paragrafo che precede con la sola specificazione che, ove l'accordo corruttivo intervenga dopo il compimento dell'atto ad opera del pubblico ufficiale, il perfezionamento del reato si avrà solo se alla promessa segua la dazione.

4.4. Ipotesi aggravata di corruzione per un atto contrario ai doveri d'ufficio (art. 319-bis c.p.)

La norma in esame commina una pena aggravata, rispetto al reato generale di corruzione *ex* art. 319, ove il *pactum sceleris* abbia ad oggetto lo specifico scopo di ottenere "*il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene, nonché il pagamento o il rimborso di tributi*".

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

Tale ipotesi di reato ricorre quando la condotta corruttiva di cui agli artt. 318 e 319 c.p. viene commessa dal pubblico ufficiale "*per favorire o danneggiare una parte in un processo civile, penale o amministrativo*".

E' prevista, al secondo comma, una pena aggravata quando dal reato derivi l'ingiusta condanna di taluno.

---

[3] L'intervento della legge anti-corruzione ha lasciato inalterata la struttura del reato ex art. 319 c.p., ovvero la corruzione nella forma c.d. antecedente o susseguente, a seconda che il compimento dell'atto da parte del pubblico ufficiale venga compiuto prima o dopo la conclusione del patto corruttivo.

Quanto al momento consumativo, si rinvia alle considerazioni espresse nei paragrafi che precedono, essendo ammessa la fattispecie di corruzione in atti giudiziari, sia nella forma c.d. antecedente, che susseguente.

Il reato si potrebbe configurare nel caso in cui l'Ente sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (quale, ad esempio, un magistrato, un cancelliere, un consulente tecnico o altro ausiliario o incaricato dal Giudice).

4.6. Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)

La norma punisce, salvo che il fatto costituisca più grave reato, *"il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità*".

E' punito, altresì, nei casi previsti dal primo comma*, "chi dà o promette denaro o altra utilità".*

La fattispecie in esame sostituisce la vecchia previsione del reato di concussione per induzione *ex* art. 317 c.p., assumendo il rango di norma autonoma a seguito della novella legislativa della legge anti-corruzione (L. n.190/2012).

Per quanto concerne gli aspetti generali, si rinvia al paragrafo dedicato al reato di concussione *ex* art. 317 (cfr. par. 4.1.), dovendo, però, specificare il significato del termine "*induzione*".

Il reato in rubrica presuppone che l'abuso della qualità o dei poteri del pubblico ufficiale siano idonei ad indurre nel soggetto passivo la convinzione di dover dare o promettere denaro o altra utilità.

Tale illecita influenza, però, dispiega un'efficacia meno pregnante rispetto alla "*costrizione*", in quanto la vittima non sarebbe totalmente coartata, ma manterrebbe spazi per autodeterminarsi in senso contrario rispetto alla prestazione richiesta dal pubblico ufficiale.

Il delitto potrebbe configurarsi, ad esempio, laddove un dipendente, in accordo con un pubblico ufficiale che abusi della sua qualità o dei suoi poteri, induca taluno a dare o promettere indebitamente denaro o altra utilità a lui o a un terzo.

Altra ipotesi nella quale può estrinsecarsi tale fattispecie di reato è quella in cui l'esponente di Stone Security S.r.l. sia il soggetto che dia o prometta denaro o altra utilità. Infatti, ai sensi dell'art .319 *quater*, è punibile anche il soggetto passivo del reato.

In ragione di tale requisito, la novella del 2012 ha disposto la punibilità anche del soggetto passivo che porrà in essere la dazione o la promessa.

Infine, sarà imputabile all'Ente la responsabilità per il reato in esame ove si accertasse che la condotta indebita del privato abbia soddisfatto un interesse, o prodotto un vantaggio per l'Ente.

4.7. Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)

Tale norma ha solo lo scopo di chiarire che le fattispecie di corruzione di cui agli artt. 318 e 319 c.p. si applicano anche all'incaricato di pubblico servizio, disponendo, altresì, una pena ridotta in misura non superiore ad un terzo.

4.8. Pene per il corruttore (art. 321 c.p.)

Con riferimento alle pene stabilite agli artt. 318, comma I, 319, 319-*bis*, 319-*ter* e 320 c.p., le stesse si applicano anche al corruttore, ovvero a chi dà o promette denaro a altra utilità al pubblico ufficiale o all'incaricato di pubblico servizio.

4.9. Istigazione alla corruzione (art. 322 c.p.)

È punito "*chiunque offre o promette denaro o altra utilità non dovuti, a un pubblico ufficiale o a un incaricato di pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, qualora l'offerta o la promessa non siano accettate*".

Sono, altresì, sanzionate le offerte o promesse corruttive finalizzate all'omissione o al ritardo di un atto proprio dell'ufficio, nonché all' emissione di un atto contrario ai doveri d'ufficio imposti al pubblico

ufficiale o all'incaricato di pubblico servizio. Questi ultimi, inoltre, sono punibili ove abbiano sollecitato l'offerta o la promessa.

La condotta di reato consiste nella c.d. proposta corruttiva non accettata, la quale, al fine dell'integrazione della fattispecie in esame, deve essere seria, concreta e determinata, ovvero idonea a generare la concreta possibilità che il destinatario possa accettarla.

L'istigazione è consumata anche quando l'offerta è indeterminata, ma è rimesso al ricevente la facoltà di fissarne i punti essenziali[4].

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

Le fattispecie di reato di cui agli artt. 317 e ss. c.p. e sopra analizzate, per l'espresso richiamo che l'art. 25 del Decreto opera in relazione all'art. 322-*bis* c.p., si applicano anche nell'ipotesi in cui il denaro o altra utilità è dato, offerto o promesso (anche a seguito di induzione o istigazione a farlo):

- ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei Conti delle Comunità europee;
- ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
- alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
- ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;
- a coloro che, nell'ambito di altri Stati membri dell'Unione Europea, svolgono funzioni o attività corrispondenti a quelle di pubblici ufficiali e incaricati di pubblico servizio;

[4] Cfr. appendice giurisprudenziale n. 5, Cass. Pen., Sez. VI, 17 ottobre 2011 n. 37402.

- ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale; [5]

- alle persone che esercitano funzioni o attività corrispondenti a quelle di pubblici ufficiali e degli incaricati di pubblico servizio nell'ambito degli Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali ovvero al fine di ottenere o di mantenere un'attività economica o finanziaria.

4.11. Trattamento sanzionatorio dei reati di cui all'art. 25 del Decreto

Ove venisse riscontrata la responsabilità in capo all'Ente, il relativo trattamento sanzionatorio è così ripartito per ciascuna ipotesi di reato prevista all'art. 25 del Decreto:

i) per i delitti di cui agli artt. 318, 321 e 322, commi I e III c.p., si applica la sanzione pecuniaria fino a 200 quote;

ii) per le fattispecie *ex* artt. 319, 319-*ter*, comma I, 321, 322, commi II e IV c.p. si applica la sanzione pecuniaria da 200 a 600 quote;

iii) per i reati previsti agli artt. 317, 319, aggravato ai sensi del 319-*bis* quando dal fatto l'Ente ha conseguito un profitto di rilevante entità, 319-*ter*, comma II, 319-*quater* e 321 c.p. si applica la sanzione pecuniaria da 300 a 800 quote.

Inoltre, le sanzioni predette si applicano all'Ente anche quando tali delitti sono stati commessi dalle persone indicate agli artt. 320 e 322-*bis* c.p.

Ove venisse disposta la condanna dell'Ente per uno dei reati di cui ai nn. 2 e 3 sopra indicati, saranno applicate anche le sanzioni interdittive previste all'art. 9, comma II, del Decreto.

5. Reati contro l'amministrazione della giustizia di cui all'art. 25-decies del Decreto

Di seguito verrà analizzata l'unica fattispecie di reato contro l'amministrazione della giustizia - tra quelle previste dal codice penale - richiamata dal Decreto all'art. 25-*decies*.

5.1. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 377-bis c.p.)

Salvo che il fatto costituisca più grave reato, è punito "*chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere*".

La norma è posta a presidio del corretto svolgimento dell'amministrazione della giustizia contro qualsiasi tipo di ingerenza indebita.

Soggetto passivo del reato deve necessariamente essere taluno che sia stato chiamato a rendere dichiarazioni all'Autorità Giudiziaria.

L'interferenza illecita deve essere idonea a consentire che vengano rilasciate informazioni mendaci, ovvero a indurre l'indagato/imputato ad avvalersi della facoltà di non rispondere, potendo, contrariamente, rilasciare la propria ricostruzione dei fatti.

Il delitto si perfeziona nel momento in cui taluno, chiamato a rendere le dichiarazioni dinnanzi l'Autorità Giudiziaria, pronunci il falso o si avvalga del diritto al silenzio.

5.2. Trattamento sanzionatorio di cui all'art. 25-decies del Decreto

[5] Art. 322 bis, comma 5-bis) inserito dall'art. 10, legge 20 dicembre 2012 n. 237.

Con riferimento al delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria, ove l'Ente venisse condannato, si applicherà la pena pecuniaria fino a 500 quote.

6. Aree a rischio

Stone Security S.r.l. ha frequenti rapporti con pubblici ufficiali o incaricati di pubblico servizio, ad esempio con riguardo ai **processi / sottoprocessi** inerenti a:

- **accreditamento;**
- **gestione rapporti Pubblica Amministrazione / enti finanziatori;**
- **gestione visite ispettive;**
- **finanziamenti pubblici.**

Si è proceduto ad una classificazione dei rischi come di seguito esposta in funzione dell'impatto e della probabilità di verificazione dell'"evento".

Giova sottolineare come, con riferimento a questa specifica categoria di reati, abbia speciale peso anche il piano dell'impatto mediatico, oltrechè giudiziario di una eventuale violazione oggetto di procedimento penale (per l'Ente "amministrativo da reato"). Ai fini, infatti, della valutazione dell'impatto si è tenuto conto anche del danno reputazionale che ne potrebbe derivare.

La valutazione del rischio di controllo, come già precedentemente descritto, è stata formalizzata attraverso apposita '**matrice dei rischi'** mediante la quale è stata rappresentata la **correlazione tra processo sensibile e aree di reato censito** con relativa evidenza **del grado di adeguatezza** dei presidi previsti dal sistema di controllo interno sviluppati in ragione del **grado di rischio** valutato in termini sia di probabilità sia di impatto (si veda, Parte generale §10).

Ciò premesso e tenuto conto dello specifico settore in cui l'Ente opera, sono state individuate le aree a rischio con riferimento alle citate diverse tipologie di reati.

Le aree che saranno di seguito indicate assumono rilevanza anche nelle ipotesi in cui le attività predette siano eseguite, in tutto o in parte, da persone fisiche o giuridiche in nome o per conto dell'Ente, in

virtù di apposite deleghe, o per la sottoscrizione di specifici rapporti contrattuali dei quali deve essere tempestivamente informato l'O.d.V..

All'interno di STONE SECURITY S.R.L. il rischio di commissione di reati contro la Pubblica Amministrazione è strettamente correlato alle seguenti **aree di attività**:

- **rapporti con la pubblica amministrazione;**
- **reclutamento, selezione e gestione del personale**;
- **gestione acquisti;**
- **emissione fatture;**

In particolare, i **processi** e le attività soggette **a maggiore sensibilità** sono le seguenti:

- Gestione dei rapporti di "alto profilo" con Soggetti Istituzionali e/o altri Soggetti appartenenti a Enti pubblici per realizzare canali di comunicazione preferenziali volti alla identificazione di nuove opportunità di business per la società;
- Gestione dei rapporti con Funzionari degli Enti Pubblici finanziatori, nazionali e stranieri per l'aggiudicazione di commesse;
- Gestione della documentazione richiesta dai funzionari pubblici in occasione delle attività di verifica ispettiva anche al fine del mantenimento/rispetto/rinnovo delle autorizzazioni e degli accreditamenti a favore della società;
- Partecipazione a Conferenze di Servizi con rappresentanti di Enti Pubblici;
- Gestione dei rapporti con le autorità di controllo in materia di tutela della salute e sicurezza sul lavoro, anche in sede di verifiche ispettive;
- Gestione dei rapporti con i funzionari pubblici per il rilascio dei certificati attestanti la conformità degli impianti collocati presso Stone Security S.r.l. alla normativa di riferimento;
- Richiesta dei provvedimenti amministrativi necessari per l'avvio dei lavori di costruzione, ristrutturazione e manutenzione degli immobili di proprietà di Stone Security S.r.l. ;
- Gestione dei rapporti con gli Enti Pubblici competenti in caso di verifiche ispettive nei locali dell'Ente;

- Gestione dei rapporti con i funzionari della Guardia di Finanza, l'Agenzia delle Entrate e gli altri Enti competenti in materia fiscale e tributaria, anche in occasione di verifiche, ispezioni e accertamenti presso la società;
- Gestione dei rapporti e delle informazioni dirette alle Autorità Amministrative Indipendenti e/o altri Ministeri o altri Enti vigilanti, anche in occasione di verifiche, ispezioni ed accertamenti;
- Gestione dei rapporti con Funzionari competenti (INPS, INAIL, ASL ecc.) per l'osservanza degli obblighi previsti dalla normativa di riferimento;
- Gestione dei rapporti con i Funzionari Pubblici in occasione di verifiche circa il rispetto dei presupposti e delle condizioni richieste dalla normativa vigente per le assunzioni agevolate;
- Gestione dei rapporti con i Funzionari Pubblici nell'ambito dell'assolvimento all'obbligo di assunzione dei disabili;
- Gestione dei rapporti con l'Ufficio Italiano Brevetti e Marchi, Ufficio Brevetti Europeo o *European Patent Office* - EPO per le attività inerenti a brevetti e marchi;
- Negoziazione, stipula e gestione dei contratti con soggetti pubblici dell'Unione Europea o *extra* europea, ottenuti tramite trattativa privata o partecipazione a procedure a evidenza pubblica;
- Selezione e assunzione del personale dipendente;
- Gestione dei flussi monetari e finanziari di Stone Security S.r.l. ;
- Selezione, negoziazione, stipula ed esecuzione di contratti di acquisto, ivi compresi gli appalti di lavori, riferita a soggetti privati, con particolare riferimento al ricevimento di beni e attività finalizzate all'attestazione di avvenuta prestazione dei servizi e di autorizzazione al pagamento specialmente in relazione ad acquisti di natura immateriale, tra cui: consulenze direzionali, commerciali, amministrativo-legali e collaborazioni a progetto; pubblicità; sponsorizzazioni; spese di rappresentanza; locazioni passive; attività di sviluppo di *software* e servizi ICT;

Di seguito è stata riportata la **matrice dei rischi** nella quale è espressa la correlazione tra la probabilità di verificazione del reato presupposto e l'impatto che lo stesso avrebbe per STONE SECURITY S.R.L. (a tal

proposito si rinvia alla nota metodologica, relativa alla mappatura dei processi e delle attività sensibili e dei rischi ad essi relativi, di cui al paragrafo 10 della Parte generale del presente Modello.

Cod.	**Reati contro la Pubblica Amministrazione**	**Amministratore**	**Delegati – procuratori speciali**
1	Fattispecie selezionate in premessa	Prob. 2 Imp. 3 Rischio: 6	Prob. 2 Imp. 3 Rischio: 6

SISTEMI DI PREVENZIONE:

7. Destinatari

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli operatori nelle aree di attività a rischio, nonché da Collaboratori Esterni e *Partners*, come già definiti nella Parte generale.

Per poter rendere efficace tale sezione, occorre che tutti i Destinatari sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che, quindi, adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

8. Protocolli preventivi

Ferma restando la specificazione operativa resa nel Manuale delle Procedure, si osserva che al fine di prevenire la commissione dei reati contro la Pubblica Amministrazione, STONE SECURITY S.R.L. si è

dotata di un sistema organizzativo, formalizzato da organigramma, mansionigramma per le figure chiave, procedure dettagliate, istruzioni e regolamenti in modo tale da garantire:

- **separazione di funzioni**, all'interno di ciascun processo ritenuto sensibile, tra il soggetto che ha il potere decisionale, il soggetto che lo esegue e il soggetto che lo controlla;
- **definizione di ruoli** con particolare riferimento alle responsabilità, rappresentanza e riporto gerarchico;
- **formale conferimento di poteri**, mediante apposita delega ovvero attraverso il rilascio di una specifica procura scritta, a tutti coloro (dipendenti, membri degli organi sociali, collaboratori, consulenti, ecc.) che intrattengono per conto di STONE SECURITY S.R.L. rapporti con la Pubblica Amministrazione;
- **conoscibilità, trasparenza e pubblicità delle responsabilità** attribuite mediante apposite comunicazioni indirizzate al personale interno (ordini di servizio, circolari, ecc.) ovvero rese conoscibili ai terzi interessati, con particolare riguardo ai soggetti appartenenti alla Pubblica Amministrazione;
- **tracciabilità** di contatto personale o documentale rilevante attraverso l'utilizzo di appositi verbali dell'incontro e moduli di report, aventi adeguato livello di formalizzazione;
- **divieto di accettare omaggi o regalie**;
- previsione di specifici **meccanismi di controllo e monitoraggio**, finalizzati alla rilevazione di eventuali anomalie e/o violazioni delle procedure;
- previsione di livelli autorizzativi e **tracciabilità dei processi decisionali**.

Per quanto strettamente attiene agli **incontri con esponenti delle Pubbliche Amministrazioni** e, più in genere, i Rapporti con la Pubblica Amministrazione, STONE SECURITY S.R.L. si è dotata di una **specifica procedura** con la quale ha previsto, tra l'altro:

- **obbligo di lasciare traccia documentale delle riunioni** intercorse con i Pubblici Ufficiali e gli incaricati di pubblico servizio, contenente, tra l'altro, l'oggetto della riunione, la sede, i partecipanti, la data, l'ora di inizio e fine, indicazione di eventuali anomalie;

- regole di comportamento in occasione di detti incontri;
- partecipazione a detti incontri di almeno due esponenti della società;
- **verbalizzazione/relazione degli incontri più rilevanti**;
- ***report*** **periodico verso l'O.d.V. degli incontri effettuati** con esponenti della Pubblica Amministrazione
- divieto di promettere e/o offrire e/o corrispondere ai rappresentanti della Pubblica Amministrazione, anche su induzione di questi ultimi e direttamente o tramite terzi, somme di denaro o altre utilità in cambio di favori, compensi o altri vantaggi per la società;
- divieto di effettuare pagamenti o riconoscere altre utilità a collaboratori, o altri soggetti terzi che operino per conto della società, che non trovino adeguata giustificazione nel rapporto contrattuale ovvero nella prassi vigenti;
- divieto di concedere promesse di assunzione a favore di chiunque e, specificatamente, a favore di, rappresentanti della Pubblica Amministrazione, loro parenti e affini e / o soggetti segnalati;
- divieto di distribuire ai rappresentanti della Pubblica Amministrazione italiana e straniera omaggi o regali, salvo che si tratti piccoli omaggi di modico o di simbolico valore, e tali da non compromettere l'integrità e la reputazione delle parti e da non poter essere considerati finalizzati all'acquisizione impropria di benefici. Eventuali richieste esplicite o implicite di benefici da parte di un pubblico ufficiale o di un incaricato di pubblico servizio, salvo omaggi d'uso commerciale e di modesto valore, debbono essere respinte ed immediatamente riferite al proprio superiore gerarchico;
- divieto di presentare presentare ad organismi pubblici nazionali e stranieri dichiarazioni non veritiere o prive delle informazioni dovute nell'ottenimento di finanziamenti pubblici, ed in ogni caso compiere qualsivoglia atto che possa trarre in inganno l'Ente pubblico nella concessione di erogazioni o effettuazioni di pagamenti di qualsiasi natura;
- divieto di destinare somme ricevute da organismi pubblici nazionali o stranieri a titolo di contributo, sovvenzione o finanziamento a scopi diversi da quelli cui erano destinati;
- divieto di rappresentare, agli Enti finanziatori, informazioni non veritiere e/o non complete o eludere obblighi di legge / normativi, ovvero obbligo di agire nel più assoluto rispetto della

legge e delle normative eventualmente applicabili in tutte le fasi del processo, evitando di porre in essere comportamenti scorretti, a titolo esemplificativo, al fine di ottenere il superamento di vincoli o criticità relative alla concessione del finanziamento, in sede di incontro con Funzionari degli Enti finanziatori nel corso dell'istruttoria;

- divieto di ricorrere a forme di pressione, inganno, suggestione o di captazione della benevolenza del pubblico funzionario, tali da influenzare le conclusioni dell'attività amministrativa;

- divieto di omettere gli obblighi ed i presidi di controllo previsti dall'Ente in ambito della gestione dei flussi finanziari (i.e. limite impiego risorse finanziarie, procedura di firma congiunta per determinate tipologie di operazioni, espressa causale impiego di risorse, etc.), in conformità ai principi di correttezza professionale e contabile, al fine di orientare in proprio favore le decisioni in merito all'ottenimento di concessioni, licenze ed autorizzazioni dalla Pubblica Amministrazione.

Per quanto concerne poi il **processo acquisti**, l'Ente

- provvede alla qualificazione dei fornitori (affidabilità) e, in linea di principio, vengono presi in considerazione come parametri i seguenti aspetti, anche in base al Compendio generale delle informazioni documentate SGI vigente di cui la società è già dotata:

  a) Capacità di soddisfare pienamente le specifiche richieste in base ai rapporti contrattuali e alla qualità attesa;

  b) Chiarezza e flessibilità nella definizione e nel rispetto dei contratti di fornitura;

  c) Eventuali titoli certificativi posseduti dal fornitore o possibilità di esibire attestati di conformità e/o prove documentali di test di verifica già effettuati dallo stesso.

- La qualifica del fornitore, viene esplicitata con un giudizio sul fornitore che può risultare Qualificato, Qualificato con Riserva, Non Qualificato e solo i fornitori che hanno raggiunto la votazione minima, possono essere inseriti nell'Elenco Fornitori Qualificati, ossia costituiranno i **fornitori a cui rivolgersi in via preferenziale**;

- I contratti tra la società ed i consulenti sono definiti per iscritto in tutte le loro condizioni e termini e contengono clausole standard per il rispetto del Codice Etico,del Modello e del d.lgs. 231/2001 ed i relativi provvedimenti in caso di mancato rispetto;

- La corresponsione di onorari o compensi ai collaboratori e consulenti esterni coinvolti nell'erogazione dei servizi è soggetta ad un preventivo controllo volto a valutare la qualità e l'effettiva erogazione della prestazione e la conseguente congruità del corrispettivo richiesto, che deve essere in linea con le tariffe e/o i prezzi di mercato; non è consentito riconoscere compensi in favore dei collaboratori e consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto, che deve in ogni caso essere documentalmente provato e della documentazione comprovante l'effettivo svolgimento dell'incarico deve essere tenuta traccia a cura dell'Ente.

Inoltre Stone Security S.r.l. ha strutturato il **processo relativo agli acquisti** secondo le seguenti modalità idonee alla prevenzione di condotte delittuose:

- l'ufficio che evidenzia il bisogno o, in alternativa, la Vice Presidente o il Consigliere delegato, invia una mail alla Logistica;
- successivamente si procede alla convalida del bisogno da parte del Direttore Amministrativo;
- per i lavori e le manutenzioni si procede con la richiesta di tre o più preventivi;
- delle deliberazioni della commissione viene redatto verbale;
- all'esito, si procede alla sottoscrizione l'ordine di acquisto ed esso viene conservato in duplice copia da parte dell'ufficio acquisti;
- lo stesso ufficio acquisti procede poi alla consegna di una copia alla ragioneria, unitamente alla fattura;
- alla consegna della merce l'ufficio acquisti procede alla verifica della stessa.

9. Principi generali di comportamento e modalità di attuazione

Scopo della presente Parte Speciale è quello di fornire adeguati sistemi comportamentali da adottare per scongiurare la concretizzazione del rischio di commissione dei reati elencati dai quali deriverebbe l'attivazione del sistema sanzionatorio previsto dal Decreto, ove venisse riscontrata la responsabilità dell'Ente.

Tali regole di condotta si applicano a tutti i Destinatari del Modello ed, in particolare, a tutti coloro i quali svolgono le proprie mansioni nelle aree di rischio segnalate nei paragrafi che precedono, inclusi i soggetti esterni alla società.

La diffusione e l'attuazione di detti sistemi sono rimessi all'Amministratore unico della società, in collaborazione con l'O.d.V..

I Destinatari sono tenuti a conoscere e rispettare tutte le regole di cui alla presente Parte Speciale, nonché:

- il Codice Etico;
- il sistema disciplinare;
- le procedure interne adottate per l'assunzione e la formazione del personale nonché per contrastare la verificazione dei reati in oggetto;
- le procedure interne adottate per la gestione dei rapporti e delle comunicazioni con la Pubblica Amministrazione;
- le procedure interne adottate per la gestione dei rapporti con i fornitori.

Stone Security S.r.l. obbliga tutti i destinatari del presente Modello:

- ad osservare tutte le leggi ed il corpo di regolamenti che disciplinano le diverse attività svolte all'interno della società e ad impegnarsi, nei limiti delle rispettive competenze, ad operare affinché sia rispettato quanto previsto dalla normativa in materia;
- ad instaurare e mantenere rapporti con la Pubblica Amministrazione basati su criteri di massima correttezza e trasparenza;
- nel caso in cui emergano, nell'ambito del rapporto con la Pubblica Amministrazione, criticità di qualsiasi natura o conflitto di interesse deve esserne data, con nota scritta, tempestiva comunicazione all'Organismo di Vigilanza;
- a porre particolare attenzione all'attuazione e al controllo degli adempimenti richiesti dalla Pubblica Amministrazione e riferire immediatamente al superiore gerarchico e all'Organismo di Vigilanza eventuali situazioni di irregolarità o anomalie nel rispetto delle modalità di segnalazione prescritte;

- a tracciare tutti i contatti, anche attraverso annotazioni nelle relative pratiche, con i funzionari pubblici. Redigere un verbale delle riunioni intercorse con i Pubblici Ufficiali e gli incaricati di pubblico servizio, contenente, tra l'altro, l'oggetto della riunione, la sede, i partecipanti, la data, l'ora di inizio e fine. Nel caso di riunioni rilevanti per l'attività di Stone Security S.r.l. ovvero di particolari criticità ai fini del rischio *ex* d.lgs. 231/01, provvedere a trasmettere un apposito verbale all'Organismo di Vigilanza per informarlo dei fatti intercorsi; segnalare immediatamente all'O.d.V. qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione o di un incaricato di pubblico servizio o di episodi di tentativi di corruzione di cui si dovesse essere destinatario o semplicemente venirne a conoscenza; nel caso la segnalazione sia stata effettuata al Responsabile, lo stesso deve trasmettere tempestivamente la segnalazione ricevuta all'O.d.V.;
- a rendere noti tutti i conflitti di interessi, reali o potenziali, e discuterli con la propria Area di afferenza, astenendosi dal prendere parte alle decisioni in cui tali interessi sono coinvolti.

E' fatto espresso **divieto** - per tutti i Destinatari ed i collaboratori esterni (questi ultimi debitamente istruiti con apposite clausole contrattuali) - di:

- adottare comportamenti che, in modo diretto o indiretto, possano integrare le fattispecie di reato di cui agli artt. 24, 25 e 25 *decies* del Decreto;
- assumere posizioni di palese conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dai delitti sopracitati;
- ostacolare, con violenza o minaccia, il regolare corso della giustizia.

In particolare, **è assolutamente proibito**:

- emettere fatture per prestazioni non realmente erogate;
- effettuare pagamenti in contanti o in natura, fatta eccezione per procedure di piccola cassa;
- ricevere e/o erogare denaro o altra utilità - sia volontariamente che su sollecitazione, direttamente o per interposta persona - nei confronti di pubblici ufficiali o incaricati di pubblico servizio, a loro coniugi ovvero discendenti, fratelli, sorelle o a persone da loro indicate, salvo che il fatto si verifichi (in conformità con quanto previsto anche dal Codice di comportamento dei dipendenti pubblici) in occasione di festività in cui sia tradizione lo scambio di doni o, comunque, questi

siano di tenue valore, o si riferisca a contribuzioni, nei limiti consentiti dalla legge, in occasione di campagne elettorali;

- distribuire e/o ricevere regali o accordare vantaggi di qualsiasi natura - di propria iniziativa o su sollecitazione - a pubblici ufficiali o incaricati di pubblico servizio che possano influenzare la terzietà o l'indipendenza di giudizio, ovvero indurre a fornire specifici vantaggi alla società;
- pagare o promettere denaro o altra utilità a seguito di una attività di induzione posta in essere da un pubblico ufficiale o un incaricato di pubblico servizio;
- assumere pubblici ufficiali ed incaricati di pubblico servizio ovvero *ex* impiegati della Pubblica Amministrazione, anche delle Comunità europee, nei due anni successivi al compimento di un atto discrezionale, di competenza di uno dei predetti soggetti, da cui sia derivato un vantaggio per la società. Il divieto sussiste anche per le ipotesi di omissione o ritardo di un atto con effetti svantaggiosi per la società;
- rilasciare promesse di assunzioni che non siano basate su criteri di merito, competenza, professionalità ma, diversamente, consistano in veri e propri favoritismi o forme clientelari privilegiate;
- attribuire compensi o prestazioni a soggetti esterni (ad es. consulenti, revisori o altri professionisti) che non trovino giustificazione in alcun tipo di incarico affidato, nonché versare compensi per prestazioni mai svolte;
- presentare dichiarazioni materialmente alterate, o dal contenuto mendace, ad organismi pubblici nazionali o appartenenti all'ordinamento comunitario, al fine di conseguire contributi o finanziamenti agevolati;
- distrarre eventuali erogazioni concesse dallo Stato, dagli Enti pubblici o dalla Comunità Europea per scopi diversi rispetto a quelli a cui erano destinati.

Per quel che riguarda la prevenzione del rischio-reato connesso alla gestione dei rapporti con la Pubblica Amministrazione:

- sono state definite con apposite deleghe i soggetti abilitati alla movimentazione dei conti correnti e delle risorse finanziarie in genere, prevedendone i limiti di utilizzo;

- al fine di assicurare una gestione trasparente dei rapporti con la Pubblica Amministrazione, sono stati previsti da parte dei soggetti a ciò appositamente delegati, puntuali obblighi informativi nei confronti dell'Amministratore unico sull'andamento e sull'esito di ogni pratica in essere;

- è fatto obbligo di respingere ogni tentativo di induzione alla dazione indebita di denaro o altra utilità proveniente da un pubblico ufficiale o un incaricato di pubblico servizio; in tale evenienza, la persona contattata deve segnalare tempestivamente l'episodio, secondo le modalità stabilite da procedure interne, sia all'amministrazione che all'Organismo di Vigilanza;

- è fatto espresso divieto influenzare o determinare le decisione dei soggetti operanti per nome e per conto della Pubblica Amministrazione con violenza, forza o inganno;

- nel caso di ispezioni da parte della Pubblica Amministrazione (ad es. forze dell'ordine), ci si dovrà far rilasciare dall'Autorità procedente una copia, da conservare presso la società, di ogni provvedimento concernente tale circostanza (ad es. decreto di ispezione, perquisizione e relativi verbali), unitamente alla documentazione del relativo procedimento;

- i fornitori devono essere selezionati in base a criteri di scelta individuati nel rispetto della legislazione regionale, nazionale e comunitaria ed in base alla loro capacità di fornire prodotti o servizi rispondenti per qualità, costo e puntualità;

- gli incarichi di consulenza esterna devono essere conferiti solo in presenza di reali esigenze della società, redatti per iscritto, contenere una descrizione chiara e precisa della prestazione da eseguire ed il relativo compenso. Prima di procedere al conferimento, gli accordi presi devono essere approvati dalla/e figura/e interna/e alla società competente e la relativa documentazione dell'incarico deve essere debitamente archiviata;

- i professionisti esterni sono tenuti ad informare la società e l'Organismo di Vigilanza circa l'esistenza di eventuali criticità riscontrate nell'espletamento dell'attività affidata, soprattutto nelle ipotesi in cui vengano individuati comportamenti che potrebbero favorire, in linea generale, la violazione del Modello e, nello specifico, il verificarsi di una delle ipotesi di reato di cui alla presente Parte Speciale.

Per quel che riguarda la prevenzione del rischio-reato connesso alle attività di erogazione/gestione dei finanziamenti pubblici:

- sono stati previsti appositi sistemi di controllo volti a garantire la veridicità delle dichiarazioni rilasciate alla Pubblica Amministrazione, o ad organismi pubblici comunitari, anche per ottenere finanziamenti;

- si è garantita una separazione tra le attività di coloro che istruiscono e decidono delle pratiche di finanziamento e coloro che sono preposti ad attività di controllo sui pagamenti, ovvero sulla destinazione dei contributi erogati, prevedendo l'immediata segnalazione all'Organismo di Vigilanza in caso di riscontro di eventuali irregolarità.

Per quel che riguarda la prevenzione del rischio-reato di frodi informatiche:

- è stata prevista la separazione di funzioni tra chi svolge le attività di gestione delle procedure informatiche, di controllo degli accessi fisici, logici e della sicurezza del *software* (ad es. responsabile dei sistemi informativi) e chi utilizza le risorse informatiche (utenti);

- è stato previsto l'accesso al sistema informatico attraverso *password* e *login* nominativi, in modo da evitare accessi non autorizzati.

Per quel che riguarda la prevenzione del rischio-reato di induzione a rendere dichiarazioni mendaci innanzi all'Autorità giudiziaria o estera:

- ogni qual volta si abbia notizia di un procedimento penale dal quale possa derivare un coinvolgimento dell'Ente, si diffida ciascun Destinatario del Modello dal porre in essere violenza o minaccia, ovvero dal dare o promettere denaro o utilità, affinché il soggetto indagato/imputato renda dichiarazioni menzognere, o eserciti la propria facoltà di non rispondere, potendo invece esporre liberamente la propria rappresentazione dei fatti.

10. Controlli O.d.V.

L'Organismo di Vigilanza verifica periodicamente tramite apposita programmazione degli interventi e con il supporto delle altre funzioni competenti:

- il **sistema di deleghe e procure** in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative, raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al delegato o vi siano altre anomalie;
- le **segnalazioni** eventualmente provenienti, attraverso i canali appositamente predisposti, da tutti coloro che operano per conto dell'Ente in relazione ad eventuali comportamenti delittuosi, quali ad esempio richiesta di indebiti vantaggi o tentativi di concussione compiuti da funzionari della PA o tentativi di corruzione da personale interno;
- i **flussi finanziari della società**, ed in particolare controlla, le riconciliazioni contabili bancarie e di cassa, le uscite di cassa ed il rispetto dei limiti dei pagamenti/incassi in contanti; controlla, inoltre la documentazione della società con particolare riferimento alle fatture passive, liberalità, donazioni e sponsorizzazioni;
- le attività connesse alle Aree a Rischio per verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello, Codice Etico (***reporting*** **verso gli organi deputati**, ecc.);
- le commesse contrattualizzate, verificando a campione i contratti stipulati e le procedure utilizzate per l'acquisizione della commessa, gli eventuali collaboratori utilizzati, verificando per questi ultimi la contrattualizzazione degli stessi, l'attività concretamente svolta dai medesimi, l'assenza di rapporti con soggetti politicamente esposti, la fatturazione e i flussi finanziari corrispondenti;
- le **procedure di selezione del personale**, anche con specifico riferimento agli inserimenti lavorativi di soggetti svantaggiati, acquisendo, anche a campione, la documentazione delle procedure di selezione suddette;
- gli **acquisti di beni o servizi**, avendo cura di verificare, anche a campione, l'effettiva prestazione del servizio o consegna del bene da parte del fornitore, la congruità del prezzo e l'insussistenza di rapporti con soggetti politicamente esposti, con rappresentanti degli enti clienti ovvero con esponenti della società;
- le **consulenze affidate**, anche a professionisti esterni, avendo cura di verificare i criteri utilizzati per la scelta del professionista ed il conferimento dell'incarico, l'effettiva prestazione della consulenza, anche mediante acquisizione della relativa documentazione, la congruità del

prezzo e l'insussistenza di rapporti con soggetti politicamente esposti, con rappresentanti degli enti clienti ovvero con esponenti della società.

Per lo svolgimento di tali verifiche, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione rilevante.

PARTE SPECIALE II

REATI SOCIETARI

QUALI FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

(Art. 25 *ter*)

1. I reati societari

Le fattispecie oggetto della presente Parte Speciale attengono alla eterogenea categoria dei reati societari, posti a tutela di beni giuridici diversificati. Ne deriva il carattere di tendenziale "plurioffensività" di tali reati. Può sostenersi che a seguito della riforma del complessivo diritto societario intervenuta nel 2002, si è passati da una concezione dei reati societari ispirati da un primario interesse di salvaguardia dell'ordine economico nazionale, ad un'altra che privilegia, prevalentemente, ma non esclusivamente, la tutela di interessi di natura patrimoniale.

In dottrina ed in giurisprudenza si sono identificati i beni giuridici protetti dalle norme in esame nella trasparenza societaria; nella salvaguardia dell'integrità del capitale sociale e del patrimonio sociale; nella correttezza della vita sociale, *sub specie* di regolare funzionamento dell'assemblea ed effettività del dovere di pubblicità; nel regolare svolgimento del potere di controllo e della funzione di vigilanza, interni od esterni alla società; nel corretto andamento del mercato.

Data la struttura societaria di Stone Security S.r.l. tali fattispecie risultano applicabili. Anche in ragione dei principi di trasparenza e correttezza di cui tali fattispecie si fanno portatrici, se ne tratta nel presente Modello.

Ai fini che qui interessano, per l'integrazione delle contravvenzioni, come per i delitti, è necessaria la sussistenza del dolo.

Molte delle fattispecie in questione sono formulate dal legislatore come reati propri, per la cui integrazione è previsto che i soggetti agenti rivestano determinate qualifiche o funzioni (di caso in caso: amministratore, direttore generale, dirigente, sindaco, liquidatori, ecc.).

L'art. 2639 c.c. prevede, in via generale, che – ai fini dell'integrazione di tali reati - al soggetto formalmente titolare della qualifica o della funzione, è equiparato quello che esercita di fatto la qualifica o la funzione.

Reati di cui all'art. 25-ter del Decreto

1.1. False comunicazioni sociali (art. 2621 c.c.) e False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 c.c.)

La disciplina delle fattispecie di false comunicazioni sociali è stata modificata dalla legge n. 69/2015.

Ai sensi dell'art. 2621 c.c. fuori dai casi previsti dall'art.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, 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 dall'Ente per conto di terzi.

Trattasi di reato proprio, ovvero commesso da soggetti qualificati (amministratori, direttori generali, dirigenti, sindaci e liquidatori) muniti di poteri di amministrazione e gestione, nonché di controllo sull'operato delle *governance*.

Il nuovo testo dell'art. 2622 cc. invece, dispone che gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, 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 consapevolmente espongono fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta

dalla legge sulla situazione economica, patrimoniale o finanziaria della società, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da tre a otto anni.

Alle società indicate nel comma precedente sono equiparate:

1) le società emittenti strumenti finanziari per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;

2) le società emittenti strumenti finanziari ammessi alla negoziazione in un sistema multilaterale di negoziazione italiano;

3) le società che controllano società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;

4) le società che fanno appello al pubblico risparmio o che comunque lo gestiscono.

Le disposizioni di cui ai commi precedenti si applicano anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

La nuova disciplina prevede pene ridotte (da 6 mesi a 3 anni) per il reato di falso in bilancio di cui all'art. 2621 c.c. "*se i fatti sono di lieve entità*" (art. 2621-*bis*). La lieve entità viene valutata dal giudice, tenendo conto "*della natura e delle dimensioni della società e delle modalità o degli effetti della condotta*". La medesima pena ridotta si applica nel caso in cui il falso in bilancio riguardi le società che non superano i limiti indicati dall'art. 1 comma 2 del R.D. 16 marzo 1942, n. 267 e che, dunque, non possono fallire. In tale ultimo caso, "*il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale*".

Il provvedimento introduce poi un nuovo art. 2621-*ter* che - ai fini dell'applicazione della nuova causa di non punibilità per particolare tenuità del fatto di cui all'art. 131-*bis* c.p. - stabilisce che il giudice debba in tal caso valutare "*in modo prevalente l'entità dell'eventuale danno cagionato alla società*".

Per quanto di maggior interesse ai nostri fini, il provvedimento, infine, ha tendenzialmente inasprito le sanzioni pecuniarie a carico dell'Ente previste dall'art. 25-*ter* del Decreto, in relazione ai reati di falso in bilancio.

Si precisa che:

- soggetti attivi del reato sono gli amministratori, i direttori generali, i dirigenti preposti alla relazione dei documenti contabili dell'Ente, i sindaci ed i liquidatori. Si tratta, dunque, di un reato proprio, che può essere commesso da soggetti che ricoprono anche di fatto determinate qualifiche;

- nella nozione di "comunicazione sociale" rientrano tutte le comunicazioni previste dalla Legge dirette ai soci o al pubblico, ivi compresi il progetto di bilancio, le relazioni, i documenti da pubblicare ai sensi degli artt. 2501 *ter*-2504 *novies* c.c. in caso di fusione o scissione, ovvero in caso di acconti sui dividendi, a norma dell'art. 2433 *bis* c.c.;

- l'esposizione di fatti non rispondenti al vero o l'occultamento di informazioni la cui comunicazione è imposta dalla Legge può essere realizzata non soltanto attraverso la materiale alterazione dei dati contabili, ma anche attraverso una valutazione estimativa artificiosa di beni o valori inseriti in dette comunicazioni (ad esempio, valutazioni estimative in materia di immobilizzazioni materiali o finanziarie che fanno parte del patrimonio dell'Ente, compiuta in difformità dai criteri indicati nella relazione o da quelli previsti dalla Legge o sulla base di parametri comunque irragionevoli);

- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;

- I fatti falsi, esposti od omessi, devono essere "rilevanti" e concretamente idonei ad indurre in errore i destinatari delle predette comunicazioni;

Il reato può essere commesso, secondo i criteri generali di imputazione di cui all'art. 5 del Decreto, nell'interesse o a vantaggio dell'Ente nel caso, ad esempio, di creazione di riserve occulte illiquide, ottenute attraverso la sottovalutazione di poste attive o la sopravvalutazione di quelle passive per favorire l'autofinanziamento dell'impresa sociale ovvero coprire eventuali perdite intervenute nell'esercizio sociale.

Le sanzioni a carico dell'Ente sono le seguenti:

- per il delitto di false comunicazioni sociali previsto dall'articolo 2621 del codice civile, la sanzione pecuniaria da duecento a quattrocento quote;
- per il delitto di false comunicazioni sociali di lieve entità previsto dall'articolo 2621-*bis* del codice civile, la sanzione pecuniaria da cento a duecento quote;
- per il delitto di false comunicazioni sociali previsto dall'articolo 2622 del codice civile, la

sanzione pecuniaria da quattrocento a seicento quote;

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

Ai sensi dell'art. 2625 c.c. 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 consiste nell'ostacolare o impedire lo svolgimento delle attività di controllo e/o di revisione - legalmente attribuite ai soci, ad organi sociali o a Società di Revisione - attraverso l'occultamento di documenti od altri idonei artifici.

Il reato, imputabile esclusivamente agli amministratori, può comportare la responsabilità dell'Ente soltanto nell'ipotesi in cui la condotta abbia causato un danno.

La fattispecie si configura non solo quando, attraverso l'occultamento di documenti o attraverso altri idonei artifici, siano impedite le predette attività, ma anche quando siano solamente ostacolate.

Ai fini della presente norma, vengono in considerazione le attività poste in essere dall'Amministratore unico, nonché dai dipendenti che prestino collaborazione a questi ultimi, che possono avere influenza sulle iniziative e sulle attività di controllo spettanti ai soci, agli altri organi sociali o alle società di revisione.

Si tratta, più precisamente, delle attività che influiscono:

- sulle iniziative di controllo dei soci previste dal codice civile e dagli altri atti normativi, quali ad esempio ad esempio l'art. 2422 c.c. che prevede il diritto dei soci di ispezionare i libri sociali;

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

La fattispecie incrimina "*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*".

Il secondo comma della norma in commento prevede che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Il delitto in esame mira a tutelare le garanzie patrimoniali dei creditori sui beni dell'Ente ove esso sia debitore.

Conseguentemente, il reato è integrato nell'ipotesi in cui l'organo di *governance* disponga di procedere ad operazioni di particolare rilevanza con la consapevolezza e lo specifico intento di pregiudicare il diritto dei creditori.

Si tratta quindi di un reato che può essere commesso con qualsiasi condotta che abbia come effetto quello di cagionare il danno ai creditori.

1.4. Corruzione tra privati (art. 2635 c.c.)

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, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni. Si applica la stessa pena se il fatto è commesso da chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo.

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, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuti 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'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.

Fermo quanto previsto dall'articolo 2641, la misura della confisca per valore equivalente non può essere inferiore al valore delle utilità date, promesse o offerte

La condotta penalmente rilevante è il c.d. patto corruttivo che intercorre tra un privato ed i membri di organi societari, affinché quest'ultimi compiano od omettano specifici atti in violazione degli obblighi inerenti la funzione ricoperta e in cambio di denaro o altra utilità.

Il delitto si consuma nel momento della promessa, ovvero della dazione ove questa effettivamente intervenga.

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

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.

Nella prima forma di manifestazione del reato sopra riportata (quello che viene definito delitto di *false comunicazioni alle autorità pubbliche di vigilanza*), l'ostacolo all'esercizio delle funzioni delle autorità di vigilanza[6] viene concepito come fine della condotta dell'agente (trattasi di fattispecie di mera condotta a dolo specifico), mentre nella seconda forma di manifestazione (quello che viene definito delitto di *ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza*) l'ostacolo costituisce l'evento dell'illecito.

Le modalità di estrinsecazione della condotta di false comunicazioni possono consistere nella formulazione di informazioni false all'interno delle comunicazioni obbligatorie, nonché nell'occultamento mediante qualsiasi mezzo fraudolento di fatti che avrebbero dovuto essere dichiarati obbligatoriamente, sempre con riferimento alla situazione economica, patrimoniale o finanziaria dell'Azienda.

Con riferimento al reato di ostacolo, l'esercizio della funzione di vigilanza deve essere ostacolato in modo rilevante. L'ostacolo può essere frapposto con qualsiasi mezzo, dunque anche con una condotta omissiva.

[6] A titolo esemplificativo, ma non esaustivo: CONSOB e Banca d'Italia. Inoltre, sul punto cfr. appendice giurisprudenziale n. 4, Cons. di Stato, Sez. IV, 21 luglio 2005 n. 3914.

2. Trattamento sanzionatorio a carico di STONE SECURITY S.R.L. in caso di realizzazione delle fattispecie di cui all'art. 25-ter del Decreto

In relazione ai reati sopra elencati, qualora venisse accertato che il fatto è stato commesso nell'interesse della società dagli amministratori, direttori generali o liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si sarebbe realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica, si applicano le seguenti sanzioni pecuniarie a carico della società:

- per il delitto di false comunicazioni sociali, prevista dall'articolo 2621 c.c., la sanzione pecuniaria da 200 a 400 quote;
- per il delitto di false comunicazioni sociali previsto dall'articolo 2621-*bis* la sanzione pecuniaria da 100 a 200 quote;
- per il delitto di false comunicazioni sociali previsto dall'articolo 2622 c.c., la sanzione pecuniaria da 400 a 600 quote;
- per il delitto di impedito controllo, previsto dall'articolo 2625, secondo comma c.c., la sanzione pecuniaria da 200 a 360 quote;
- per il delitto di operazioni in pregiudizio dei creditori, previsto dall'articolo 2629 c.c., la sanzione pecuniaria da 300 a 660 quote;
- per i delitti di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, previsti dall'articolo 2638, primo e secondo comma c.c., la sanzione pecuniaria da 400 a 800 quote;
- per il delitto di corruzione tra privati, nei casi previsti dal terzo comma dell'articolo 2635 c.c., la sanzione pecuniaria da 200 a 400 quote.

Qualora l'Ente, in seguito alla commissione dei reati sopra indicati, abbia conseguito un profitto di rilevante entità, le sanzioni pecuniarie in concreto applicabili vengono aumentate di un terzo.

3. Aree a rischio

Come anticipato, oggetto della presente Parte Speciale sono i cd. "reati societari". Per quanto ai presenti fini interessa, si tratta di fattispecie le cui condotte vengono poste in essere da soggetti che ricoprono specifici ruoli all'interno della società (ad es. amministratori, esponenti della società), cagionando, in linea generale, un danno nei confronti della società stessa e dei suoi creditori.

Le attività che possono aver rilievo in ordine alla prevenzione del rischio dei reati societari sono:

- **gestione dei rapporti con il personale**, con inclusione degli aspetti contabili, economici, giuridici, assicurativi, previdenziali e sociali;
- **tenuta e conservazione dei libri obbligatori, delle scritture contabili e del Modello di organizzazione e controllo *ex* d.lgs. 231/01**;
- predisposizione, tenuta e conservazione di qualsiasi dichiarazione e comunicazione avente valore o rilievo fiscale per la società, ai fini delle imposte dirette e indirette e di qualsiasi altra tassa o contributo;
- **qualunque attività di carattere amministrativo od operativo funzionale** o direttamente connessa alla conduzione della società.

Tenuto conto dell'attività principalmente svolta da STONE SECURITY S.R.L. , sono state rilevate le seguenti **attività a rischio:**

- la formazione di documenti inerenti alla situazione economica, patrimoniale e finanziaria della società;
- la predisposizione di prospetti informativi o notizie sullo stato patrimoniale, produttivo ed economico della società da divulgare all'esterno;
- approvazione progetto di bilancio;
- deliberazione operazioni;
- gestione controlli e verifiche interne;
- la gestione di rapporti e comunicazioni con Autorità pubbliche di Vigilanza;
- comunicazione informazioni;
- gestione risorse finanziarie.

Di seguito è stata riportata la **matrice dei rischi** nella quale è espressa la correlazione tra la probabilità di verificazione del reato presupposto e l'impatto che lo stesso avrebbe per STONE SECURITY S.R.L. (a tal proposito si rinvia alla nota metodologica, relativa alla mappatura dei processi e delle attività sensibili e dei rischi ad essi relativi, di cui al paragrafo 10 della Parte generale del presente Modello.

Cod.	**Reati societari**	**Amministratore**	**Delegati – procuratori speciali**
2	Fattispecie selezionate in premessa	Prob. 2 Imp. 3 Rischio: 6	Prob. 2 Imp. 3 Rischio: 6

SISTEMI DI PREVENZIONE:

4. Destinatari

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli operatori nelle aree di attività a rischio, nonché da Collaboratori Esterni e *Partners*, come già definiti nella Parte Generale.

Per poter rendere efficace tale sezione, occorre che tutti i Destinatari sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che, quindi, adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

5. Protocolli preventivi

Per la presente parte si rinvia alla specificazione operativa resa nel Manuale delle Procedure.

6. Principi generali di comportamento e modalità di attuazione

Scopo della presente Parte Speciale è quello di fornire adeguati sistemi comportamentali da imporre per scongiurare la concretizzazione del rischio di commissione dei reati oggetto di analisi, dai quali deriverebbe l'attivazione del sistema sanzionatorio previsto dal Decreto ove venisse accertata la responsabilità dell'Ente.

Tali regole di condotta si applicano a tutti i Destinatari del Modello e, in particolare, a tutti coloro che svolgono le proprie mansioni nelle aree di rischio segnalate nel paragrafo che precede, inclusi i soggetti esterni alla società.

La diffusione e l'attuazione di detti sistemi sono rimessi all'Amministratore unico, in collaborazione con l'O.d.V..

I Destinatari sono tenuti a conoscere e rispettare tutte le regole di cui alla presente Parte Speciale, nonché:

- il Codice Etico STONE SECURITY S.R.L. ;
- il sistema disciplinare delineato dal Corpo dei Regolamenti interno alla società;
- le procedure interne per la gestione ed il trattamento delle informazioni riservate e per la comunicazione all'esterno di documenti e informazioni;
- i processi amministrativo - contabili per la formazione del bilancio di esercizio;
- il complesso della situazione contabile della società e le regole di gestione;
- le procedure imposte per lo svolgimento di azioni significative e gestione delle situazioni di interesse;
- le regole per l'affidamento di consulenze o incarichi a professionisti esterni;
- le istruzioni per la gestione dello sconfinamento del fido rilasciato a ciascun cliente;
- i Procedure adottati per la richiesta di emissione di garanzie bancarie e per la negoziazione di valute estere;
- le normative afferenti al sistema di controllo interno.

E' fatto espresso divieto a tutti i Destinatari e i collaboratori esterni - debitamente informati con apposite clausole contrattuali - di:

- tenere condotte di qualsiasi natura tali da integrare i reati societari suddetti;

- assumere comportamenti contrari ai principi di correttezza e trasparenza, ovvero in violazione di legge o regolamenti, nonché contrari alle procedure della società, previste per lo svolgimento di tutte le funzioni di gestione e per le comunicazioni esterne delle informazioni sullo stato patrimoniale, economico e finanziario della società. In particolare, si diffida chiunque dall'alterare o riportare dati falsi in relazione alla stesura dei prospetti informativi, nonché con l'intenzione di rappresentare in modo non veritiero la situazione economica e finanziaria della società;

- porre in essere condotte che, se pur lecite, possano favorire, direttamente o indirettamente, la commissione dei reati di cui sopra;

- in relazione alla formazione del bilancio e alla tenuta delle scritture contabili, con particolare riferimento all'Amministratore unico, i Destinatari sono diffidati dall'approvare, alterare o falsificare i dati predisposti e contenuti in dette scritture, dovendosi attenere ai principi e alle prescrizioni vigenti per garantire le fondamentali esigenze di trasparenza e veridicità dei documenti predetti;

- ostacolare il regolare funzionamento degli organi della società, con particolare riferimento alle attività di controllo interno sulla gestione sociale previste dalla legge;

- tenere comportamenti finalizzati, mediante atti materiali o qualsiasi mezzo fraudolento, ad ostacolare le attività di controllo;

- omettere il rilascio di comunicazioni chiare, complete e tempestive nei confronti delle Autorità pubbliche di Vigilanza, ovvero occultare o esporre fatti non corrispondenti al vero, nonché porre in essere qualsiasi condotta fraudolenta diretta ad ostacolare l'esercizio delle funzioni affidate all'Autorità predette;

- effettuare operazioni lesive dei diritti dei creditori;

- effettuare od offrire denaro o altre liberalità finalizzate ad ottenere trattamenti di favore nella conduzione di attività della società, incluse controparti italiane o estere che possano influenzare l'indipendenza di giudizio o indurre ad assicurare qualsiasi vantaggio per l' Azienda nella sua interezza;

- promettere o riconoscere compensi o prestazioni in favore di fornitori, consulenti o altri *partners* che non trovino ragione in apposite attività richieste, incarichi da svolgere e regolarmente conseguiti secondo specifici rapporti contrattuali stipulati e approvati dall'Amministratore unico della società.

Con riferimento ai preposti aventi potere di spendita del nome della società verso l'esterno a fini negoziali, sono imposti ulteriori obblighi comportamentali, in quanto quest'ultimi sono soggetti che, in ragione delle attività a loro affidate, possono in concreto realizzare i reati di cui alla presente Parte Speciale.

Al fine di scongiurare una circostanza siffatta, oltre ai divieti suindicati, è altresì imposto all'Amministratore unico, anche per il tramite di un amministratore e/o dirigente appositamente incaricato:

- di curare il sistema interno di revisione della documentazione attinente al bilancio di esercizio, alle scritture contabili, alla relazione semestrale, avente ad oggetto informazioni sullo stato economico e patrimoniale della società, verificando che detta documentazione raggiunga gli obiettivi di veridicità e correttezza dei dati;

- di verificare e, conseguentemente, attestare l'adeguatezza del bilancio d'esercizio (di tutta la documentazione riguardante lo stato patrimoniale, contabile e finanziario della società), alle caratteristiche della società e che siano stati rispettati i criteri imposti dalla legge per la formazione di dette scritture, con particolare riferimento ai criteri formali e sostanziali richiesti dalla normativa contabile.

L'Amministratore e/o il dirigente è tenuto, altresì, a riferire periodicamente all'Amministratore unico e all'O.d.V. un aggiornamento periodico dell'attività svolta.

Ove la società provvedesse a conferire incarico ad un revisore contabile e/o Società di revisione legale, l'Amministratore unico deve assicurare:

- che il professionista non si trovi in situazioni di incompatibilità previste dalla legge;

- che venga individuato il personale STONE SECURITY S.R.L. tenuto a trasmettere al revisore la documentazione necessaria per lo svolgimento dell'incarico affidato;

- che il professionista contabile e/o la Società di revisione legale prenda contatti con l'Organismo di Vigilanza e, congiuntamente all'Amministratore unico, venga predisposto e assicurato un sistema di informazione continua tra questi ultimi ed il revisore.

Sotto il profilo generale, è imposto ai destinatari del presente Modello:

- nella partecipazione a gare d'appalto, di non intrattenere rapporti con esponenti dell'Ente committente per ragioni diverse da quelle meramente professionali;
- nell'ambito di risoluzione di controversie con eventuali *partners* contrattuali, anche mediante il ricorso ad accordi transattivi, di impegnarsi a garantire procedure trasparenti e tracciabili;
- di astenersi dal concedere o promettere denaro o altra liberalità che non sia effettuata in buona fede o motivata dalla volontà di influenzare la capacità di giudizio della controparte.

Infine, l'Amministratore unico di STONE SECURITY S.R.L. potrà provvedere ulteriori misure a maggiore tutela delle aree a rischio individuate, ad integrazione degli adempimenti sopra elencati.

E' fatto espresso **obbligo** a carico dei predetti destinatari di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure 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 di STONE SECURITY S.R.L. , segnalando anche eventuali interessi in conflitto;
- tenere comportamenti corretti, nel rispetto delle norme di legge e delle procedure interne, al fine di garantire la tutela del patrimonio degli investitori e dei soci, in particolare nella fase di acquisizione, elaborazione ed illustrazione dei dati e delle informazioni relative ai prodotti finanziari ed ai loro emittenti;
- assicurare il regolare funzionamento della società e dei suoi organi, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge;
- agevolare ogni forma di controllo interno sulla gestione sociale;
- osservare le regole che presiedono alla corretta formazione del prezzo degli strumenti finanziari, evitando di porre in essere comportamenti idonei a provocarne una sensibile e artificiosa alterazione;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non opponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate.

Nell'ambito dei suddetti comportamenti **è fatto divieto di**:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria dell' Azienda;

- omettere la comunicazione di dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società;

- alterare i dati e le informazioni destinati alla predisposizione del prospetto;

- illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria dell'emittente e sull'evoluzione della sua attività, nonché sui prodotti finanziari e relativi diritti;

- inficiare la comprensibilità del prospetto inserendo dati non richiesti, in grado di alterare le effettive esigenze informative dell'investitore;

- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque costituiscano ostacolo allo svolgimento all'attività di controllo o di revisione della gestione sociale;

- determinare o influenzare l'assunzione delle deliberazioni dell'organo di indirizzo, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà consiliare;

- pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento aventi ad oggetto strumenti finanziari quotati o non quotati ed idonei ad alterarne sensibilmente il prezzo;

- pubblicare o divulgare notizie false, anche attraverso comunicati stampa, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento idonei a diffondere sfiducia nel pubblico di banche o gruppi bancari, alterandone l'immagine di stabilità e liquidità;

- omettere di effettuare, con la dovuta tempestività, correttezza e trasparenza, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa di settore nei confronti delle Autorità di Vigilanza cui è soggetta l'attività della società, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette Autorità;

- esporre, nelle predette comunicazioni e trasmissioni, fatti non rispondenti al vero, ovvero occultare fatti rilevanti, in relazione alle condizioni economiche, patrimoniali o finanziarie della società;

- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità Pubbliche di Vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

7. Principi di attuazione dei comportamenti prescritti

Occorre ora indicare i principi e le modalità di attuazione dei comportamenti sopra descritti, in relazione alle diverse tipologie dei reati societari.

7.1. Bilanci ed altre comunicazioni sociali

La redazione del bilancio annuale, della relazione sulla gestione, della relazione semestrale viene elaborata secondo i seguenti principi:

- in ogni unità organizzativa competente, siano adottate misure idonee a garantire che le operazioni sopra indicate, siano effettuate con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza, e siano tempestivamente segnalate eventuali situazioni anomale;

- siano adottate misure idonee a garantire che l'informazione comunicata ai soggetti gerarchicamente sovraordinati da parte dei responsabili dell'unità organizzativa competente sia veritiera, corretta, accurata, tempestiva e documentata, anche con modalità informatiche;

- siano adottate misure idonee ad assicurare che qualora siano formulate richieste, da chiunque provenienti, di variazione quantitativa dei dati, rispetto a quelli già contabilizzati in base alle procedure correnti, chi ne sia a conoscenza informi, senza indugio, l'Organismo di Vigilanza;

- siano adottate misure idonee a garantire che qualora siano formulate ingiustificate richieste di variazione dei criteri di rilevazione, registrazione e rappresentazione contabile, chi ne sia a conoscenza informi, senza indugio, l'Organismo di Vigilanza;

- l'obbligo in capo a chi fornisce informazioni, previste dalla presente procedura, alle unità gerarchicamente sovraordinate di indicare i documenti o le fonti originarie dalle quali sono tratte ed elaborate le informazioni trasmesse, al fine di garantire la verificabilità delle stesse. Qualora possibile, e utile per la comprensione e la verifica dell'informazione, deve essere allegata copia dei documenti eventualmente richiamati.

7.2. Prospetti informativi

La redazione, o partecipazione alla redazione, di prospetti informativi dovrà essere effettuata sulla base di procedure fondate sui seguenti principi:

- verifica, nella misura massima possibile, delle correttezza dei dati o delle informazioni, nonché, ove tale verifica non sia ragionevolmente possibile, acquisizione dell'attestazione di veridicità da parte dei soggetti da cui l'informazione proviene;

- controllo rigoroso sulla professionalità dei soggetti preposti alle suddette operazioni, anche in relazione alla valutazione del contributo proveniente dagli altri soggetti coinvolti nella redazione del prospetto;

- informazione sulle norme in materia di falso in prospetto e sulle discipline tecniche contabili ed economiche rilevanti ai fini della redazione dei prospetti;

- informativa all'Organismo di Vigilanza, da parte del responsabile dell'operazione, di ciascuna iniziativa che comporti la redazione o la partecipazione alla redazione di prospetti informativi, al fine di consentire il controllo sul rispetto delle regole e delle procedure predette e, al termine dell'operazione, dell'avvenuta pubblicazione.

7.3. Regolare funzionamento della società

Al fine di prevenire la commissione del reato di impedito controllo sulla gestione della società da parte degli organi di governo sono stabilite le seguenti regole e procedure interne:

- attribuzione all'Organismo di Vigilanza dei compiti di coordinare la raccolta delle informazioni e documenti richiesti dagli organi di controllo, di valutarne la validità e disporne la consegna o comunicazione;
- diffusione dei principi di comportamento in materia previsti nel presente Modello nel contesto dell'intera organizzazione aziendale, in modo che gli amministratori, il *management* e tutti i dipendenti possano fornire agli organi di controllo la massima collaborazione, trasparenza e correttezza professionale;
- previsione di idoneo sistema sanzionatorio.

7.4. Attività soggette a vigilanza

Con riferimento alle attività della società soggette alla vigilanza di pubbliche autorità in base alla normativa vigente, al fine di prevenire la commissione dei reati di false comunicazioni alle autorità e di ostacolo alle funzioni di vigilanza, le attività soggette a vigilanza dovranno essere svolte in base a tali principi fondamentali:

- effettuazione delle segnalazioni periodiche alle autorità previste da leggi e regolamenti;
- trasmissione dei documenti previsti in leggi e regolamenti (bilanci e verbali delle riunioni degli organi societari);
- trasmissione di dati e documenti specificamente richiesti dalle autorità di vigilanza;
- correttezza, professionalità e trasparenza nella condotta da tenere nel corso degli accertamenti ispettivi, in particolare con la messa a disposizione, con tempestività e completezza, dei documenti che gli incaricati ritengano necessario acquisire;
- qualità e tempestività delle comunicazioni alle autorità di vigilanza;

- attuazione di tutti gli interventi di natura organizzativo - contabile necessari ad estrarre i dati e le informazioni per la corretta compilazione delle segnalazioni e puntuale invio all'autorità di vigilanza, secondo le modalità ed i tempi stabiliti dalla normativa di settore;

- esistenza di un sistema informativo affidabile e controlli interni efficaci, tali da garantire l'attendibilità delle informazioni fornite alle autorità di vigilanza;

- predisposizione di idonei strumenti per la messa a disposizione dell'Organismo di Vigilanza di detta documentazione, per le verifiche periodiche da effettuarsi da parte di quest'ultimo;

- previsione di idoneo sistema sanzionatorio.

PARTE SPECIALE III

REATI DI RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA ED AUTORICICLAGGIO

QUALI FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

(Art. 25-*octies*)

1. I reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio

Con il d. lgs. n. 231 del 21 novembre 2007 - in vigore dal 29 dicembre 2007 - il legislatore ha dato attuazione alla direttiva 2005/60/CE del Parlamento e del Consiglio, del 26 ottobre 2005, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (c.d. III direttiva antiriciclaggio), e alla direttiva 2006/70/CE della Commissione che ne reca misure di esecuzione.

L'intervento normativo comporta un riordino della complessa normativa antiriciclaggio presente nel nostro ordinamento giuridico. In particolare, l'art. 64 prevede l'abrogazione del Capo I del d.l. n. 143/1991 (convertito in l. n. 197/1991), ad eccezione degli artt. 5, commi 14 e 15, 10 e 13, che ha dato attuazione alla I direttiva antiriciclaggio (1991/308/CE), nonché l'integrale abrogazione del d. lgs. n. 56/2004, che ha dato attuazione alla II direttiva antiriciclaggio (2001/97/CE). Per quanto riguarda il coordinamento tra il d. lgs. 231/2007 e i precedenti provvedimenti in materia di antiriciclaggio, si rinvia alle precisazioni contenute nella nota emanata in data 19 dicembre 2007 dal Ministero dell'Economia e delle Finanze, d'intesa con la Banca d'Italia, l'Ufficio Italiano dei Cambi e la Guardia di Finanza.

L'art. 25-*octies* (introdotto dall'art. 63, comma 3 del d.lgs. 231/2007) estende la responsabilità amministrativa degli enti ai reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio - artt. 648, 648-*bis*, 648-*ter* e 648 *ter*.1[7] del C.P.- con la previsione di una sanzione pecuniaria da 200 a 800 quote, che diviene da 400 a 1000 quote nel caso in cui il denaro, i beni o le altre

[7] Il reato di autoriciclaggio di cui all'art. 648 ter.1. c.p. è stato introdotto dall'art. 3, comma 3, l. 15 dicembre 2014, n. 186.

utilità provengano da delitto (cd. "principale") per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni. La nuova disposizione prevede, altresì, nel caso di condanna dell'Ente, l'applicabilità delle sanzioni interdittive di cui all'articolo 9, c. 2, per una durata non superiore a due anni.

L'art. 64, c. 1, lett. f), inoltre, abroga i commi 5 e 6 dell'art. 10 della l. n. 146/2006, di contrasto al crimine organizzato transnazionale che già prevedevano a carico dell'Ente la responsabilità e le sanzioni *ex* 231 per i reati di riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (artt. 648-bis e 648-ter C.P.), se caratterizzati dagli elementi della transnazionalità, secondo la definizione contenuta nell'art. 3 della stessa legge 146/2006.

Ne consegue che ai sensi dell'art. 25-*octies*, d. lgs. n. 231/2001, l'Ente sarà ora punibile per i reati di ricettazione, riciclaggio, impiego di capitali illeciti, nonché per la nuova fattispecie di autoriciclaggio anche se compiuti in ambito prettamente "nazionale", sempre che ne derivi un interesse o vantaggio per l'Ente medesimo.

La finalità del decreto n. 231/2007 consiste nella protezione del sistema finanziario dal suo utilizzo a fini di riciclaggio o di finanziamento del terrorismo. Tale tutela viene attuata con la tecnica della prevenzione per mezzo di apposite misure e obblighi di comportamento per una vasta platea di soggetti - individuati agli artt. 10, c. 2, 11, 12, 13 e 14 del decreto - che comprende, oltre alle banche e agli intermediari finanziari, anche gli altri soggetti a cui erano già stati estesi gli obblighi antiriciclaggio dal d. lgs. n. 56/04: professionisti; revisori contabili; altri soggetti.

Nell'ambito di tale ultima categoria rientrano, in generale, gli operatori che svolgono attività il cui esercizio è subordinato a licenze, autorizzazioni, iscrizioni in albi/registri o dichiarazioni di inizio attività richieste da norme di legge (es. recupero crediti per conto terzi, custodia e trasporto di denaro contante, di titoli o valori con o senza l'impiego di guardie giurate, agenzie di affari in mediazione immobiliare, case da gioco, commercio di oro per finalità industriali o di investimento, fabbricazione, mediazione e commercio di oggetti preziosi, fabbricazione di oggetti preziosi da parte di imprese artigiane, commercio di cose antiche, esercizio di case d'asta o galleria d'arte, ecc.). Nei loro confronti trovano applicazione, sia gli obblighi di cui al citato decreto n. 231/2007, nel rispetto di limiti, modalità e casi specificamente indicati dallo stesso decreto, sia le specifiche disposizioni e istruzioni applicative, in materia di identificazione/registrazione/conservazione delle informazioni/segnalazione delle operazioni sospette, dettate a carico degli operatori c.d. "non finanziari" dal decreto del MEF n. 143 del 3 febbraio 2006 e dal provvedimento UIC del 24 febbraio 2006, cui si rinvia per approfondimenti.

L'inadempimento a siffatti obblighi viene sanzionato dal decreto con la previsione di illeciti amministrativi e di reati penali cd. "reati-ostacolo", tendenti a impedire che la progressione criminosa giunga alla realizzazione delle condotte integranti ricettazione, riciclaggio o impiego di capitali illeciti.

A tal proposito, merita di essere considerato l'art. 52 del decreto che obbliga i diversi organi di controllo di gestione, tra cui l'Organismo di Vigilanza, esistenti negli enti destinatari della disciplina a vigilare sull'osservanza della normativa antiriciclaggio e a comunicare le violazioni delle relative disposizioni di cui vengano a conoscenza nell'esercizio dei propri compiti o di cui abbiano altrimenti notizia. Tali obblighi di comunicazione riguardano in particolar modo le possibili infrazioni relative alle operazioni di registrazione, segnalazione e ai limiti all'uso di strumenti di pagamento e di deposito (contante, titoli al portatore, conti e libretti di risparmio anonimi o con intestazioni fittizie) e sono destinati ad avere effetto sia verso l'interno dell'Ente (titolare dell'attività o legale rappresentante) che verso l'esterno (autorità di vigilanza di settore, Ministero Economia e Finanze, Unità di Informazione Finanziaria presso la Banca d'Italia).

La lettera della norma potrebbe far ritenere sussistente in capo a tutti i suddetti organi una posizione di garanzia *ex* art. 40, c. 2, c.p. finalizzata all'impedimento dei reati in commento.

Una corretta e coerente interpretazione dovrebbe invece tenere in debito conto i differenti poteri/doveri assegnati ai diversi organi di controllo, sia dalla normativa in questione che dalle disposizioni generali dell'ordinamento (*in primis*, il codice civile). Mentre per alcuni dei suddetti organi di controllo sembrerebbe sussistere una tale posizione di garanzia, che ha un ruolo equipollente a quanto rinvenibile in seno al Collegio sindacale nelle società di capitali - sulla base delle disposizioni civilistiche (cfr. art. 2403 C.C.), con specifico riferimento all'Organismo di Vigilanza una simile responsabilità appare del tutto incompatibile con la natura dei poteri/doveri ad esso originariamente attribuiti dalla legge.

Pertanto, dovrebbe prevalere un'interpretazione sistematica della norma che limiti il dovere di vigilanza di cui al c. 1 dell'art. 52 e le relative responsabilità all'adempimento degli obblighi informativi previsti dal c. 2 della medesima disposizione.

In altri termini, l'adempimento dei doveri di informazione a fini di antiriciclaggio deve essere commisurato ai concreti poteri di vigilanza spettanti a ciascuno degli organi di controllo contemplati dal comma 1 dell'art. 52, nell'ambito dell'Ente di appartenenza che sia destinatario della normativa.

Ne deriva, che il dovere di informativa dell'Organismo di Vigilanza non può che essere parametrato alla funzione, prevista dall'art. 6, c. 1, lett. b) del decreto 231, di vigilare sul funzionamento e

sull'osservanza dei modelli e, con specifico riferimento all'antiriciclaggio, di comunicare quelle violazioni di cui venga a conoscenza nell'esercizio delle proprie funzioni o nelle ipotesi in cui ne abbia comunque notizia (es. su segnalazione di dipendenti o altri organi dell'Ente). Tale ultima previsione risulta, d'altra parte, coerente con gli obblighi di informazione stabiliti dalla legge nei confronti dell'Organismo medesimo allo scopo di migliorare l'attività di pianificazione dei controlli e di vigilanza sul Modello da parte di quest'ultimo (art. 6, c. 2, lett. d).

Tale chiave di lettura, senza riconoscere una posizione di garanzia, in assenza di effettivi poteri impeditivi dell'Organismo di Vigilanza rispetto alle fattispecie di reato in esame, viene completata dalla sanzione penale della reclusione fino a 1 anno e della multa da 100 a 1000 euro in caso di mancato adempimento dei suddetti obblighi informativi (art. 55, c. 5).

Vale la pena sottolineare che quello in esame è l'unico caso in cui il legislatore abbia espressamente disciplinato una specifica fattispecie di reato a carico dell'O.d.V. (reato omissivo proprio), peraltro a seguito del riconoscimento di una atipica attività a rilevanza esterna dello stesso.

La responsabilità amministrativa dell'Ente per i reati previsti dagli art. 648, 648-*bis* e 648-*ter*, c.p. è limitata alle ipotesi in cui il reato sia commesso nell'interesse o a vantaggio dell'Ente medesimo.

Considerato che le fattispecie delittuose in questione possono essere realizzate da chiunque (c.d. reati comuni), si dovrebbe ritenere che la ricorrenza del requisito oggettivo dell'interesse o vantaggio vada escluso ogni qual volta non vi sia attinenza tra la condotta incriminata e l'attività esercitata dall'Ente.

Tale attinenza, ad esempio, potrebbe ravvisarsi nell'ipotesi di acquisto di beni produttivi provenienti da un delitto di furto, ovvero nel caso di utilizzazione di capitali illeciti per l'aggiudicazione di un appalto, ecc. Viceversa, non è ravvisabile l'interesse o il vantaggio per l'Ente nell'ipotesi in cui l'apicale o il dipendente acquistino beni che non abbiano alcun legame con l'esercizio dell'impresa in cui operano. Lo stesso può dirsi per l'impiego di capitali in attività economiche o finanziarie che esorbitano rispetto all'oggetto sociale.

Peraltro, anche nel caso in cui l'oggetto materiale della condotta di ricettazione o di riciclaggio, ovvero l'attività economica o finanziaria nel caso del reato ex art. 648-*ter* c.p, siano pertinenti rispetto alla specifica attività d'impresa, occorre pur sempre un accertamento in concreto da parte del giudice, da condurre caso per caso, circa la sussistenza dell'interesse o del vantaggio per l'Ente.

La responsabilità diretta dell'Ente è collegata alla commissione dei reati elencati dall'art. 10 Legge 146/2006, richiamato nell'art. 25-*octies* del d.lgs. 231/2001 quando tali reati abbiano altresì la natura di reati transnazionali.

Prima di esaminare i reati di cui all'art. 10 (che vanno dall'associazione per delinquere al riciclaggio, dai reati concernenti il traffico di migranti a quelli di intralcio della giustizia), è preliminare individuare la nozione di **reato transnazionale**, poiché soltanto se caratterizzati in tale peculiare modo, i reati in discorso possono costituire il presupposto per la responsabilità diretta dell'Ente.

La nozione di reato transnazionale (mai presente prima della Legge 146/06 nel nostro ordinamento) è dettata in via tassativa dall'art. 3 Legge cit. secondo cui: "*ai fini della presente legge si considera reato transnazionale il reato* punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

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

Necessario per un quadro non approssimato della definizione di reato transnazionale anche il disposto dell'art. 4 Legge 146/2006, che contempla una circostanza aggravante "*per i reati puniti con la pena della reclusione non inferiore nel massimo a quattro anni nella commissione dei quali abbia dato il suo contributo un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato*".

La nozione di reato transnazionale dipende, dunque, dal concorrere di tre requisiti dettati dal primo comma dell'art. 3: due di essi (indicati nella prima parte del primo comma) attengono rispettivamente alla gravità del reato (reclusione 1 – edittale – non inferiore nel massimo a quattro anni) e a una componente soggettiva ("qualora sia coinvolto un gruppo criminale organizzato"); il terzo requisito (definito in dottrina "transnazionalità in senso stretto") è integrato, alternativamente, da uno dei caratteri definiti nelle lettere da a) a d) del medesimo primo comma.

L'impiego dei termini "coinvolto" e "implicato" nel primo comma dell'art. 3, soprattutto se lo si compara con l'uso della formula "nella commissione dei quali [reati] abbia dato il suo contributo un gruppo

criminale organizzato impegnato in attività criminali in più di uno Stato", suggerisce, di fronte allo scadente tecnicismo della redazione delle norme, un'interpretazione nella quale il valore da attribuire al termine definitorio "coinvolto" (così come a "implicato") allude a una situazione che non realizza la fattispecie di concorso di persone nel reato e neppure quella di favoreggiamento reale o personale, bensì a un contesto nel quale il vantaggio, il profitto, l'utilità, l'interesse del fatto di reato si riverberano a favore del gruppo criminale organizzato. Siffatta lettura permette, infatti, di mantenere distinto il criterio adottato con riguardo all'aggravante, dove il "contributo alla commissione" del reato sembra designare una situazione nella quale uno dei partecipi al gruppo criminale organizzato ha posto in essere almeno una frazione della condotta tipica del reato medesimo.

Combinando questi parametri con quelli indicati dall'art. 10 Legge 146/2006 (disposizione che, come detto, stabilisce la responsabilità diretta dell'Ente), si deve ritenere che la responsabilità diretta dell'Ente (nel caso di specie di STONE SECURITY S.R.L.) trova il suo presupposto nella circostanza che un soggetto dell'Ente abbia commesso uno dei reati indicati dall'art. 10 quando tale reato abbia il carattere della transnazionalità come definita dall'art. 3 Legge cit.: in altri e più specifici termini che il reato di riciclaggio abbia un riverbero a favore del gruppo organizzato criminale e che il reato sia stato commesso in uno dei contesti alternativi indicati nelle lettere da a) a d) dell'art. 3 c..1 Legge 146/2006, ferma restando la necessaria consapevolezza (anche nella forma della eventualità) da parte dell'esponente dell'Ente del carattere transnazionale del fatto.

1.1. Ricettazione (art. 648 c.p.)

Fuori dalle ipotesi di concorso di persone nel reato, è punito "*chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare*".

È comminata un pena ridotta ove il fatto sia di particolare tenuità, nonché la norma specifica che quanto stabilito dal predetto articolo trova applicazione anche nelle ipotesi in cui "*l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile, ovvero quando manchi una condizione di procedibilità*".

Oltre alle condotte materiali tipizzate e descritte consistenti nell'acquisto, la ricezione o l'occultamento dei beni di provenienza delittuosa, la norma persegue anche la mera mediazione dell'agente indipendentemente dal raggiungimento dello scopo.

È richiesto in capo al soggetto attivo lo specifico scopo di trarre, dalla consumazione del reato, una qualsivoglia forma di profitto, tendenzialmente di natura economica, per sé o per terzi.

Oggetto del materiale della ricettazione può essere il denaro o ogni altra cosa, mobile o immobile.

1.2. Riciclaggio (art. 648 bis c.p.)

Il delitto sanziona, fuori dalle ipotesi di concorso di persone nel reato, "*chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa*".

La pena è aggravata se il fatto è commesso durante l'esercizio di una attività professionale, mentre è diminuita se il reato presupposto prevede la pena della reclusione inferiore nel massimo a cinque anni.

Trova, altresì, applicazione il medesimo precetto stabilito per il delitto di ricettazione, ovvero la punibilità per riciclaggio non è esclusa se "*l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità*".

Tutte le condotte tipizzate hanno un requisito comune perché devono essere realizzate in modo da ostacolare l'identificazione della provenienza delittuosa del loro oggetto; la prova dell'idoneità delle condotte a raggiungere lo scopo, trattandosi di un reato di mera condotta e non di evento, è sufficiente per integrare il delitto in esame senza dovere accertare l'effettiva dissimulazione.

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

Fuori dalle ipotesi di concorso di persone nel reato e dei casi previsti dagli articoli 648 e 648-*bis* c.p., è punito "*chiunque impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto".*

La pena prevista per detto reato è aumentata o diminuita nelle medesime ipotesi di cui all'art. 648-*bis* c.p., nonché si applica il disposto di cui all'art. 648, ultimo comma, c.p. ovvero la punibilità per il reato di impiego di denaro, beni o altra utilità di illecita provenienza anche qualora "*l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità".*

Con riferimento al reato di riciclaggio, sussiste tra le due fattispecie un rapporto di specialità, in ragione del quale non solo il delitto ex art. 648-*ter* si applica in via sussidiaria rispetto a quello di riciclaggio, ma soprattutto si differenzia in relazione alla volontà dell'agente di perseguire lo scopo di occultare la provenienza delittuosa tramite il reimpiego dei proventi illeciti in una lecita attività.

Questa figura di reato costituisce l'ultima fase di un "ciclo criminoso" e consiste nell'impiego dei proventi di origine delittuosi esclusivamente in attività (e, quindi, non in singoli affari) economiche o finanziarie (ovvero per la produzione e la circolazione di beni o servizi o la circolazione di denaro o di valori mobiliari purché non sia prevalente l'aspetto intellettuale).

1.4. Autoriciclaggio (art. 648-ter1 c.p.)

L'art. 648-*ter*1, introdotto dall'art. 3, comma 3, della L. 15 dicembre 2014, n. 186, recita: "*si applica la pena della reclusione da due a otto anni e della multa da 5.000 a 25.000 euro a chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa".*

La condotta di "*impiego*" consiste nella re-immissione del provento delittuoso nel circuito economico, mentre il "*trasferimento*" e la "*sostituzione*" alludono a comportamenti che causino un mutamento della titolarità del bene o che ne determinino un utilizzo non più personale.

L'oggetto materiale è costituito dal denaro, beni o altre utilità provenienti da delitto non colposo.

Al quarto comma viene prevista una causa di non punibilità allorché l'agente destini il denaro, i beni o le altre utilità provenienti dal reato presupposto "*alla mera utilizzazione o al godimento personale*".

La norma, inoltre, prevede una diversificazione del trattamento sanzionatorio in relazione alla gravità del fatto. In particolare:

- ai sensi del secondo comma, si applica la pena della reclusione da uno a quattro anni e della multa da 2.500 a 12.500 euro se il denaro, i beni e le altre utilità provengono dalla commissione di un delitto non colposo punito con la pena della reclusione inferiore nel massimo a cinque anni;

- ai sensi del terzo comma, si applica in ogni caso, e dunque anche nell'ipotesi da ultimo citata, la pena della reclusione da due a cinque anni e della multa da euro 5.000 a euro 25.000 se il denaro, i beni e le altre utilità provengono da un delitto commesso avvalendosi delle condizioni previste dall'art. 416-*bis* c.p., o con la finalità di agevolare l'attività delle associazioni previste dal medesimo art. 416-*bis* c.p.;

- ai sensi del quinto comma, la pena è aumentata se i fatti sono commessi nell'esercizio di attività bancaria, finanziaria o altra attività professionale;

- ai sensi del sesto comma, la pena è diminuita fino alla metà se il colpevole si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni provenienti da reato;

Anche per il reato in questione, come già per il riciclaggio e il reimpiego, si applica il disposto di cui all'art. 648, ultimo comma, c.p.: la condotta è punibile anche qualora "*l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità*".

1.5. Trattamento sanzionatorio per le fattispecie di cui all'art. 25 octies del Decreto

Con riferimento ai delitti sopra analizzati, ove venisse accertata la responsabilità dell'Ente, sono comminate in suo confronto le seguenti sanzioni:

- in relazione ai reati di cui agli articoli 648, 648-*bis* e 648-*ter* e 648 *ter 1* del codice penale, si applica all'Ente la sanzione pecuniaria da 200 a 800 quote;
- nel caso in cui il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni si applica la sanzione pecuniaria da 400 a 1000 quote;

- nei casi di condanna per uno dei delitti in esame si applicano all'Ente le sanzioni interdittive previste dall'articolo 9,comma 2 del Decreto per una durata non superiore a due anni.

2. Aree a rischio

In relazione ai reati oggetto della presente Parte Speciale ed alle attività svolte da STONE SECURITY S.R.L. sono stati individuati i seguenti processi sensibili:

- **Autorizzazione disposizioni di pagamento**
- **Gestioni acquisti**

Si riporta una esemplificazione delle possibili modalità di commissione dei reati in esame all'interno della società:

- Il reato di Riciclaggio (art. 648-*bis* c.p.) potrebbe realizzarsi, ove fosse sostituito o trasferito denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compiute in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

- Il reato di Impiego di denaro, beni o altre utilità di provenienza illecita (art. 648-*ter* c.p.) si perfeziona con l'impiego in attività economiche o finanziarie denaro, beni o altre utilità di provenienza delittuosa.

- Il reato di Autoriciclaggio (art. 648-*ter*.1 c.p.) potrebbe verificarsi nell'ipotesi in cui, a seguito della commissione di delitti non colposi (anche estranei a quelli inclusi nel d.lgs. 231/2001), ad esempio i reati tributari in materia dichiarativa o la truffa, il profitto conseguito sia impiegato in modo tale da occultarne la provenienza illecita.

- Il reato di Ricettazione (art. 648 c.p.) potrebbe configurarsi laddove un dipendente dell'Ente, al fine di procurare per lo stesso Ente un profitto, acquistasse, ricevesse od occultasse denaro o cose provenienti da un qualunque delitto ovvero si intromettesse a tal fine.

Da quanto appena descritto appare evidente che il rischio di commissione di reati contro la Pubblica Amministrazione è strettamente correlato alle seguenti **aree di attività**:

- **gestione incassi;**
- **gestione acquisti;**
- **rimborso note spese/trasferte.**

Sebbene quelle precedentemente individuate siano le aree di attività maggiormente esposte a rischio commissione dei reati indicati nella presente Parte Speciale, a titolo esemplificativo ma non esaustivo, si indicano possibili modalità di commissione del reato nella realtà della società che possono riguardare potenzialmente **tutte le aree di attività** all'interno di STONE SECURITY S.R.L. :

- sostituzione, trasferimento o impiego in attività economiche o finanziarie o imprenditoriali o speculative di denaro, beni o altre utilità provenienti da un delitto non colposo in modo da ostacolare concretamente l'identificazione della provenienza delittuosa (art. 648-*ter1*. c.p.);

- trasferimento su conto *off shore* di somme derivanti da violazioni delle norme tributarie penalmente rilevanti, come false fatturazioni, frodi fiscali, omesso versamento IVA ecc.;

- acquisto tramite soggetti fiduciari di strumenti finanziari;

- trasferimento delle provviste su conti correnti intestati ad altri soggetti con causale non veritiera;

- sostituzione, trasferimento o impiego, con modalità tali da ostacolare concretamente l'identificazione della provenienza delittuosa della provvista, del profitto illecito derivante da delitti non colposi, come ad esempio il delitto di attività organizzate per il traffico illecito di rifiuti o quello di combustione illecita di rifiuti;

- Impiegare in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, ad esempio gestendo impianti i cui *iter* di sviluppo e/o autorizzativi siano stati realizzati anche commettendo delitti, o utilizzando beni (quali materiali da costruzione, ecc.) di origine delittuosa.

In relazione ai reati sopra esplicitati, le aree ritenute più specificatamente a rischio risultano essere , dunque, ai fini della presente Parte Speciale, le operazioni finanziarie o commerciali poste in essere con: persone fisiche e giuridiche residenti nei Paesi a rischio individuati nelle c.d. "Liste Paesi" e/o con persone fisiche o giuridiche collegate reati di criminalità organizzata transnazionale, ricettazione, riciclaggio, impiego di denaro beni o utilità di provenienza illecita riportati nelle c.d. "Liste Nominative", entrambe rinvenibili nel sito internet dell'UIF o pubblicate da altri organismi nazionali e/o internazionali riconosciuti; o società

controllate direttamente o indirettamente dai soggetti sopraindicati o da soggetti a rischio reati di cui alla presente Parte Speciale.

Si richiamano, in particolar modo, le operazioni svolte nell'ambito di attività di approvvigionamento o attività di *merger & acquisition* internazionale, che possono originare flussi finanziari diretti verso Paesi esteri.

2.1. Alcune osservazioni in tema di autoriciclaggio

L'introduzione nel nostro ordinamento del reato di autoriciclaggio tra i reati presupposto sanzionati ai sensi del d. lgs. n. 231/2001 estende le aree di responsabilità amministrativa per gli Enti.

La struttura della norma è tale che ingenerare dubbi interpretativi che si riflettono sulla portata degli adempimenti da realizzare per garantire l'adeguatezza del Modello rispetto al reato in questione.

Il problema si pone con riferimento alla necessità (o meno) di considerare, tra i reati idonei a configurare la responsabilità dell'Ente *ex* Decreto 231, non solo l'autoriciclaggio, quale figura criminosa determinata ed esclusiva, ma anche i reati presupposto dell'autoriciclaggio, ovvero quei reati - il cui ambito è evidentemente indeterminato - dalla cui commissione provengono i beni oggetto delle condotte di autoriciclaggio.

L'intento del legislatore, fin dall'adozione originaria del d. lgs. n. 231/2001, è stato quello di configurare la responsabilità amministrativa dell'Ente derivante da reati con riferimento ad un catalogo determinato di fattispecie criminose, incrementato di volta in volta attraverso i successivi interventi legislativi. Ciò in ossequio al principio di tassatività.

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

Sul punto (come rilevato nella Parte Speciale del presente Modello relativa ai reati associativi) è intervenuta la Corte di Cassazione circoscrivendo l'operatività dell'art. 24-*ter* nel senso di negare la possibilità di attrarre indirettamente alla responsabilità *ex* 231 i delitti-scopo del reato associativo; a ragionare diversamente, infatti, "*la norma incriminatrice di cui all'art. 416 c.p. si trasformerebbe, in violazione del principio di tassatività del sistema sanzionatorio contemplato dal D.Lgs. n. 231 del 2001, in una disposizione 'aperta', dal contenuto elastico, potenzialmente idoneo a ricomprendere nel novero dei reati-presupposto qualsiasi fattispecie di reato, con il pericolo di un'ingiustificata dilatazione dell'area di potenziale responsabilità dell'ente collettivo, i cui organi direttivi, peraltro,*

verrebbero in tal modo costretti ad adottare su basi di assoluta incertezza e nella totale assenza di oggettivi criteri di riferimento, i modelli di organizzazione e di gestione previsti dal citato d.lgs., art. 6, scomparendone, di fatto, ogni efficacia in relazione agli auspicati fini di prevenzione" (Cass. pen., Sez. VI, 20 dicembre 2013, n. 3635).

Pertanto, se pure, in ossequio al principio di tassatività non può pretendersi che la società sia costretta ad adottare nel Modello contromisure idonee ad impedire od ostacolare la commissione di un numero indiscriminato di reati, nondimeno, nell'ottica - che ispira la disciplina introdotta dal Decreto 231 - di prevenzione delle condotte criminali che trovano occasione di realizzarsi nell'ambito di attività delle persone giuridiche, si ritiene che la funzione del Modello di organizzazione e di gestione possa utilmente essere rivolta anche alla prevenzione di taluni reati presupposto dell'autoriciclaggio.

L'introduzione dei reati di riciclaggio nel catalogo dei reati 231 è sintomatica della volontà del legislatore di neutralizzare gli sviluppi economici del reato presupposto compiuto a monte dal reo evitando che le condotte di riciclaggio o reimpiego dei beni derivanti da reato possano essere svolte per mezzo o attraverso la copertura di una persona giuridica.

Con l'inserimento nel decreto della nuova fattispecie di autoriciclaggio si è inteso rivolgere l'attenzione ai fenomeni criminosi nei quali i reati presupposto delle condotte di riciclaggio o reimpiego siano, per così dire, "endogeni" allo stesso Ente, ovvero compiuti - nell'interesse o a vantaggio dell'Ente - da quelle stesse persone fisiche che si renderanno responsabili – sempre, naturalmente, nell'interesse o a vantaggio dell'Ente - delle condotte di autoriciclaggio incriminate dall'art. 648-*ter*1.

Compiendo un'analisi dell'attività della società e delle possibili criticità emergenti nella descritta ottica di individuazione e perimetrazione delle ulteriori aree di rischio derivanti dall'introduzione del delitto di autoriciclaggio, l'attenzione deve essere rivolta primariamente ai reati tributari, fattispecie criminose che il legislatore non ha ritenuto, fino ad oggi, di includere tra i reati fonte di responsabilità dell'Ente *ex* Decreto 231 e che tuttavia presentano i più concreti rischi di verificazione.

Di seguito è stata riportata la **matrice dei rischi** nella quale è espressa la correlazione tra la probabilità di verificazione del reato presupposto e l'impatto che lo stesso avrebbe per STONE SECURITY S.R.L. (a tal proposito si rinvia alla nota metodologica, relativa alla mappatura dei processi e delle attività sensibili e dei rischi ad essi relativi, di cui al paragrafo 10 della Parte generale del presente Modello.

Cod.	**Reati di ricettazione, riciclaggio,**	**Amministr.**	**Direttore**	**Personale**

	impiego di denaro, beni o utilità di provenienza illecita ed auto riciclaggio	**unico**	**Amm.vo**	**tecnico amm.vo preposto alla funzione**
3	Fattispecie selezionate in premessa	Prob. 1 Imp. 3 Rischio: 3	Prob. 1 Imp. 3 Rischio: 3	

SISTEMI DI PREVENZIONE:

3. Destinatari

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli operatori nelle aree di attività a rischio, nonché da Collaboratori Esterni e *Partners*, come già definiti nella Parte Generale.

Per poter rendere efficace tale Sezione, occorre che tutti i Destinatari sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che, quindi, adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

4. Protocolli preventivi

L'Ente, al fine di prevenire e mitigare il rischio di commissione dei reati in esame, prescrive una serie di adempimenti, coerenti con la normativa antiriciclaggio, posti a carico del personale, collaboratori, organi sociali e terze parti coinvolti nei processi ritenuti sensibili; nello specifico:

- obbligo di rispettare i limiti prescritti dalla normativa in materia di antiriciclaggio per i pagamenti/incassi in contanti;
- divieto di trasferimento, anche frazionato, di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) in euro o in valuta estera, effettuato a qualsiasi titolo tra soggetti diversi quando il valore dell'operazione è pari o superiore a Euro 1.000. Il trasferimento può tuttavia essere eseguito per il tramite di banche, istituti di moneta elettronica e Poste Italiane S.p.A.
- obbligo di effettuare tempestive comunicazioni delle possibili violazioni degli obblighi in tema di antiriciclaggio agli Organi interni alla società e all'O.d.V.;
- monitoraggio dei flussi finanziari in entrata ed in uscita, con particolare attenzione alla regolarità degli incassi e dei pagamenti e dalla corrispondenza tra destinatari/ordinanti dei pagamenti e controparti contrattuali coinvolte nella transazione;
- formazione ed informazione, in materia di riciclaggio, del personale coinvolto nei processi sensibili al fine di garantire la conoscenza della normativa vigente e le modalità operative interne di applicazione degli obblighi di legge e di gestione delle operazioni sospette;
- divieto di intrattenere rapporti commerciali e contrattuali con soggetti di cui si conosca o si sospetti l'appartenenza ad organizzazioni criminali o svolgano attività illecite (ricettazione, riciclaggio, terrorismo, ecc.) o che comunque presentino comportamenti non trasparenti e non improntati al rispetto delle norme di legge;
- la selezione dei soggetti con cui intrattenere rapporti commerciali e contrattuali, quali fornitori, consulenti, partner, avviene secondo una comparazione obiettiva e trasparente delle offerte basata su criteri oggettivi documentabili;
- nei contratti stipulati con i fornitori, consulenti e partner viene inserita una specifica clausola con la quale dichiarano di essere a conoscenza dei principi etici e comportamentali osservati dall'Ente e dei principi contenuti nel presente Modello e si impegnano al loro rispetto. In caso di mancato rispetto di detti principi viene prevista l'applicazione di una penale o, a seconda della gravità, la risoluzione del contratto.

5. Principi generali di comportamento

Obiettivo della presente Parte Speciale è che tali soggetti si attengano, nella misura in cui gli stessi siano coinvolti nello svolgimento delle attività rientranti nelle c.d. Aree a Rischio e in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti della società, a regole di condotta conformi a quanto prescritto nella medesima Parte Speciale, al fine di prevenire ed impedire il verificarsi dei reati di criminalità organizzata, transnazionale, ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita.

Ai Collaboratori esterni e ai *Partners* deve essere resa nota l'adozione del Modello, del Codice Etico da parte di STONE SECURITY S.R.L. .

La presente Parte Speciale dispone a carico degli Esponenti di STONE SECURITY S.R.L. , dei Collaboratori esterni e dei *Partners* e parti terze tutte, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti della società nell'ambito dell'espletamento delle attività considerate a rischio, di attenersi ai seguenti principi generali di condotta.

Ai soggetti coinvolti nelle Aree considerate a rischio STONE SECURITY S.R.L. fa **obbligo** di:

- non compiere atti tali da integrare le fattispecie di reato esaminate nella presente Parte Speciale e sanzionate dall'art. 25-*octies* del Decreto Legislativo o che, pur non rientrando nelle ipotesi criminose sopra delineate, possa in astratto diventarlo;
- improntare il proprio comportamento a principi di correttezza e trasparenza nel rispetto della normativa vigente in materia di antiriciclaggio;
- rispettare i principi generali di comportamento previsti dal Codice Etico e le disposizioni interne previste dal presente Modello, dalle procedure o comunicate tramite apposite circolari che disciplinano le attività di incasso e pagamento;
- privilegiare modalità di incasso e di pagamento che consentano la tracciabilità delle singole operazioni e, ove ciò non sia possibile, registrare tempestivamente le operazioni effettuate e garantirne la documentabilità.

E' fatto espresso **divieto** a carico dei predetti Destinatari di:

1. porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare i reati di criminalità organizzata transnazionale, ricettazione, riciclaggio, impiego di denaro beni o utilità di provenienza illecita ed autoriciclaggio;

2. 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;

3. utilizzare anche occasionalmente la società o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei reati di cui alla presente Parte Speciale;

4. utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;

5 intrattenere rapporti commerciali con fornitori, consulenti e partner che compiono o si sospetti che possano compiere attività contrarie alle normative vigenti;

6 effettuare elargizioni in denaro a individui, società od organizzazioni anche solo sospettate di svolgere attività illecite, in particolare attività terroristiche o sovversive dell'ordine pubblico.

Con particolare riferimento al reato di autoriciclaggio, nella prospettiva di rendere il Modello il più possibile adeguato ad assolvere la propria funzione di prevenzione, si ritiene che i principi di comportamento sopra indicati con riferimento ai rischi di verificazione dei reati di riciclaggio (principi di comportamento senz'altro idonei a dispiegare efficacia anche nei confronti dei rischi di verificazione del reato di autoriciclaggio) debbano essere integrati con ulteriori presidi organizzativi e gestori, indirizzati alla prevenzione del rischio di commissione dei reati tributari commessi da esponenti nell'interesse o a vantaggio della società. Ciò, dunque, con la finalità indiretta di evitare il rischio che il denaro, i beni o le altre attività derivanti dalla commissione di reati tributari compiuti da esponenti (apicali o sottoposti all'altrui vigilanza) possa dar luogo alla realizzazione delle condotte di riciclaggio o reimpiego da parte degli stessi soggetti che hanno commesso o concorso a commettere i reati presupposti.

Con riferimento ai reati tributari in materia di dichiarazioni (d. lgs. n. 74/2000, titolo II, capo I) occorrerà fare riferimento ai principi di comportamento previsti nella Parte Speciale del Modello dedicata ai reati societari di cui all'art. 25-*ter* del Decreto, con particolare riferimento alle norme di condotta riguardanti la redazione delle scritture contabili, dei bilanci e delle altre comunicazioni sociali. E' evidente, infatti, la stretta interdipendenza esistente tra la corretta rappresentazione contabile dei fatti di gestione e la veridicità e fedeltà delle dichiarazioni fiscali.

Le stesse norme comportamentali elencate nella Parte Speciale relativa ai reati societari potranno risultare efficaci in funzione preventiva anche con riferimento al rischio di verificazione dei reati attinenti

l'emissione e la tenuta della documentazione fiscale (artt. 8, 9 e 10 d. lgs. n. 74/2000). Tali presidi possono utilmente essere integrati, con specifico riferimento al reato di emissione e di utilizzazione di fatture o altri documenti per operazioni inesistenti, con le norme di comportamento previste nella Parte Speciale del Modello per i reati di corruzione di cui all'art. 25 del Decreto. Ciò con riferimento al rischio che le condotte corruttive ivi descritte possano estrinsecarsi attraverso il ricorso a false fatturazioni.

Con riferimento ai reati di omesso pagamento di imposte (artt. 10-*bis*, 10-*ter*, 10-*quater* e 11 d. lgs. n. 74/2000) i principi di comportamento da osservare saranno da individuare tra quelli, contenuti nella Parte Speciale relativa ai reati societari, posti a presidio del rispetto delle scadenze contabili e dei rapporti con gli istituti di credito.

6. Principi di attuazione dei comportamenti prescritti

Si indicano qui di seguito i principi procedurali che in relazione ad ogni singola Area a Rischio gli Esponenti sono tenuti a rispettare e che, ove opportuno, potranno essere implementati in specifiche procedure interne alla società ovvero oggetto di comunicazione da parte dell'Organismo di Vigilanza:

1. verifica dell'attendibilità commerciale e professionale dei Fornitori, Collaboratori esterni e *Partner* commerciali/finanziari, sulla base di alcuni indici rilevanti (es. dati pregiudizievoli pubblici – protesti, procedure concorsuali – o acquisizione di informazioni commerciali sui soci e sugli amministratori tramite società specializzate; entità del prezzo sproporzionata rispetto ai valori medi di mercato; coinvolgimento di "persone politicamente esposte", come definite all'art. 1 dell'Allegato tecnico del d. lgs. 21 novembre 2007, n. 231, di attuazione della direttiva 2005/60/CE);

2. verifica che Fornitori, Clienti e *Partner* non abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi dal Gruppo di Azione Finanziaria contro il riciclaggio di denaro (GAFI);

3. effettuazione di specifici e periodici controlli nei rapporti instaurati con soggetti esterni alla società (Fornitori, Clienti o *Partner*) allorché la sede legale della società controparte sia stabilita in paesi considerati come non cooperativi dal Gruppo di Azione Finanziaria contro il riciclaggio di denaro (GAFI), nonché in presenza di eventuali schermi societari e strutture fiduciarie utilizzate per eventuali operazioni straordinarie;

4. verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;

5. controlli formali e sostanziali dei flussi finanziari dell'ente, con riferimento ai pagamenti verso terzi. Tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;

6. verifiche sulla Tesoreria (rispetto delle soglie per i pagamenti per contanti, eventuale utilizzo di libretti al portatore o anonimi per la gestione della liquidità, ecc.);

7. previsione di regole disciplinari in materia di prevenzione dei fenomeni di riciclaggio;

8. verifica dei criteri di selezione, stipulazione ed esecuzione di accordi/*joint-venture* con altre imprese per la realizzazione di investimenti. Trasparenza e tracciabilità degli accordi/*joint-venture* con altre imprese per la realizzazione di investimenti;

9. verifica della congruità economica di eventuali investimenti effettuati in *joint venture* (rispetto dei prezzi medi di mercato, utilizzo di professionisti di fiducia per le operazioni di *due diligence*);

10. eventuale adozione di adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.

7. Controlli dell'Organismo di Vigilanza

In riferimento ai reati in esame, l'O.d.V. ha il compito di monitorare il rispetto degli obblighi e dei divieti impartiti al personale interno coinvolto nei processi sensibili effettuando verifiche periodiche sui movimenti finanziari della società e sulla corretta e ordinata tenuta dei documenti attestanti le operazioni svolte.

L'O.d.V. condurrà controlli a campione diretti a verificare da un lato la corretta applicazione delle regole di cui al presente Modello e, in particolare, delle procedure/istruzioni interne ad hoc emanate, dall'altro l'effettiva adeguatezza delle prescrizioni in essi contenute a prevenire i reati potenzialmente commissibili, proponendo o collaborando, qualora necessario, alla predisposizione delle procedure di

controllo relative ai comportamenti da seguire nell'ambito delle Aree a Rischio individuate nella presente sezione della Parte Speciale. In particolare, l'Organismo di Vigilanza potrà effettuare controlli a campione sulle fatture passive, selezionate anche con riferimento agli importi più rilevanti e alle operazioni con parti correlate, verificandone la corrispondenza a prestazioni realmente eseguite, la riferibilità a un regolare contratto, la congruità nonché l'effettiva esistenza del corrispondente flusso finanziario.

L'Organismo di Vigilanza dovrà esaminare, inoltre, le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari ed opportuni, conservando i flussi informativi ricevuti e le evidenze dei controlli eseguiti.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione rilevante.

PARTE SPECIALE IV

REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

QUALI FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

(Art. 24-*bis*)

La legge 18 marzo 2008, n. 48 "*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 intero*" ha ampliato le fattispecie di reato che possono generare la responsabilità degli enti.

L'art. 7 del predetto provvedimento ha introdotto nel Decreto l'art. 24 - bis "*Delitti informatici e trattamento illecito di dati*", che riconduce la responsabilità amministrativa degli enti ai reati di seguito individuati.

Art. 491* - bis *c.p. Falsità in documenti informatici

"*Se alcune delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, avente efficacia probatoria, si applicano le disposizioni del Capo stesso concernenti rispettivamente gli atti pubblici e le scritture private*".

La norma conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici. I reati di falso richiamati sono i seguenti:

Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.): "Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni"; Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.): "Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni"; Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.): "Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della

reclusione da uno a tre anni"; Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.): "Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476"; Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.): "Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni"; Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.): "Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro"; Falsità materiale commessa da privato (art. 482 c.p.): "Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo"; Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.): "Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi"; Falsità in registri e notificazioni (art. 484 c.p.): "Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00"; Falsità in scrittura privata (art. 485 c.p.): "Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia u0so o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata"; Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.): "Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la

reclusione da sei mesi a tre anni. Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito"; Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.): "Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480"; Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.): "Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private"; Uso di atto falso (art. 489 c.p.): "Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo. Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno"; Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.): "Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente"; Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.): "Agli effetti delle disposizioni precedenti, nella denominazione di "atti pubblici" e di "scritture private" sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti"; Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p.): "Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro Ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni".

1. Delitti informatici e illecito trattamento dei dati

Per quanto concerne la presente Parte Speciale, si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati nell'art. 24-*bis* del Decreto, articolo introdotto dall'art. 7 della legge 18 marzo 2008, n. 48.

Si tratta di reati in parte connotati dall'uso illegittimo degli strumenti informatici e finalizzati all'accesso abusivo in un sistema informatico, alla modifica o al danneggiamento dei dati ivi contenuti, ovvero al danneggiamento del medesimo. Per altro verso, gli illeciti riguardano condotte di intercettazione,

sempre illegittima, di comunicazioni informatiche o telematiche. Infine, è stata introdotta anche la fattispecie di frode informatica del soggetto certificatore della firma elettronica.

E' importante, altresì, segnalare che la medesima legge parifica, ai fini penali, il documento informatico[8] pubblico all'atto pubblico scritto e quello privato alla scrittura privata cartacea.

1.1. Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)

Chiunque 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 il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque 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 violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) 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 i fatti di cui ai commi primo e secondo riguardino 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 (nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio).

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

[8] Per documento informatico, secondo la relazione al disegno di legge originario (v. C. 2807) deve intendersi la "*rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".

Tale fattispecie punisce chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5164 Euro. La pena è della reclusione da uno a due anni e della multa da 5.164 euro a 10.329 Euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617 *quater*.

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

Chiunque, allo scopo di danneggiare illecitamente 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, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a Euro 10.329.

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

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 sei mesi a quattro 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 cui 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 uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro Ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) 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, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato.

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

Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte 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. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo.

1.6. Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)

Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

1.7. 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.)

Salvo che il atto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo

Stato o da altro Ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. 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 tre a otto anni. Se ricorre la circostanza di cui al numero 1), del secondo comma, dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

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

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 uno a cinque anni.

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

Se il fatto di cui all'articolo 635-*quater* è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

1.10. Frode informatica del certificatore di firma elettronica (art. 640 quinquies c.p.)

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero di arrecare ad altri danno, viola gli obblighi previsti alla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

2. Aree a rischio

Il rischio di commissione dei reati informatici e di trattamento illecito dei dati è particolarmente rilevante per la natura delle attività poste in essere dall'Azienda.

In considerazione della *ratio* normativa, i processi che presentano una sensibilità diretta ai rischi di reato sono tutti quelli che presuppongono l'utilizzo di una rete ovvero di un sistema informatico, dunque, tenuto conto delle attività svolte da STONE SECURITY S.R.L. , **gran parte dei processi sono esposti a tale rischio di reato.**

In particolare, con riferimento a tutti i processi di gestione dei singoli tributi, risulta particolarmente sensibile l'attività di verifica e bonifica della banca dati dei contribuenti.

Pertanto, tali reati potrebbero realizzarsi nell'ambito del più ampio processo relativo alla gestione dei Sistemi Informativi nel caso, ad esempio, in cui non siano previste o attivate le misure minime di profilazione utente per gli accessi ai diversi programmi e *database* gestiti dall'Ente, con conseguente possibile manipolazione o alterazione illegittima sugli stessi dati, informazioni e programmi con l'obiettivo di far risultare condizioni essenziali utili ad esempio a garantire un maggiore incasso con conseguente ed evidente beneficio economico per l'Ente.

I reati in esame possono essere commessi da chiunque abbia accesso ai sistemi informatici della società e, in particolare, dai soggetti con significativa dimestichezza informatica o da coloro che in qualità di responsabili del trattamento dati o amministratori di sistema siano in possesso di profili di accesso privilegiato ovvero detengano diversi codici di accesso.

Il reato di Falsità in documenti informatici (art. 491-*bis* c.p.) potrebbe realizzarsi nel caso in cui venga commessa, su un documento informatico avente efficacia probatoria, una delle falsità previste dal Capo III (Falsità in atti) del Titolo VII, Libro II, del Codice (Delitti contro la Fede Pubblica): Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.); Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.); Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici e in attestati del contenuto di atti (art. 478 c.p.); Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.); Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative (art. 480 c.p.); Falsità materiale commessa dal privato in atto pubblico (art. 483 c.p.); Falsità in registri e notificazioni (art. 484 c.p.); Uso di atto falso (art. 489 c.p.).

Il reato di Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.) potrebbe configurarsi laddove un dipendente di STONE SECURITY S.R.L. , anche in concorso con terzi, si introduca in un sistema informatico o telematico protetto da misure di sicurezza, o anche in banche dati, ovvero vi si mantenga senza titolo.

I processi ritenuti maggiormente sensibili per tale fattispecie delittuosa sono i seguenti:

- Gestione delle risorse economiche e finanziarie;
- Gestione risorse umane.

A titolo esemplificativo si indicano possibili modalità di commissione del reato nella realtà dell'Ente:

- accesso da amministratori o utenti ad aree non autorizzate contenenti dati dei clienti o dei dipendenti e del personale in genere quali le cartelle di posta elettronica o il *database* delle retribuzioni del personale, dei dati sensibili (anagrafici, indicatori situazione patrimoniale etc.);

- accesso abusivo ai sistemi che elaborano le buste paga;

- accesso abusivo ai sistemi che realizzano la fatturazione dei servizi ai clienti per alterare le informazioni e i programmi al fine di realizzare un profitto illecito.

Il reato di Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 - *quater* c.p.) potrebbe configurarsi laddove un esponente, un dipendente, fornisca a terzi non autorizzati credenziali di accesso a sistemi informatici posseduti da STONE SECURITY S.R.L. , ovvero consentano a terzi di continuare ad utilizzare le predette credenziali pur non avendone più titolo.

A titolo esemplificativo si indicano possibili modalità di commissione del reato nella realtà imprenditoriale di riferimento:

- detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (art. 615-*quater* c.p.), anche con finalità di accesso abusivo quali quelle sopra indicate (ad esempio credenziali di dipendenti, concorrenti, fornitori, pubbliche amministrazioni ecc.);

- diffusione abusiva (art. 615-*quater* c.p.) di numeri seriali di telefoni cellulari altrui al fine della clonazione degli apparecchi.

Relativamente ai reati della presente Parte Speciale si è proceduto ad individuare ulteriori possibili modalità di commissione del reato nella realtà della società:

- cancellazione o danneggiamento di informazioni, dati, programmi, sistemi o infrastrutture informatiche di soggetti privati (Artt. 615 *quinquies*, 635 *bis*, 635 *quater* c.p.) (ad esempio: danneggiamento di informazioni, dati e programmi di un concorrente causato mediante la diffusione di virus o altri programmi malevoli commessa da soggetti che utilizzano abusivamente la rete o i sistemi di posta elettronica;

- danneggiamento di informazioni, dati, programmi informatici o di sistemi informatici di terzi, anche concorrenti, commesso dal personale incaricato della loro gestione, nello svolgimento delle attività di manutenzione e aggiornamento di propria competenza;

- danneggiamento dei sistemi su cui i concorrenti conservano la documentazione relativa ai propri prodotti/progetti allo scopo di distruggere le informazioni e ottenere un vantaggio competitivo.

- cancellazione o danneggiamento di informazioni, dati, programmi, sistemi o infrastrutture informatiche di soggetti pubblici o di pubblica utilità (Artt. 635-*ter*, 635-*quinquies* c.p.) (ad esempio: danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso enti pubblici quali (es. polizia, uffici giudiziari, ecc.), da parte di dipendenti di enti coinvolti a qualunque titolo in procedimenti o indagini giudiziarie);

- danneggiamento di informazioni, dati e programmi informatici utilizzati da enti pubblici commesso dal personale incaricato della gestione dei sistemi di clienti della Pubblica Amministrazione).

- produzione, riproduzione, importazione, diffusione, comunicazione, consegna o messa a disposizione di apparecchiature, dispositivi o programmi informatici, allo scopo di danneggiare o interrompere sistemi informatici o telematici, o intercettare comunicazione (art. 615-*quinquies* c.p.);

- installazione delle apparecchiature di cui al punto precedente (art. 617-*quinquies*) in particolare per le finalità sopra indicate.

- concorso con un soggetto che presta servizi di certificazione di firma elettronica nella violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato (art. 640-*quinquies*).

Di seguito è stata riportata la **matrice dei rischi** nella quale è espressa la correlazione tra la probabilità di verificazione del reato presupposto e l'impatto che lo stesso avrebbe per STONE SECURITY S.R.L. (a tal proposito si rinvia alla nota metodologica, relativa alla mappatura dei processi e delle attività sensibili e dei rischi ad essi relativi, di cui al paragrafo 10 della Parte generale del presente Modello.

Cod.	**Reati informatici**	**Amministr. unico**	**Direttore Amm.vo**	**Personale tecnico amm.vo preposto alla funzione**
4	Fattispecie selezionate in premessa	Prob. 2 Imp. 3 Rischio: 6	Prob. 2 Imp. 3 Rischio: 6	

SISTEMI DI PREVENZIONE:

3. Destinatari

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli operanti nelle aree di attività a rischio, nonché da Collaboratori esterni e *Partners*, come già definiti nella Parte generale.

Per poter rendere efficace tale sezione, occorre che tutti i Destinatari sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che adottino, pertanto, regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

4. Protocolli preventivi

Al fine di prevenire il presentarsi delle fattispecie delittuose sopra menzionate, STONE SECURITY S.R.L. si è dotata di specifici Procedure preventive:

- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- la definizione delle misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati;
- la previsione di interventi formativi degli incaricati del trattamento dei dati;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del Titolare;

- la nomina dell'Amministratore di sistema, al quale è designata la gestione e la manutenzione del sistema informatico della società o dei clienti;
- la definizione di un procedimento di autenticazione degli utenti mediante *username* e *password* a cui corrisponde un accesso limitato in relazione al ruolo, compiti e responsabilità ricoperte all'interno dell'Ente;
- la disattivazione, al momento delle dimissioni/licenziamento dell'utente, dei profili personali;
- la tracciabilità delle attività e operazioni compiute dagli utenti attraverso i log di sistema sottoposti a controlli periodici e formali al fine di evitare il compimento di operazioni non autorizzate o inusuali;
- accesso alla rete informatica della società, per la consultazione e l'elaborazione di dati, documenti e informazioni da comunicare o ricevuti dalla Pubblica Amministrazione, ovvero per qualunque intervento sui programmi destinati ad elaborarli, avviene attraverso l'utilizzo di ***id* e *password* personali**; gli operatori sono tenuti a mantenere segrete le loro *password*;
- protezione **del *server* e dei dati attraverso l'utilizzo di sistemi anti-intrusione, di *software* antivirus costantemente aggiornati ed attività di *back up*;**
- limitazioni **agli accessi alla rete informatica dall'esterno**, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei destinatari;
- sottoscrizione da parte dei dipendenti, collaboratori e consulenti di uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo delle risorse informatiche della società in conformità con il presente Modello, con il Codice etico dei quali STONE SECURITY S.R.L. si è dotata;
- formare ed informare dipendenti, collaboratori e consulenti sui sistemi informativi, con particolare riferimento all'importanza di mantenere i propri codici di accesso (username e password) confidenziali e di non divulgare gli stessi a soggetti terzi, e alla necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;
- impostazione dei sistemi informatici stessi in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
- limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei destinatari; limitare l'accesso alle aree ed ai siti internet particolarmente sensibili poiché veicolo per la

distribuzione e diffusione di programmi infetti capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti; predisposizione ed aggiornamento annuale del Documento Programmatico di Sicurezza (DPS), nel quale sono analizzate le situazioni ed organizzate procedure per la garanzia della sicurezza nei trattamenti dei dati.

5. Principi generali di comportamento

STONE SECURITY S.R.L. prescrive una serie di regole comportamentali, di seguito indicate, che devono essere obbligatoriamente seguite dai propri dipendenti, collaboratori, consulenti, membri degli organi sociali e di controllo nonché da soggetti terzi con cui intrattiene relazioni.

È anzitutto fatto obbligo di

- rispettare le leggi e i regolamenti applicabili alla materia della protezione e sicurezza dei dati personali e dei sistemi informatici (Codice della Privacy), unitamente alle Policy di sicurezza informatica definita all'interno del sistema di gestione aziendale;
- non divulgare informazioni relative ai sistemi informatici dell'Ente;
- utilizzare le informazioni, i programmi e le apparecchiature aziendali esclusivamente per motivi di ufficio;
- non prestare o cedere a terzi apparecchiature informatiche senza la preventiva autorizzazione da parte del Responsabile dei sistemi informativi; in caso di smarrimento o furto, informare tempestivamente il Responsabile dei Sistemi informativi e presentare denuncia presso l'Autorità Giudiziaria preposta;
- garantire ed agevolare ogni forma di controllo interno e di supervisione sulla adozione delle misure di sicurezza implementate;
- indicare con tempestività e correttezza le eventuali misure da adottare qualora si rilevassero delle carenze nella gestione dei sistemi informatici e di protezione dei dati personali;
- adottare misure di sicurezza, organizzative, fisiche e logistiche per il trattamento dei dati personali;

- evitare di trasferire all'esterno o trasmettere file, documenti o documentazione riservata, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni; astenersi dall'effettuare copie non autorizzate di dati e di *software*;
- gestire come riservati le informazioni e i dati, non pubblici, relativi a clienti e terze parti (commerciali, organizzative, tecniche;
- in caso di smarrimento o furto, informare tempestivamente il Responsabile e presentare senza ritardo denuncia all'Autorità Giudiziaria preposta;
- in mancanza di specifica autorizzazione, astenersi dall'effettuare copie di dati e di software.

È fatto divieto di:

- rappresentare, alle autorità pubbliche e agli organismi di vigilanza, situazioni non veritiere o comunicare dati falsi, lacunosi o, comunque, non rispondenti alla realtà, per influenzarle indebitamente;
- modificare in qualunque modo la configurazione delle postazioni di lavoro fisse o mobili assegnate, installando o utilizzando *software* e *hardware* non approvati dall'Ente e non correlati con l'attività professionale ricoperta;
- acquisire, possedere o utilizzare strumenti *software* e/o *hardware* che potrebbero essere adoperati per compromettere la sicurezza dei sistemi informatici o telematici (sistemi per individuare le password, decifrare i file criptati, intercettare il traffico in transito, ecc.), a meno che non sia esplicitamente contemplato nei propri compiti lavorativi;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o *software* allo scopo di danneggiare il sistema informatico o telematico di soggetti, pubblici o privati, al fine di danneggiare le informazioni, i dati o i programmi in esso contenuti oppure di favorire l'interruzione totale o parziale o l'interruzione del suo funzionamento;
- ottenere abusivamente credenziali di accesso a sistemi informatici o telematici, dei clienti o di terze parti, di soggetti pubblici o privati con metodi o procedure differenti da quelle a tale scopo autorizzate dall'Ente, al fine di acquisire informazioni riservate, alterarle e/o cancellarle;

- divulgare, cedere o condividere con personale interno o esterno all'Ente le proprie credenziali di accesso ai sistemi e alla rete, anche di clienti o di terze parti;
- accedere abusivamente al sistema al fine di alterare e/o cancellare dati e/o informazioni;
- accedere abusivamente al sistema al fine di acquisire informazioni riservate;
- accedere alle banche dati per ottenere informazioni non strettamente connesse all'attività svolta;
- manomettere, sottrarre o distruggere il patrimonio informatico dell'Ente, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici dell'Ente, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici dell'Ente, di clienti o di terze parti;
- comunicare a persone non autorizzate, interne o esterne all'Ente, le misure di controllo implementate sui sistemi informativi e le modalità con cui tali misure sono applicate;
- distorcere, oscurare, sostituire la propria identità e inviare e-mail riportanti false generalità;
- compiere attività di *spamming* e di risposta allo *spam*;
- duplicare programmi per elaboratore;
- installare nella rete di ateneo un *software* che possa impedire, interrompere o danneggiare le comunicazioni all'interno dell'Ente o verso l'esterno o che possa rallentare o bloccare l'intera rete informatica;
- installare nella rete aziendale o sui singoli pc, ovvero utilizzare, duplicare un software in violazione della normativa sul diritto d'autore.

Di fondamentale importanza è regolamentare le modalità di gestione degli accessi ai *personal computers* ed alla rete aziendale e ad *internet*, quali profili centrali nell'identificazione dell'utente.

Sono indicate nel prosieguo anche procedure generali di verifica degli accessi, di visibilità e modificabilità dei dati, nonché di conservazione dei medesimi.

- E' proibito agli utenti della rete internet della società di trasmettere o scaricare materiale considerato osceno, pornografico, minaccioso o che possa molestare la razza o la sessualità.

Tale divieto integra le prescrizioni dettate al riguardo dal Codice Etico della società;

- l'uso dei *computers* disponibili nella rete della società è concesso previa autorizzazione del diretto superiore o del personale preposto e solo per fondati motivi di lavoro o di didattica;
- l'utilizzo di ogni elaboratore (di seguito PC) è riservato e protetto da *password*;
- ogni PC deve disporre di *username* e *password* (che il sistema informatico impone di modificare periodicamente).
- l'accesso ai programmi di contabilità, gestione ed amministrazione della società è concesso, secondo le necessità e con diverse autorizzazioni a seconda della funzione.
- l'utilizzo di *internet* è parimenti strettamente regolamentato.
- il personale non ha accesso alla rete esterna se non previa autorizzazione del proprio diretto superiore gerarchico concessa solo per comprovate ragioni lavorative.

Ogni violazione delle procedure interne enucleate ed *enucleande* per l'utilizzo del sistema informativo e internet deve essere tempestivamente comunicata all'Organismo di Vigilanza.

6. Principi di attuazione dei comportamenti prescritti

6.1. Modalità di accesso ai singoli PC

Ogni singolo PC fa parte del dominio interno predefinito dalla società e, quindi, deve essere autenticato ogni volta che un utente richiede l'accesso al dominio stesso.

Ogni utente è fornito di ***password*** di accesso, sia al PC, che al dominio ed in alcuni casi anche della *password* del BIOS all'accensione del PC.

Le *password* sono personalizzate e vengono modificate con cadenza periodica.

A ciascun utente sono stati forniti i relativi privilegi di accesso a seconda della mansione/attività: la regola generale in tal senso è che ogni utente ha accesso alla propria cartella sul *server* ed ad una cartella

pubblica per lo scambio di informazioni tra utenti. Alcuni utenti hanno accessi condivisi su cartelle di interesse comune.

È fatto divieto di divulgare, cedere o condividere con personale interno o esterno alla società le proprie credenziali di accesso ai sistemi ed alla rete aziendale o di terze parti.

È fatto divieto di accedere a cartelle contenenti informazioni estranee o non pertinenti alle proprie mansioni/attività, facendo utilizzo di postazioni o credenziali altrui, sebbene l'accesso sia in ipotesi autorizzato dal titolare della postazione di lavoro, o delle credenziali in violazione del divieto di cui sopra. Tale divieto si estende anche ai casi in cui le cartelle contenenti informazioni estranee o non pertinenti alle proprie mansioni/attività siano in altro modo accessibili.

È fatto, inoltre, divieto di accedere, copiare in qualunque forma, archiviare e trasferire all'esterno della società, se non previamente autorizzati per ragioni connesse all'esercizio delle proprie mansioni/attività, informazioni e documenti concernenti dati personali di colleghi ed altri soggetti, per qualsiasi finalità.

In caso di assenze del titolare, deve essere regolamentato il passaggio di consegne in ordine ad eventuali scadenze di legge aventi ad oggetto adempimenti telematici, con previsione delle modalità per la sostituzione ed il ripristino delle credenziali di accesso.

6.2. Modalità di archiviazione dei dati e backup

I dati che vengono memorizzati all'interno dei server sono salvati quotidianamente (di norma durante la notte), tramite procedura di *back up*, anche su supporti removibili.

Le copie di salvataggio vengono conservate in zone ignifughe e protette, disponibili solo ad utenti autorizzati.

È fatto divieto di installare e utilizzare programmi per lo scarico, l'archiviazione ed il trasferimento dei dati presenti sul *server* della società, salva autorizzazione espressa del proprio supervisore gerarchico.

6.3. Modalità di visibilità dei dati tra diversi PC

E' possibile condividere con altri utenti/PC risorse locali come stampanti e/o cartelle di dati del proprio PC o del *server* locale.

Gli archivi, anche elettronici, della struttura di gestione sono protetti mediante opportune misure volte ad inibire l'accesso ad operatori appartenenti a settori diversi da quello cui l'archivio si riferisce.

L'accesso è sempre regolamentato da autorizzazioni, previamente concesse dietro presentazione di comprovate esigenze lavorative.

La modifica dei dati può avvenire solo ove autorizzata ed ogni PC che dispone di tale facoltà è utilizzato con *password* d'accesso personale, in modo tale da poter agevolmente risalire alla paternità dell'inserimento o della modifica del dato.

6.4. Modalità di accesso ad internet ed a singoli PC

Ogni utente su PC ha la possibilità di navigare in internet senza alcun limite di tempo, solo se previamente autorizzato dal proprio superiore gerarchico e per esigenze lavorative.

La navigazione è protetta, ossia sono adottati dispositivi tecnici idonei a vietare l'accesso a siti pedopornografici noti alla società.

Per garantire la sicurezza del sistema e dei dati, ogni PC è protetto tramite *antivirus* centralizzato e distribuito dal *server*, costantemente aggiornato.

6.5. Modalità di accesso dall'esterno alla rete aziendale

Dall'esterno possono accedere soltanto gli utenti registrati forniti di connettività mobile, per interrogare la propria casella di posta elettronica attraverso il servizio di *Web-mail*, messo a disposizione dal server di posta elettronica della società e per accedere attraverso una vpn (con le stesse *user* e *password*) alle cartelle personali e/o della funzione per cui sono accordate le autorizzazioni, sempre tramite autenticazione di dominio con il nome utente e la *password* relative.

L'Azienda opera nell'ambito della consulenza in ambito di sicurezza delle informazioni esegue presso i propri clienti attività volte al soddisfacimento dei requisiti normativi richiesti dal Regolamento europeo 679/2016 (GDPR). Pertanto, l'Azienda ha organizzato corsi di formazione per i propri dipendenti, ottenendo l'attestato di esecuzione del percorso di alta formazione GDPR. I contenuti del corso ed il relativo esame finale sono riconosciuti ai fini dell'iter di certificazione AICQ SICEF.

7. Controlli O.d.V.

In riferimento ai reati in esame, l'O.d.V. ha il compito di monitorare il rispetto degli obblighi e dei divieti impartiti al personale interno effettuando verifiche periodiche, anche a campione:

- sulla protezione della rete e dei sistemi informatici;
- sugli accessi degli utenti, sulla sicurezza dei dati nonché sulle attività di *back up* svolte da ciascun dipendente;
- sul funzionamento del sistema di tracciamento degli accessi al *server*;
- sugli accessi effettuati dai dipendenti sul sistema Punto Fisco e sulla coerenza degli stessi rispetto alle pratiche oggetto di lavorazione;
- sull'attivazione di un *antivirus* centralizzato;
- sull'autenticità e la genuinità dei sistemi operativi installati;
- sull'efficacia del sistema di *firewall* e antintrusione;
- sulle eventuali e personalizzate limitazioni agli accessi a internet e sull'eventuale sussistenza ed efficacia di *proxy server*;

- sul rispetto delle politiche di autenticazione in ordine all'accesso alla rete *wireless*.

L'O.d.V. condurrà quindi controlli a campione diretti a verificare le procedure/istruzioni interne ed i Procedure contenuti nel presente Modello nonché l'adeguatezza delle prescrizioni a prevenire i rischi di reato potenziali.

PARTE SPECIALE V

DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

QUALI FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

(Art. 25-*novies*)

1. Reati di violazione del diritto d'autore

I delitti in materia di violazione del diritto d'autore sono stati introdotti con l'inserimento dell'art. 25-*novies* del d.lgs. 231/2001 ad opera della Legge n.99 del 23 luglio 2009

Dettaglio fattispecie criminose: art. 25 novies

1.1. 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, l. 633/1941 comma 1 lett. a) bis)

La norma punisce chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa.

1.2. 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, l. 633/1941 comma 3)

La norma punisce la fattispecie delittuosa di cui all'art. 171, comma 1 lett. a) *bis*, se il reato è commesso con riferimento ad un'opera altrui 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 od alla reputazione dell'autore.

1.3. 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 SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis l. 633/1941 comma 1)

La norma punisce chiunque 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 (S.I.A.E.) e chiunque utilizzi qualsiasi altro mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

1.4. 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 l. 633/1941 comma 2)

La norma punisce chiunque, al fine di trarne profitto, su supporti non contrassegnati S.I.A.E. 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* della legge 633/1941, 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.

1.5. 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. 633/1941)

La norma punisce chiunque, a fini di lucro e per uso non personale: a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati; c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b); d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società Italiana degli Autori ed Editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla

decodificazione di trasmissioni ad accesso condizionato; f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto; f-*bis*) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-*quater* ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale; h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-*quinquies,* ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse. 2. La norma punisce chiunque: a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; a-*bis*) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1; c) promuove o organizza le attività illecite di cui al comma 1.

1.6. Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies l. 633/1941)

La norma punisce i produttori o gli importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis della legge 633/1941 che non comunicano alla Società Italiana degli Autori ed Editori (S.I.A.E.), entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione, i dati necessari alla univoca identificazione dei supporti medesimi, ovvero chiunque

dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-*bis*, comma 2 della medesima legge.

1.7. 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. 633/1941)

La norma punisce chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato 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. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi, visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

2. Aree a rischio

Con riferimento al gruppo di reati, previsti dall'art. 25-*novies* del d.lgs. 231/01, si elencano le fattispecie che potrebbero astrattamente verificarsi nell'ambito dei processi ritenuti sensibili e che presentano un livello di rischio critico o rilevante.

Il reato di messa a disposizione del pubblico in un sistema di reti telematiche di un'opera dell'ingegno protetta o parte di essa o per la quale risulti offeso l'onore o la reputazione (art. 171 l. 633/1941) potrebbe configurarsi in tutte le ipotesi in cui la società, per la realizzazione delle proprie

attività formative e didattiche utilizzasse un'opera dell'ingegno protetta o parte di essa, anche mediante eventuale emissione della stessa in un sistema di reti telematiche.

Il reato di abusiva duplicazione di programmi o predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione per elaborare (art. 171-*bis*, comma 1, L. 633/1941) potrebbe realizzarsi in tutte le ipotesi in cui la società, per la realizzazione delle proprie attività formative e didattiche, utilizzasse programmi contenuti in supporti non contrassegnati dalla SIAE, ovvero abusivamente duplicasse, distribuisse, vendesse o detenesse a scopo imprenditoriale o concedesse in locazione detti programmi.

Il reato di riproduzione o trasferimento su un altro supporto, distribuzione, presentazione in pubblico del contenuto di una banca dati (art. 171-ter, L. 633/1941) potrebbe configurarsi in tutte le ipotesi in cui la società, per lo svolgimento delle proprie attività formative e didattiche, ovvero anche nell'attività di formazione rivolta ai dipendenti, ovvero nelle attività di comunicazione, utilizzasse, riproducendoli, trasmettendoli o diffondendoli in pubblico, in tutto o in parte, le opere di cui all'articolo in esame;

I delitti in materia di violazione del diritto d'autore (artt. 171 *septies* e *octies*, L. 633/1941) potrebbero configurarsi laddove la società, anche quale eventuale importatore o produttore dei supporti non soggetti a contrassegno, non comunicasse alla SIAE, entro trenta giorni dalla data di immissione nel commercio o di importazione, i dati necessari alla identificazione dei supporti, ovvero dichiarasse falsamente l'avvenuto assolvimento degli obblighi di legge; ovvero laddove la società, per la realizzazione delle proprie attività, utilizzasse, installasse o modificasse apparati o parte di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato.

Di seguito è stata riportata la **matrice dei rischi** nella quale è espressa la correlazione tra la probabilità di verificazione del reato presupposto e l'impatto che lo stesso avrebbe per Stone Security S.r.l. (a tal proposito si rinvia alla nota metodologica, relativa alla mappatura dei processi e delle attività sensibili e dei rischi ad essi relativi, di cui al paragrafo 10 della Parte generale del presente Modello.

Cod.	Reati in materia di violazione del diritto d'autore	Amministr. unico	Direttore Amm.vo	Personale tecnico amm.vo preposto alla funzione
5	Fattispecie selezionate in premessa	Prob. 1 Imp. 3 Rischio: 3	Prob. 1 Imp. 3 Rischio: 3	

SISTEMI DI PREVENZIONE

Per la presente Sezione si rinvia a quanto rilevato in riferimento ai reati della precedente Parte speciale (reati informatici).

PARTE SPECIALE VI

REATI ASSOCIATIVI E TRANSNAZIONALI

QUALI FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

(Art. 24 *ter*)

1. Delitti di criminalità organizzata: Associazione per delinquere (art. 24 ter)

Con riferimento ai reati presupposto della responsabilità amministrativa dell'Ente, la Legge n. 94/09 del 15 luglio 2009 ha introdotto (art. 2, c. 29) nel d.lgs. 231/01 il nuovo art. 24-*ter*. L'articolo annovera la fattispecie di reato *Associazione per delinquere* (previsto e punito dall'art. 416 c.p.).

La fattispecie di delitto in esame si realizza quando tre o più persone si associano allo scopo di commettere più delitti. L'art. 416 c.p. punisce coloro che promuovono o costituiscono od organizzano l'associazione. Anche il solo fatto di partecipare all'associazione costituisce reato. I capi soggiacciono alla stessa pena stabilita per i promotori. La pena è aumentata se il numero degli associati è di dieci o più. L'art. 416, primo comma, c.p., ancor prima di richiamare le singole condotte di promozione, costituzione, direzione, organizzazione, ovvero di semplice partecipazione, subordina la punibilità al momento in cui (al "quando") "tre o più persone" si sono effettivamente "associate" per commettere più delitti.

2. Aree a rischio

Di seguito è stata riportata la **matrice dei rischi** nella quale è espressa la correlazione tra la probabilità di verificazione del reato presupposto e l'impatto che lo stesso avrebbe per STONE SECURITY S.R.L. (a tal proposito si rinvia alla nota metodologica, relativa alla mappatura dei processi e delle attività sensibili e dei rischi ad essi relativi, di cui al paragrafo 10 della Parte generale del presente Modello.

Cod.	Reato di associazione per delinquere	Amministr. unico	Direttore Amm.vo	Personale tecnico amm.vo preposto alla funzione
6	Fattispecie selezionate in premessa	Prob. 1 Imp. 3 Rischio: 3	Prob. 1 Imp. 3 Rischio: 3	

SISTEMI DI PREVENZIONE:

3. Destinatari

Le prescrizioni contenute nella presente Parte Speciale sono vincolanti per tutti i titolari, preposti, legali rappresentanti, dipendenti e/o operai in qualsivoglia modo inquadrati nell'azienda.

4. Protocolli preventivi

L'Ente, al fine di prevenire e mitigare il rischio di commissione dei reati in esame, prescrive una serie di adempimenti, coerenti con la normativa, posti a carico del personale, collaboratori, organi di *governance* e terze parti coinvolti nei processi ritenuti sensibili; nello specifico:

• Definizione dei requisiti del personale e dei collaboratori tutti;

• Controlli sul rispetto delle procedure e delle deleghe;

• Formazione continua al personale;

• Divieto di intrattenere rapporti commerciali e contrattuali con soggetti di cui si conosca o si sospetti l'appartenenza ad organizzazioni criminali o svolgano attività illecite (ricettazione, riciclaggio, terrorismo, ecc.) o che comunque presentino comportamenti non trasparenti e non improntati al rispetto delle norme di legge;

• La selezione dei soggetti con cui intrattenere rapporti commerciali e contrattuali, quali fornitori, consulenti, *partner* istituzionali e commerciali, avviene secondo una comparazione obiettiva e trasparente delle offerte basata su criteri oggettivi documentabili e verificabili.

5. Principi e regole di comportamento

Al fine di prevenire la commissione dei reati in trattazione, l'Ente impone:

l'**OBBLIGO** di:

- osservare tutte le leggi e regolamenti che disciplinano le diverse attività svolte all'interno dell'Ente ed impegnarsi, nei limiti delle rispettive competenze, ad operare affinché sia rispettato quanto previsto dalla normativa in materia;
- rispettare il Codice Etico;
- comunicare tempestivamente e con nota scritta all'Organismo di Vigilanza situazioni che possano far ipotizzare il compimento di attività illecite o la sussistenza di conflitto di interessi.

il **DIVIETO** di:

- ricevere danaro, doni o qualsiasi altra utilità ovvero accettarne la promessa, da chiunque sia o intenda entrare in rapporto con l'Ente e voglia conseguire indebitamente un trattamento in violazione della normativa o delle disposizioni impartite o, comunque, un trattamento più favorevole rispetto a quello dovuto;

- eseguire prestazioni e/o riconoscere compensi in favore dei consulenti, collaboratori esterni che non siano adeguatamente giustificati in relazione al tipo di incarico da svolgere, al rapporto contrattuale in essere con l'Ente ed alle prassi vigenti in ambito locale;
- erogare finanziamenti a partiti politici al di fuori dei limiti e delle condizioni stabilite dalla normativa vigente;
- formare dolosamente in modo falso o artefatto documenti dell'Ente.

6. Controlli dell'Organismo di Vigilanza

In relazione all'osservanza del Modello per quanto concerne le prescrizioni di cui alla presente sezione, l'O.d.V. procede a:

• Esaminare le segnalazioni di presunte violazioni del Modello con particolare riferimento alla segnalazione di contatti intercorsi tra esponenti dell'Ente e soggetti che rivestano la qualità di testimoni, potendo anche convocare i medesimi, dopo che abbiano svolto il loro ufficio di testimone, al fine di verificare se abbiano ricevuto pressioni indebite;

• Conservare traccia dei flussi informativi ricevuti e delle verifiche eseguite, ivi compresa la verbalizzazione delle eventuali audizioni di cui al punto che precede.

A tal fine, all'O.d.V. è garantito libero accesso a tutta la documentazione in possesso della società necessaria allo svolgimento delle verifiche, ivi compresa la documentazione relativa ai procedimenti giudiziari di cui l'Ente o gli esponenti dello stesso siano parte.

6.1. Reati transnazionali

Lo stesso reato di cui *supra* rileva ai fini del Modello 231 anche per quanto riguarda quel tipo di reati, i Reati transazionali, nel compimento dei quali sono coinvolti soggetti operanti in più Stati.

Sono di seguito individuati i reati alla cui commissione da parte di soggetti riconducibili all'Azienda (soggetti apicali e persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali, ai sensi dell'art. 5 del Decreto) è collegato il regime di responsabilità a carico della stessa Azienda, previsti dalla legge 16 marzo 2006, n. 146, che ratifica e dà esecuzione alla Convenzione e ai Procedure

delle Nazioni Unite contro il crimine organizzato transnazionale adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001 (di seguito "Convenzione").

La Convenzione si prefigge lo scopo di promuovere la cooperazione per prevenire e combattere il crimine organizzato transnazionale in maniera più efficace. A tale riferimento, richiede che ogni Stato parte della Convenzione adotti le misure necessarie, conformemente ai suoi principi giuridici, per determinare la responsabilità degli enti e delle società per i fatti di reato indicati dalla Convenzione stessa.

Come già rilevato nella Sezione III della presente Parte Speciale l'art. 10 (Responsabilità amministrativa degli Enti) della citata legge prevede l'estensione della disciplina del d.lgs. 231/2001 in riferimento ad alcuni reati, ove ricorrano le condizioni di cui all'art. 3, ossia ove il reato possa considerarsi **transnazionale**. In questo caso, non sono state inserite ulteriori disposizioni nel corpo del d.lgs. 231/2001. La responsabilità deriva da un'autonoma previsione contenuta nel predetto art. 10 della legge n. 146/2006, il quale stabilisce le specifiche sanzioni amministrative applicabili ai reati sopra elencati, disponendo – in via di richiamo - nell'ultimo comma che "agli illeciti amministrativi previsti dal presente articolo si applicano le disposizioni di cui al d.lgs. 8 giugno 2001, n. 231".

Ai sensi dell'art. 3 della legge sopra menzionata si considera reato transnazionale "il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché: sia commesso in più di uno Stato; ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato; ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; L'articolo 10 della Convenzione così recita:"1. Ogni Stato Parte adotta misure necessarie, conformemente ai suoi principi giuridici, per determinare la responsabilità delle persone giuridiche che partecipano a reati gravi che coinvolgono un gruppo criminale organizzato e per i reati di cui agli artt. 5, 6, 8 e 23 della presente Convenzione. 2 Fatti salvi i principi giuridici dello Stato Parte, la responsabilità delle persone giuridiche può essere penale, civile o amministrativa. 3 Tale responsabilità è senza pregiudizio per la responsabilità penale delle persone fisiche che hanno commesso i reati. 4 Ogni Stato Parte si assicura, in particolare, che le persone giuridiche ritenute responsabili ai sensi del presente articolo siano soggette a sanzioni efficaci, proporzionate e dissuasive, di natura penale o non penale, comprese sanzioni pecuniarie." ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato."

Per "gruppo criminale organizzato" ai sensi della citata Convenzione si intende "un gruppo strutturato, esistente per un periodo di tempo, composto da tre o più persone che agiscono di concerto al fine di commettere uno o più reati gravi o reati stabiliti dalla convenzione, al fine di ottenere, direttamente o indirettamente, un vantaggio finanziario o un altro vantaggio materiale".

E' prevista, quale conseguenza della commissione dei reati transnazionali elencati, l'applicazione all'Ente delle sanzioni amministrative sia pecuniarie che interdittive (a eccezione dei reati di intralcio alla giustizia per i quali è prevista la sola sanzione pecuniaria).

Di seguito è stata riportata la **matrice dei rischi** nella quale è espressa la correlazione tra la probabilità di verificazione del reato presupposto e l'impatto che lo stesso avrebbe per STONE SECURITY S.R.L. (a tal proposito si rinvia alla nota metodologica, relativa alla mappatura dei processi e delle attività sensibili e dei rischi ad essi relativi, di cui al paragrafo 10 della Parte generale del presente Modello.

7. Aree a Rischio

Cod.	**Reati transnazionali**	**Amministr. unico**	**Direttore Amm.vo**	**Personale tecnico amm.vo preposto alla funzione**
7	Fattispecie selezionate in premessa	Prob. 1 Imp. 3 Rischio: 3	Prob. 1 Imp. 3 Rischio: 3	

SISTEMI DI PREVENZIONE:

8. Destinatari

Le prescrizioni contenute nella presente Parte Speciale sono vincolanti per tutti i titolari, preposti, legali rappresentanti, dipendenti e/o operai in qualsivoglia modo inquadrati nell'azienda.

9. Protocolli preventivi

Presupposto necessario per la responsabilità dell'Ente è che i suindicati reati vengano commessi in un contesto internazionale. Se ciò, in considerazione dell'attività svolta da STONE SECURITY S.R.L. ha un basso impatto in termini probabilistici, tuttavia si tratta di un gruppo di reati che necessita comunque di essere mappato, in considerazione della possibilità che esso venga commesso da dipendenti o soggetti apicali della società in concorso con terzi.

Inoltre, dal momento che l'art. 3 della legge 146/2006 considera transnazionale quel reato commesso in uno Stato ma di cui "una parte sostanziale della preparazione, pianificazione, direzione o controllo avvenga in un altro Stato", ben ci si avvede di come i Procedure preventivi debbano sostanzialmente coincidere con quelli previsti per le stesse fattispecie di reato commesse in ambito nazionale, cui si rimanda.

10. Principi e regole di comportamento

I principi e le regole di comportamento sono sostanzialmente le medesime già affrontate e analizzate nella trattazione delle medesime fattispecie di reato commesse in ambito nazionale.

Si rimanda, perciò, oltre a quanto stabilito nel presente Modello nelle trattazioni che precedono, al rispetto costante delle Procedure, del Codice Etico dei quali STONE SECURITY S.R.L. si è dotata.

11. Controlli dell'Organismo di Vigilanza

Anche con riferimento ai controlli da parte dell'O.d.V., in relazione all'osservanza del Modello per quanto concerne le prescrizioni di cui alla presente Sezione, oltre a rimandarsi a quanto stabilito nei paragrafi che precedono per quanto riguarda le medesime tipologie di reato già affrontate, si evidenziano le seguenti verifiche:

- Esaminare le segnalazioni di presunte violazioni del Modello con particolare riferimento alla segnalazione di contatti intercorsi tra esponenti della società e soggetti che rivestano la qualità di testimoni, potendo anche convocare i medesimi, dopo che abbiano svolto il loro ufficio di testimone, al fine di verificare se abbiano ricevuto pressioni indebite;
- Conservare traccia dei flussi informativi ricevuti e delle verifiche eseguite, ivi compresa la verbalizzazione delle eventuali audizioni di cui al punto che precede.

A tal fine, all'O.d.V. è garantito libero accesso a tutta la documentazione necessaria allo svolgimento delle verifiche, ivi compresa la documentazione relativa ai procedimenti giudiziari di cui l'Ente o gli esponenti dello stesso siano parte.

PARTE SPECIALE VII

REATI IN MATERIA DI INFORTUNI SUL LAVORO

QUALI FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

(Art. 25-*septies*)

1. I reati in materia di infortuni sul lavoro

La legge 3 agosto 2007, n. 123, ha inserito nel d.lgs. 231/2001 l'art. 25-*septies*, estendendo la responsabilità dell'Ente ai reati di omicidio colposo e lesioni colpose gravi e gravissime commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro. Il Consiglio dei Ministri, in data 1 aprile 2008, ha approvato il Decreto Legislativo 81/2008, attuativo della delega di cui all'articolo 1 della legge 3 agosto 2007 n. 123 in materia di tutela della salute e sicurezza nei luoghi di lavoro, modificato dal Decreto Legislativo 3 agosto 2009, n. 106 "Disposizioni integrative e correttive del decreto legislativo 9 aprile 2008, n. 81, in materia di tutela della salute e della sicurezza nei luoghi di lavoro".

Di seguito si riporta una breve descrizione delle fattispecie di reato "presupposto" della responsabilità amministrativa della società.

1.1. Omicidio colposo (art. 589, comma 2, c.p.)

La fattispecie in esame si realizza quando si cagiona per colpa la morte di una persona con violazione delle norme per la prevenzione degli infortuni sul lavoro.

1.2. Lesioni colpose gravi o gravissime (art. 590, comma 3, c.p.)

La fattispecie in esame si realizza quando si cagiona ad altri per colpa una lesione personale grave o gravissima con violazione delle norme per la prevenzione degli infortuni sul lavoro. Il delitto, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale, è perseguibile

d'ufficio. Ai sensi dell'art. 583 c.p., la lesione personale è: grave: - 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; - se il fatto produce l'indebolimento permanente di un senso o di un organo; gravissima se dal fatto deriva: - una malattia certamente o probabilmente insanabile; - la perdita di un senso; - la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella; - la deformazione, ovvero lo sfregio permanente del viso.

In astratto si ipotizza il rischio di sanzioni per negligenza o in virtù di una politica di contenimento dei costi che concretizza il vantaggio per l'Ente, ad esempio per omessa o ridotta dotazione di Dispositivi Individuali di Protezione (DPI) e/o riduzione dei controlli per inerzia e/o inadempienza da parte di coloro che sono tenuti ad osservare o far osservare le norme di prevenzione e protezione (ossia RSPP, soggetti destinatari di deleghe di funzione specifiche, ecc., nonché i medesimi lavoratori); il tutto aggravato da una mancata comunicazione agli organi competenti in caso di infortunio.

Esclusione della responsabilità amministrativa dell'Ente:

Il d.lgs. n. 81/2008, all'art. 30, ha indicato le caratteristiche e i requisiti che deve possedere un Modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al Decreto.

I PROCESSI SENSIBILI

I reati considerati in questa Parte speciale, anziché di natura dolosa sono di natura colposa, ossia commessi in conseguenza di negligenza, imprudenza o imperizia, ovvero commessi per inosservanza di Leggi, Regolamenti, ordini o discipline da parte del soggetto agente. Per questo la funzione esimente del Modello organizzativo è rappresentata da previsioni volte a far sì che i destinatari pongano in essere una condotta (priva della volontà dell'evento morte o lesioni personali) rispettosa delle procedure previste dal sistema di prevenzione e protezione ai sensi del Testo Unico sulla Sicurezza del Lavoro, congiuntamente agli obblighi di vigilanza previsti dal Modello organizzativo.

Nell'ambito delle attività svolte da STONE SECURITY S.R.L. le aree e i processi sensibili che risultano attinenti con i reati in tema di salute e sicurezza sul lavoro sono connessi alla Gestione della Sicurezza sul Lavoro del personale dipendente, dei consulenti e dei collaboratori esterni di cui la società si avvale in particolare per lo svolgimento delle attività svolte al di fuori della sede lavorativa (es: attacchini, rilevatori) non trascurando, tuttavia, la tutela del personale che opera stabilmente presso la sede da STONE SECURITY S.R.L. , nonchè presso gli Uffici distaccati.

La società ha, pertanto, previsto e implementato un sistema di gestione e prevenzione in materia di sicurezza, in linea alle normative vigenti in materia.

Oltre a ciò rilevano:

1) tutte le attività della società individuate come a rischio nell'apposito documento redatto ai sensi degli articoli 17 e 28 d.lgs 81/2008;
2) L'attività stessa di individuazione dei rischi per la sicurezza e dell'aggiornamento documento di cui all'art. 28 d.lgs 81/2008;
3) Gli adempimenti relativi alle prescrizioni sulla sicurezza e più in generale di ogni altra normativa vigente, nazionale e/o sovranazionale;
4) L'adempimento dei doveri e degli obblighi imposti dalle normative vigenti nazionali e/o sovranazionali;
5) Formazione ed aggiornamento dei lavoratori;
6) Gestione degli acquisti dei dispositivi di protezione, collettivi e individuali e di tutti i beni che possano influire sulla sicurezza;
7) Attività di controllo e sanzione di comportamenti che possano costituire fattori di rischio per la sicurezza;
8) Sensibilizzazione della *governance* della società e del personale operante a tutti i livelli presso STONE SECURITY S.R.L. circa la necessità di centrare gli obiettivi prefissati in materia di sicurezza e salubrità del lavoro;

Le scelte organizzative assunte dalla società sono tali da assicurare la migliore competenza e professionalità dei soggetti incaricati a vario titolo di garantire sicurezza e salubrità del luogo di lavoro, nonché piena certezza sui compiti e le deleghe loro conferiti.

I relativi processi sono adeguatamente formalizzati dalla società e vengono sottoposti periodicamente al monitoraggio dell'Organismo di Vigilanza.

ORGANIZZAZIONE DELLE ATTIVITA' PER LA SICUREZZA

Le attività tese a garantire la sicurezza e la salubrità del luogo di lavoro sono formalizzate mediante apposite Procedure alle quali si rinvia integralmente.

Di seguito è stata riportata la **matrice dei rischi** nella quale è espressa la correlazione tra la probabilità di verificazione del reato presupposto e l'impatto che lo stesso avrebbe per STONE SECURITY S.R.L. (a tal proposito si rinvia alla nota metodologica, relativa alla mappatura dei processi e delle attività sensibili e dei rischi ad essi relativi, di cui al paragrafo 10 della Parte generale del presente Modello.

2. Aree a Rischio

Cod.	**Reati in materia di infortuni sul lavoro**	**Amministr. unico**	**Direttore Amm.vo**	**Personale tecnico amm.vo preposto alla funzione**
8	Fattispecie selezionate in premessa	Prob. 2 Imp. 3 Rischio: 6	Prob. 2 Imp. 3 Rischio: 6	

SISTEMI DI PREVENZIONE

3. Destinatari

Le prescrizioni contenute nella presente Parte Speciale sono da rivolte ai dipendenti di STONE SECURITY S.R.L. , ai membri degli Organi di governo della società, agli esponenti, ai collaboratori, *partners*, fornitori ecc., i quali sono espressamente tenuti ad osservarle al fine di eliminare o ridurre a livelli accettabili il rischio di commissione dei reati descritti nella presente Sezione, nella misura in cui essi operano nelle aree a rischio ed in relazione ai diversi ruoli e obblighi, al fine di impedire la commissione di reati colposi in violazione delle norme relative alla tutela della salute e della sicurezza sul lavoro.

4. Protocolli preventivi

Il presente paragrafo contempla i principi generali e specifici di comportamento, nonché i Procedure adottati, che tutti i soggetti coinvolti (Dipendenti, membri degli Organi di governo della società, Collaboratori, ecc.) sono espressamente tenuti ad osservare al fine di eliminare o ridurre a livelli accettabili il rischio di commissione dei reati descritti, nella misura in cui essi operano nelle aree a rischio ed in relazione ai diversi ruoli e obblighi, al fine di impedire la commissione di reati colposi in violazione delle norme relative alla tutela della salute e della sicurezza sul lavoro.

Stone Security S.r.l. al fine di prevenire i reati descritti provvede:

- a nominare, previa verifica del possesso dei requisiti previsti dalla legge di riferimento, il RSPP, il Medico competente, i dipendenti incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave ed immediato, di salvataggio, di primo soccorso e di gestione delle emergenze;

- a fornire ai dipendenti i necessari ed idonei dispositivi di protezione individuale, sentito il RSPP ed il Medico Competente;

- a adottare le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico;

- a garantire il rispetto degli obblighi di informazione, formazione ed addestramento;

- a garantire l'aggiornamento delle misure di prevenzione in relazione ai mutamenti organizzativi che hanno rilevanza ai fini della salute e sicurezza del lavoro;

- a garantire la sicurezza dei locali, delle attrezzature e dei macchinari ai quali i dipendenti e/o collaboratori a vario titolo hanno accesso.

Il Responsabile del Servizio di Prevenzione e Protezione (RSPP) provvede:

- all'individuazione dei fattori di rischio ed alla valutazione dei rischi specifici per le attività svolte;

- ad elaborare, per quanto di competenza, le misure preventive e protettive a seguito della valutazione dei rischi e dei sistemi di controllo di tali misure;

- ad elaborare le procedure/istruzioni di sicurezza specifiche per le attività svolte all'interno della società;

- a proporre i programmi di informazione e formazione dei dipendenti e dei collaboratori tutti;

- a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro nonché alla riunione periodica di cui all'art. 35 del d. lgs. 81/2008;

- a fornire ai destinatari della presente Parte Speciale ogni informazione in tema di tutela della salute e sicurezza sul lavoro che si renda necessaria;

- a monitorare l'effettiva adozione da parte del personale e collaboratori dei dispositivi di protezione individuale ed ogni azione preventiva per la messa in sicurezza degli stessi.

Il Medico competente provvede a:

- collaborare con la società e con il RSPP alla valutazione dei rischi, anche ai fini della programmazione - ove necessario - della sorveglianza sanitaria, alla adozione delle misure per la tutela della salute e dell'integrità psicofisica dei dipendenti e collaboratori, all'attività di formazione ed informazione nei loro confronti, per la parte di competenza, e all'organizzazione del servizio di primo soccorso considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro;

- programmare ed effettuare la sorveglianza sanitaria;

- istituire, aggiornare e custodire sotto la propria responsabilità una cartella sanitaria e di rischio per ogni lavoratore sottoposto a sorveglianza sanitaria;

- fornire informazioni sul significato degli accertamenti sanitari a cui sono sottoposti ed informandoli sui relativi risultati;

- comunicare per iscritto i risultati anonimi collettivi della sorveglianza sanitaria effettuata, fornendo indicazioni sul significato di detti risultati ai fini dell'attuazione delle misure per la tutela della salute e della integrità psicofisica;

- visitare gli ambienti di lavoro almeno una volta all'anno o a cadenza diversa in base alle risultanze dell'attività di valutazione dei rischi;

- partecipare alla programmazione dell'attività di controllo sull'esposizione a rischi specifici dei dipendenti, i cui risultati gli sono forniti con tempestività ai fini della valutazione del rischio e della sorveglianza sanitaria.

- il Rappresentante dei lavoratori (RSL) viene eletto per rappresentare i Lavoratori in materia di salute e sicurezza sul lavoro e riceve la prevista formazione specifica. Può essere consultato preventivamente e tempestivamente in merito a: la designazione del RSPP, del Medico Competente, dei Responsabili e degli incaricati; la valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive; l'organizzazione delle attività formative. Promuove l'elaborazione, l'individuazione e l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei Lavoratori e partecipa alla riunione periodica di prevenzione e protezione dai rischi;

- i Preposti alla prevenzione incendi, all'evacuazione dei luoghi di lavoro, al salvataggio, al primo soccorso e alla gestione delle emergenze.

La Politica della Sicurezza riguarda tutti i processi operativi della società e ha l'obiettivo di enunciare i principi ispiratori di ogni singola attività a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della società, nell'ottica della tutela della salute e sicurezza dei Lavoratori.

Nel rispetto della Politica della Sicurezza, STONE SECURITY S.R.L. , con il supporto operativo del RSPP e del Medico Competente, assicura la predisposizione del Documento di Valutazione dei Rischi (DVR), il quale contiene:

- una valutazione di tutti i rischi, relativi alle attività svolte nell'ambito della società, per la sicurezza e la salute sul lavoro, nella quale siano specificati i criteri adottati per la valutazione stessa;

- l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuale adottati a seguito della suddetta valutazione dei rischi (artt. 74-79 del d.lgs. 81/2008);

- il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;

- l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione interna alla società che vi debbono provvedere;

- l'indicazione dei nominativi del RSPP, del RLS e del Medico Competente che abbiano partecipato alla valutazione dei rischi;

- l'individuazione delle mansioni che eventualmente espongono a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione ed addestramento;

- una valutazione del livello di rischio residuo presente all'interno dell'Ente, nonostante le attività di prevenzione e controllo implementate.

Il DVR viene aggiornato ogni qualvolta che vi siano modifiche nei processi di svolgimento delle attività proprie dell'Ente significative ai fini della sicurezza e della salute dei Lavoratori.

5. Principi e regole di comportamento

Al fine di impedire il verificarsi dei Reati in esame, tutti i soggetti coinvolti nell'attività di tutela della salute e della sicurezza e nelle attività esposte a rischi di infortunio sul lavoro sono tenuti a rispettare, ciascuno secondo le proprie competenze, i principi di seguito riportati:

a. È OBBLIGATORIO:

- identificare ed applicare scrupolosamente le prescrizioni delle norme vigenti in tema di tutela della salute e sicurezza sul lavoro, con particolare riferimento al d.lgs. 81/2008, e archiviare con diligenza la documentazione attestante l'avvenuto adeguamento alle prescrizioni in materia;

- definire obiettivi, in materia di tutela della salute e della sicurezza sul lavoro, allineati con gli impegni definiti nelle politiche governative di tutela della salute e della sicurezza sul lavoro ed elaborare

programmi per il raggiungimento di tali obiettivi con relativa definizione di priorità e tempi, attribuzione delle responsabilità ed assegnazione di adeguate risorse;

- sensibilizzare tutti gli addetti operanti a qualsivoglia titolo nell'ambito dell'azienda, al fine di garantire il raggiungimento degli obiettivi prefissati, anche attraverso la programmazione di piani di informazione e formazione incentrati, in particolare, sui seguenti argomenti: monitoraggio, periodicità dei controlli, fruizione dei corsi di formazione, aggiornamento e promozione dell'apprendimento, prevedendo anche corsi differenziati per soggetti esposti a rischi specifici;

- rispettare quanto stabilito in tema di sicurezza sul lavoro; in particolare la segnalazione di una eventuale deviazione dal DVR deve essere rilevata dal RSPP e fornita all'O.d.V.;

- attuare adeguate attività di monitoraggio, verifica ed ispezione al fine di assicurare l'efficacia del sistema di gestione della salute e sicurezza sul lavoro, in particolare per ciò che concerne:

- l'adozione di misure di mantenimento e miglioramento;

- la gestione, rettifica ed inibizione dei comportamenti posti in essere in violazione delle norme e relativi provvedimenti disciplinari;

- la coerenza tra attività svolta e competenze possedute;

- garantire ed agevolare ogni forma di controllo interno e di supervisione sulla adozione delle misure previste dalla normativa indicata;

- osservare le disposizioni impartite dalla *governance* della società e dai Preposti, prendendosi cura della propria salute e sicurezza e valutando sempre con attenzione gli effetti delle proprie condotte in relazione al rischio di infortunio;

- rispettare le procedure di sicurezza, emergenza trasmesse dal RSPP e le prescrizioni impartite dalla segnaletica di sicurezza nonché i contenuti delle procedure vigenti;

- dare tempestiva segnalazione all'RSPP e all'O.d.V. di eventuali situazioni di pericolo in atto o in potenza o di quasi infortunio, di cui si è venuti a conoscenza, ed informare tempestivamente l'Organismo di Vigilanza in caso di morte o lesione personale grave o gravissima;

- assicurare un costante ed efficace monitoraggio delle misure preventive e protettive adottate per la gestione della salute e sicurezza sul lavoro, dell'adeguatezza e della funzionalità del sistema di gestione delle

misure a tutela della salute e della sicurezza sul lavoro volte a raggiungere gli obiettivi prefissati e della sua corretta applicazione;

- assicurare la verificabilità di ciascuna operazione ed azione di controllo e monitoraggio mediante la predisposizione, da parte dei soggetti incaricati della funzione, di un report semestrale, relativo alle eventuali problematiche riscontrate ed indirizzato all'Organismo di Vigilanza addetto alla supervisione.

- adottare tempestivamente le necessarie azioni correttive e preventive in funzione degli esiti dell'attività di monitoraggio;

- compiere un'approfondita analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere;

- provvedere alla conservazione, sia su supporto cartaceo che informatico, dei seguenti documenti: cartella sanitaria visite mediche obbligatorie, la quale deve essere istituita e aggiornata dal Medico Competente e custodita dal Datore di Lavoro; registro degli infortuni; DVR;

- garantire evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal Medico Competente;

- adottare e mantenere aggiornato il registro delle pratiche delle malattie professionali riportante, data, malattia, data emissione certificato medico e data inoltro della pratica;

- organizzare e gestire dei corsi di formazione per gli addetti alla gestione delle emergenze antincendio (rischio medio e alto), evacuazione e primo soccorso;

- conservare tutta la documentazione relativa alle attività di informazione e formazione a cura del RSPP e messa a disposizione dell'Organismo di Vigilanza;

- effettuare un periodico riesame del sistema di gestione della salute e sicurezza sul lavoro al fine di valutarne l'efficacia ed efficienza a raggiungere gli obiettivi prefissati, nonché l'adeguatezza di questi ultimi rispetto sia alle contingenze reali della'Ente che ad eventuali cambiamenti nella sua attività o organizzazione;

- dotare i singoli lavoratori dei dispositivi di protezione individuali in funzione dell'attività lavorativa; gli stessi hanno l'obbligo di farne uso.

b. È VIETATO:

- mettere in atto comportamenti tali da esporre la società o da favorire l'attuarsi di una delle fattispecie di reato previste dall'art. 25 - *septies* del D.lgs. 231/2001;

- omettere l'aggiornamento delle misure di prevenzione, in relazione a mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e della sicurezza del lavoro, ovvero in relazione al grado di evoluzione della tecnica, della prevenzione e della protezione;

- omettere l'adozione di misure preventive lasciando libero accesso, ai lavoratori che non abbiano ricevuto adeguate istruzioni e formazione, a zone che espongono a rischi gravi e specifici;

- emanare ordini di ripresa del lavoro, nonostante la persistenza di una situazione di pericolo grave ed immediato;

- omettere l'adozione di misure antincendio e di pronta evacuazione in caso di pericolo grave ed immediato;

- rappresentare situazioni non veritiere o comunicare alle Autorità competenti dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sullo stato delle misure antinfortunistiche e a tutela dell'igiene e della salute sul posto di lavoro assunte;

- omettere dati ed informazioni imposti dalla legge sulle misure antinfortunistiche ed a tutela dell'igiene e della salute sul posto di lavoro;

- assumere o somministrare bevande alcoliche nell'ambito dello svolgimento di attività che presentano un maggiore rischio di infortunio e un rischio elevato per la sicurezza, incolumità o la salute di terzi.

6. Controlli dell'Organismo di Vigilanza

In relazione alla tutela della salute e della sicurezza sul lavoro, l'Organismo di Vigilanza svolge le seguenti attività:

- verifiche periodiche, avvalendosi eventualmente della collaborazione di consulenti qualificati, sul rispetto dei principi e degli adempimenti previsti dalla normativa vigente e dai regolamenti interni in

materia valutandone periodicamente l'efficacia a prevenire la commissione dei reati di cui all'art. 25 - *septies* del Decreto;

- suggerimento di eventuali azioni correttive qualora vengano rilevate violazioni delle norme sulla tutela della salute e sicurezza sul lavoro, ovvero in occasione di cambiamenti significativi nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;

- collaborazione alla predisposizione e/o aggiornamento delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate, volte ad assicurare la tutela della salute e della sicurezza sul lavoro.

Allo scopo di svolgere i propri compiti, l'Organismo di Vigilanza:

- verifica l'effettivo svolgimento degli incontri o eventi formativi organizzati dalla società in materia di sicurezza sul lavoro;

- incontra periodicamente le funzioni preposte alla sicurezza ossia il RSPP, il RLS ed il Medico Responsabile, e partecipa alle loro riunioni periodiche in tema di sicurezza sul lavoro;

- accede a tutta la documentazione e le informazioni necessarie per lo svolgimento dei propri compiti.

Inoltre l'Organismo di Vigilanza è destinatario di specifici flussi informativi, almeno quadrimestrali, da parte delle funzioni preposte, atti a consentire l'acquisizione delle informazioni necessarie per il monitoraggio dei Procedure preventivi e delle eventuali criticità rilevate, nonché degli eventi relativi ad incidenti o infortuni, in atto o potenziali.

Sulla base dei flussi informativi ricevuti, l'Organismo di Vigilanza conduce verifiche mirate su determinate operazioni effettuate nell'ambito delle aree a rischio, volte ad accertare, da un lato, il rispetto di quanto stabilito nel presente Modello e nei Procedure, dall'altro l'effettiva adeguatezza delle prescrizioni in essi contenute a prevenire i reati potenzialmente commissibili.

PARTE SPECIALE VIII

REATI AMBIENTALI

QUALI FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

(Art. 25-*undecies*)

Premessa

Il presente Modello rappresenta parte integrante ed, insieme, strumento di sintesi del sistema di prevenzione per la gestione ambientale in essere presso STONE SECURITY S.R.L. finalizzato a garantire il raggiungimento degli obiettivi di tutela dell'ambiente.

La società agisce nel pieno rispetto della normativa vigente in materia di tutela ambientale.

STONE SECURITY S.R.L. , in tale ottica si impegna:

- al rispetto della legislazione in materia di tutela dell'ambiente;
- al miglioramento continuo del sistema di gestione dell'ambiente;
- a fornire le risorse economiche, umane e strumentali necessarie;
- a far sì che i dipendenti e i lavoratori in genere siano sensibilizzati, informati e formati per assumere le loro responsabilità in materia di ambiente;
- a coinvolgere e consultare i lavoratori, anche attraverso il responsabile per l'ambiente;
- a riesaminare periodicamente la politica adottata in materia di ambiente ed il sistema di gestione attuato;
- a definire e diffondere, all'interno della società, gli obiettivi di ambiente e i relativi programmi di attuazione;

- a monitorare costantemente la salvaguardia dell'ambiente, attraverso la verifica del raggiungimento degli obiettivi e della funzionalità del sistema.

La società, nell'ottica di un continuo e progressivo miglioramento degli standard qualitativi e di conformità normativi ha ritenuto opportuno dotarsi delle seguenti certificazioni ISO9001, ISO14001, ISO45001.

1. I reati ambientali

L'art. 25-*undecies* del Decreto, per come modificato con Legge 22 maggio 2015, n. 68, prevede la responsabilità dell'ente in relazione ad alcuni reati ambientali ed in particolare per le fattispecie che di seguito saranno descritte:

1.1. Inquinamento Ambientale (art. 452- bis c.p.)

Il delitto, introdotto dalla Legge n. 68/2015, punisce 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.

Ai sensi dell'art. 25-*undecies*, comma 1, lett. a) del Decreto, così come modificato dalla Legge n. 68/2015, si applica all'Ente la sanzione pecuniaria da 250 a 600 quote.

Inoltre, in caso di condanna, si applica all'Ente una delle sanzioni interdittive *ex* art. 9 del Decreto per una durata non superiore ad un anno (art. 25 *undecies*, comma 1–*bis* del Decreto).

Nell'ipotesi in cui il reato sopra descritto sia stato commesso con colpa e non con dolo, ai sensi dell'art. 452-*quinquies* c.p. si applica all'Ente la sanzione pecuniaria da 200 a 500 quote (come previsto dall'art. 25-*undecies*, comma 1, lett. c del Decreto).

1.2. Delitti associativi aggravati. Associazione per delinquere e di stampo mafioso finalizzata a commettere uno dei delitti previsti dal nuovo Titolo VI – bis del codice penale (art. 452 - octies c.p.)

L'art. 452 *octies* c.p., introdotto dalla Legge 22 maggio 2015, n. 68, estende la categoria dei possibili reati – scopo dell'associazione per delinquere (art. 416 c.p.) e dell'associazione di stampo mafioso (art. 416 *bis* c.p.) ricomprendendovi anche i reati previsti e disciplinati dal nuovo Titolo VI – *bis* del codice penale, intitolato "Dei delitti contro l'ambiente".

In particolare, la norma di nuovo conio prevede, al primo comma, un aumento delle pene di cui all'art. 416 c.p., quando l'associazione è diretta, in via esclusiva o concorrente, allo scopo di commettere taluno dei delitti di cui al nuovo titolo VI–*bis* del codice penale.

Il secondo comma prescrive, invece, un aumento delle pene di cui all'art. 416-*bis* c.p., quando l'associazione di stampo mafioso è finalizzata a commettere taluno dei delitti previsti dallo stesso titolo VI–*bis* del codice penale, ovvero è diretta ad acquisire la gestione o il controllo di attività economiche, di concessioni, di autorizzazioni, di appalti o di servizi pubblici in materia ambientale.

Le pene di cui ai commi primo e secondo sono aumentate da un terzo alla metà se dell'associazione fanno parte pubblici ufficiali o incaricati di un pubblico servizio che esercitano funzioni o svolgono servizi in materia ambientale.

In tale ipotesi si applica all'Ente la sanzione pecuniaria da 300 a 1000 quote (art. 25-*undecies*, comma 1, lett. d).

1.3. Gestione dei rifiuti (art. 256, comma 1, lett. a e comma 6, primo periodo, d.lgs. n. 152/2006)

L'art. 256, comma 1, del d. lgs. n. 152/2006 dispone, per quanto di interesse in questa sede (lettera a), che chiunque, fuori dai casi sanzionati ai sensi dell'articolo 29-*quattuordiecies*, comma 1, 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 con la pena dell'arresto da tre mesi a un anno o con ammenda da duemilaseicento euro a ventiseimila euro se si tratta di rifiuti non pericolosi.

Il comma 6 dell'art. 256, invece, punisce con la pena dell'arresto da tre mesi ad un anno o con la pena dell'ammenda da duemilaseicento euro a ventiseimila euro, 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).

Ai sensi dell'art. 25-*undecies*, comma 2, lett. b), n. 1, del Decreto si applica all'Ente la sanzione pecuniaria fino a 250 quote. Tale sanzione è ridotta della metà nel caso di commissione del reato previsto dall'art. 256, comma 4 d. lgs n. 152/2006 (inosservanza delle prescrizioni contenute o richiamate nelle autorizzazioni, nonché nelle ipotesi di carenza dei requisiti e delle condizioni richiesti per le iscrizioni o comunicazioni), come previsto dall'art. 25-*undecies*, comma 6 del Decreto.

1.4. Gestione dei rifiuti (art. 256, commi 1, lett. b, 3, primo periodo, e 5 d. lgs. n. 152/2006)

L'art. 256, comma 1, del d. lgs. n. 152/2006, per quanto di interesse in questa sede (lett. b) prevede che chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti pericolosi in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214,215 e 216 è punito con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro.

Lo stesso articolo, al comma 3, prevede che chiunque, fuori dai casi sanzionati ai sensi dell'articolo 29-*quattuordecies*, comma 1, dello stesso provvedimento "*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*".

Il comma 5, infine, prevede che chiunque, in violazione del divieto di cui all'articolo 187, effettua attività non consentite di miscelazione di rifiuti, è punito con la pena suddetta, di cui al comma 1, lettera b).

Per gli illeciti in questione si applica all'Ente la sanzione pecuniaria da 150 a 250 quote (art. 25-*undecies*, comma 2, lett. b), n. 2 del Decreto). Tale sanzione è ridotta della metà nel caso previsto dall'art. 256, comma 4, d. lgs n. 152/2006 (inosservanza delle prescrizioni contenute o richiamate nelle autorizzazioni, nonché nelle ipotesi di carenza dei requisiti e delle condizioni richiesti per le iscrizioni o comunicazioni), come previsto dall'art. 25-*undecies*, comma 6, del Decreto.

1.5. Gestione dei rifiuti (art. 256, comma 3, secondo periodo, d. lgs. n. 152/2006)

La norma incriminatrice, nella parte rilevante per la responsabilità degli enti, punisce con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro la condotta di chiunque realizza o gestisce una discarica non autorizzata destinata, anche in parte, allo smaltimento di rifiuti pericolosi.

La sanzione pecuniaria carico dell'Ente è, in questo caso, da 200 a 300 quote (art. 25-*undecies*, comma 2, lett. b), n. 3 del Decreto), ridotta della metà nel caso previsto dall'art. 256, comma 4, d. lgs n. 152/2006 (inosservanza delle prescrizioni contenute o richiamate nelle autorizzazioni, nonché nelle ipotesi di carenza dei requisiti e delle condizioni richiesti per le iscrizioni o comunicazioni), come previsto dall'art. 25-*undecies*, comma 6, del Decreto.

Inoltre, in caso di condanna, è prevista l'applicazione di una delle sanzioni interdittive previste dall'art. 9, comma 2 del Decreto, per una durata non superiore a sei mesi.

1.6. Tenuta di registri e formulari (art. 258, comma 4, secondo periodo, d. lgs. n. 152/2006)

Secondo quanto disposto dalla norma in questione, si applica la pena di cui all'art. 483 del codice penale (falsità ideologica commessa dal privato in atto pubblico) 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.

Si applica all'Ente la sanzione pecuniaria da 150 a 250 quote, come previsto dall'art. 25-*undecies*, comma 2, lett. d) del Decreto.

1.7. Traffico illecito di rifiuti (art. 259, comma 1, d. lgs. n. 152/2006)

L'art. 259, comma 1 del d. lgs. n. 152/2006 prescrive che 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.

Ai sensi dell'art. 25-*undecies*, comma 2, lett. e), si applica all'Ente la sanzione pecuniaria da 150 a 250 quote.

1.8. Attività organizzate per il traffico illecito di rifiuti (al posto dell'art. 260, commi 1 e 2, D.lgs. n. 152/2006, richiamo da intendersi riferito all'articolo 452-quaterdecies del codice penale ai sensi dell'articolo 7 del decreto legislativo 1 marzo 2018 n. 21)

Ai sensi dell'art. 452 – *quaterdecies* c.p., 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.

Si applica all'Ente la sanzione pecuniaria da 300 a 500 quote (art. 25-*undecies*, comma 2, lett. f del Decreto).

Il secondo comma della stessa norma prevede l'applicazione della pena della reclusione da tre a otto anni se si tratta di rifiuti ad alta radioattività.

All'Ente si applica, in quest'ultimo caso, la sanzione pecuniaria da 400 a 800 quote (art. 25-*undecies*, comma 2, lett. f del Decreto)

In caso di condanna, è prevista l'applicazione di una delle sanzioni interdittive previste dall'art. 9, comma 2 del Decreto, per una durata non superiore a sei mesi, come prevede l'art. 25-*undecies*, comma 7, del Decreto.

Inoltre, se l'Ente o una sua unità organizzativa vengono stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione del reato di cui all'art. 260 del d. lgs. n. 152/2006 in commento, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'art. 16, comma 3 del Decreto (art. 25-*undecies*, comma 8 del Decreto).

2. Aree a rischio

L'attività svolta dalla Stone Security S.r.l. non annovera nel proprio oggetto sociale la gestione, trasporto o smaltimento dei rifiuti, se non limitatamente ai "toner" esausti delle stampanti e fotocopiatrici detenuti presso la sede nonché relativamente ai materiali di risulta dei singoli interventi presso il cliente.

In ordine allo smaltimento dei detti materiali la società si avvale della collaborazione di società abilitate allo smaltimento degli stessi. Degli interventi svolti a tal fine viene conservata traccia in forma cartacea in sede.

L'attività svolta dalla Società non comporta alcuna emissione in atmosfera.

In ragione di quanto sopra, di seguito è stata riportata la **matrice dei rischi** nella quale è espressa la correlazione tra la probabilità di verificazione del reato presupposto e l'impatto che lo stesso avrebbe per Stone Security S.r.l. .

Cod.	Reati ambientali	Amministr. unico	Direttore Amm.vo	Personale tecnico amm.vo preposto alla funzione
9	Fattispecie selezionate in premessa	Prob. 0/1 Imp. 3 Rischio: 0/3	Prob. 0/1 Imp. 3 Rischio: 0/3	

SISTEMI DI PREVENZIONE:

3. Destinatari

La presente Parte Speciale si riferisce a comportamenti posti in essere dai destinatari della società operanti nelle aree di attività a rischio, nonché da Collaboratori Esterni e *Partners*, come già definiti nella Parte Generale. La presente Parte Speciale si riferisce, infatti, a comportamenti posti in essere dai Destinatari, esponenti, collaboratori esterni, fornitori, *partner* e parti terze.

Obiettivo della presente Parte Speciale è che tutti i Destinatari si attengano, 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 di essi assume nei confronti di Stone Security S.r.l. , a regole di condotta conformi a quanto prescritto nella medesima Parte Speciale al fine di prevenire e impedire il verificarsi dei reati indicati dall'art. 25-*undecies*.

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, i destinatari sono tenuti in generale a conoscere e rispettare tutte le regole ed i principi che governano questo settore.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, gli esponenti sono tenuti a conoscere e rispettare tutte le regole ed i principi contenuti:

1. nel Codice Etico;

2. nelle attività organizzative di informazione, formazione, prevenzione in materia ambientale;

3. nelle procedure operative volte a garantire l'attuazione delle direttive in materia ambientale.

4. Principi Generali di comportamento

E' fatto espresso divieto a carico dei predetti destinatari di:

1. porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate;

2. 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;

3. utilizzare, anche occasionalmente, la società o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei Reati di cui alla presente Parte Speciale.

5. Principi di attuazione dei comportamenti prescritti

Si indicano qui di seguito i principi procedurali e le azioni che in relazione alle Aree a Rischio, i destinatari sono tenuti a realizzare e rispettare:

1. attribuzione chiara di compiti, funzioni e responsabilità in materia ambientale;
2. pianificazione delle attività di formazione a tutti i livelli in materia ambientale;
3. pianificazione ed effettuazione delle attività di verifica periodica degli impianti (di primo e secondo livello) e di manutenzione ordinaria e straordinaria degli *asset* interni, necessarie ad assicurarne la piena funzionalità e la conduzione nel rispetto della normativa ambientale;
4. pianificazione ed adozione delle azioni ed iniziative idonee a fronteggiare ed eliminare le eventuali anomalie;
5. adozione di strumenti organizzativi idonei a garantire la individuazione, valutazione e gestione delle prescrizioni derivanti dalle autorizzazioni ambientali ottenute dall'Azienda;
6. adozione di strumenti organizzativi idonei a fronteggiare le emergenze ambientali, che contemplino non soltanto le azioni tecnico gestionali, ma anche gli obblighi di comunicazione nei confronti delle Autorità;
7. adozione di strumenti organizzativi idonei a garantire il costante aggiornamento normativo anche tramite contratto quadro con azienda di consulenza;
8. selezione dei fornitori destinati a fornire i servizi di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti ed altri servizi aventi impatto ambientale (ad es. di *facility management*), siano essi *Partner* e Collaboratori Esterni, svolta con particolare attenzione (con esclusione, ad esempio, delle imprese con alta incidenza di manodopera non qualificata). L'affidabilità di tali *Partners* e dei Collaboratori Esterni deve essere valutata, ai fini della prevenzione dei Reati di cui alla presente Parte Speciale, anche attraverso specifiche indagini *ex ante,* rivolte ad esempio alla verifica dell'iscrizione agli albi trasportatori, al possesso delle necessarie autorizzazioni; la selezione dei fornitori deve essere eseguita anche sulla base della verifica dei prezzi di mercato, escludendo i fornitori che propongono prezzi inspiegabilmente bassi rispetto al mercato;
9. contrattualizzazione dei fornitori di servizi di gestione rifiuti e di altri servizi aventi impatto ambientale secondo modelli *standard* adottati tramite contratti formalizzati, che vietino il doppio livello di subappalto, prevedano la possibilità di effettuare *audit* di seconda parte e stabiliscano penali contrattuali e clausole risolutive espresse in caso di violazione della normativa ambientale

nello svolgimento del servizio; richiesta ai *Partners* e ai Collaboratori esterni dell'impegno al rispetto degli obblighi di legge in tema di gestione delle proprie attività che possono avere un impatto sulle componenti ambientali;

10. nel caso in cui si ricevano segnalazioni di violazione delle norme del Decreto da parte dei propri Esponenti e/o *Partners* e/o Collaboratori Esterni, intraprendere le iniziative più_idonee per acquisire ogni utile informazione al riguardo; in caso persistano dubbi sulla correttezza di comportamenti dei Partner e dei Collaboratori Esterni, trasmettere una segnalazione all'Organismo di Vigilanza.

L'espressa punibilità, anche della condotta di chi, nella predisposizione di un certificato di analisi di rifiuti, scarichi idrici, emissioni in atmosfera, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti, sulla concentrazione degli inquinanti negli scarichi e nelle emissioni in atmosfera e a chi fa uso di un certificato, comporta la necessità di presidiare adeguatamente anche ***l'attività di laboratorio e di analisi secondo idonee procedure*****, ancorché delegata a terzi, mediante specifiche attività di *due diligence* dei laboratori nell'ambito delle procedure di selezione dei fornitori e comunque di controllo di seconda parte**.

E' di fondamentale importanza verificare ***l'affidabilità dei fornitori e delle parti terze*** con le quali la società intrattiene rapporti di fornitura di tali servizi. Particolare attenzione dovrà essere data alla ***stipula dei contratti*** ed al puntuale ed effettivo svolgimento delle prestazioni concordate in conformità delle leggi vigenti.

Ai consulenti, *partner*, fornitori e parti terze deve essere resa nota l'adozione del Modello e del Codice Etico da parte dell'Azienda.

6. Istruzioni e Verifiche dell'O.d.V.

Devono essere immediatamente segnalati all'O.d.V. tutti i casi in cui siano riscontrate violazioni ambientali significative o comunque inosservanze rispetto al Codice etico, alla presente Parte Speciale ed ai relativi documenti di attuazione, nonché gli incidenti ambientali significativi.

L'O.d.V. deve, altresì, essere tempestivamente informato:

- di qualsiasi accertamento in corso in materia ambientale da parte delle Autorità di controllo e deve ricevere tutta la documentazione relativa al procedimento, oltre che le eventuali prescrizioni impartite e sanzioni irrogate;
- delle eventuali sanzioni disciplinari elevate per violazioni delle norme e delle procedure ambientali nel semestre di riferimento.

Devono altresì essere tempestivamente messe a disposizione dell'O.d.V. tutte le informazioni comunque richieste dall'O.d.V. medesimo ai fini dell'assolvimento dei propri compiti istituzionali.

PARTE SPECIALE IX

IMPIEGO DI CITTADINI STRANIERI IL CUI SOGGIORNO E' IRREGOLARE

QUALI FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

(Art. 25-*duodecies*)

Reato di impiego di cittadini stranieri il cui soggiorno è irregolare (art. 22, commi 12 e 12-bis, d. lgs. n. 286/1998) di cui all'art. 25-duodecies D.lgs. n. 231/2001.

1. Il reato di impiego di lavoratori stranieri il cui soggiorno è irregolare (art. 22, commi 12 e 12-bis, d. lgs. n. 286/1998) di cui all'art. 25-duodecies del Decreto

Ai sensi dell'art. 22, comma 12, del d. lgs n. 260/1998 è punito "*il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato*".

Il successivo comma 12-*bis* dell'art. 22 dispone un aumento di pena quando i lavoratori occupati siano in numero superiore a tre, ovvero siano minori in età non lavorativa, nonché qualora gli stessi siano sottoposti a condizioni lavorative di particolare sfruttamento descritte dall'art. 603-*bis* c.p.[9].

[9] Si riporta il testo dell'art. 603-*bis* c.p.: "***Intermediazione illecita e sfruttamento del lavoro***
Salvo che il fatto costituisca più grave reato, è punito con la reclusione da uno a sei anni e con la multa da 500 a 1.000 euro per ciascun lavoratore reclutato, chiunque:
1) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;
2) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.
Se i fatti sono commessi mediante violenza o minaccia, si applica la pena della reclusione da cinque a otto anni e la multa da 1.000 a 2.000 euro per ciascun lavoratore reclutato.
Ai fini del presente articolo, costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni:
1) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;

L'art. 25-*duodecies* del Decreto prevede la responsabilità della persona giuridica per il reato in esame nella sola forma aggravata di cui all'art. 22, comma 12-*bis* del D.lgs. n. 260/1998.

Ciò, ovviamente, non esime l'Azienda dall'adozione di misure e regole comportamentali idonee a prevenire il verificarsi del reato *de quo* anche nella forma c.d. ordinaria di cui al precedente comma 12 dell'art. 22.

Trattasi di reato posto a tutela della regolarità della presenza dello straniero sul territorio italiano e dei rapporti lavorativi che lo interessano.

La contravvenzione in esame assume natura di reato proprio, perché la condotta penalmente sanzionata deve essere commessa da taluno che ricopra la qualifica di "datore di lavoro".

Trattasi di reato permanente che si perfeziona al momento dell'assunzione o con l'inizio dell'attività lavorativa, si consuma per tutta la durata del rapporto di lavoro e cessa solo con il cessare di questo.

Sotto il profilo dell'elemento soggettivo, trattandosi di contravvenzione, l'agente risponde non solo a titolo di dolo ma anche a titolo di colpa, dal che deriva che sul datore di lavoro (nella specie STONE SECURITY S.R.L.) incombe, sulla base della sua ordinaria diligenza, l'onere di verificare il possesso e la validità del permesso di soggiorno del lavoratore straniero.

1.1. Trattamento sanzionatorio per le fattispecie di cui all'art. 25 duodecies del Decreto

Ove venisse accertata la responsabilità dell'Ente, sarà applicata la sanzione pecuniaria da 100 a 200 quote, comunque entro il limite di Euro 150.000.

---

2) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
3) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
4) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.
Costituiscono aggravante specifica e comportano l'aumento della pena da un terzo alla metà:
1) il fatto che il numero di lavoratori reclutati sia superiore a tre;
2) il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa;
3) l'aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

2. Aree a rischio

- **Gestione risorse umane**

Il reato di Impiego di lavoratori irregolari (art. 22, c. 12-bis, d.lgs. 286/1998) potrebbe in concreto configurarsi laddove l'Ente impiegasse alle proprie dipendenze lavoratori stranieri privi di permesso di soggiorno regolare e/o in corso di validità. A tal riguardo dovrà farsi riferimento anche a lavoratori formalmente non inquadrati come dipendenti dell'Ente, ma che potrebbero rivendicare l'accertamento e/o la costituzione del rapporto di lavoro (ad es. somministrazioni irregolari e altre ipotesi previste dalla legge).

A titolo esemplificativo ma non esaustivo si indicano ulteriori possibili modalità di commissione del reato nella realtà della società:

- impiego di lavoratori stranieri privi del permesso di soggiorno, o il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, o il cui permesso sia stato revocato o annullato;

- concorso con il datore di lavoro di un fornitore nell'impiego da parte dello stesso di lavoratori stranieri privi del permesso di soggiorno, o il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, o il cui permesso sia stato revocato o annullato;

- rapporti contrattuali con imprese che utilizzino lavoratori non qualificati e provenienti da paesi non appartenenti all'Unione Europea;

- *partnership* con imprese che operano, in maniera prevalente, presso Stati extracomunitari.

Le aree indicate assumono rilevanza anche nell'ipotesi in cui le attività sopra elencate siano eseguite, in tutto o in parte, da persone fisiche o giuridiche in nome e per conto di STONE SECURITY S.R.L. , in virtù di apposite deleghe o per la sottoscrizione di specifici rapporti contrattuali, dei quali deve essere tempestivamente informato l'O.d.V..

Di seguito è stata riportata la **matrice dei rischi** nella quale è espressa la correlazione tra la probabilità di verificazione del reato presupposto e l'impatto che lo stesso avrebbe per STONE SECURITY S.R.L. (a tal

proposito si rinvia alla nota metodologica, relativa alla mappatura dei processi e delle attività sensibili e dei rischi ad essi relativi.

Cod.	**Reato di Impiego di cittadini stranieri con soggiorno irregolare**	**Amministr. unico**	**Direttore Amm.vo**	**Personale tecnico amm.vo preposto alla funzione**
10	Fattispecie selezionate in premessa	Prob. 1 Imp. 3 Rischio: 3	Prob. 1 Imp. 3 Rischio: 3	

3. Destinatari

La presente Parte Speciale è rivolta principalmente a tutti quei soggetti che all'interno della società prendono parte ai processi di selezione e assunzione del personale dipendente di STONE SECURITY S.R.L. .

4. Protocolli preventivi

Ai fini della prevenzione del reato di Impiego di lavoratori irregolari, è fatto divieto agli apicali e ai dipendenti di assumere dei comportamenti tali da integrare la fattispecie di reato prevista dall'art. 25-*duodecies* del d.lgs. 231/01.

Oltre a ciò, è fatto espresso obbligo di:

- tenere un comportamento rispettoso con quanto stabilito dalle procedure di selezione e assunzione del personale dell'Ente;
- nell'ambito delle stesse procedure di cui al punto che precede, verificare la regolarità della documentazione dei candidati;

È fatto inoltre divieto di impiegare ed assumere alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno ovvero in possesso di soggiorno scaduto e del quale non sia stato chiesto, nelle more, il rinnovo.

Inoltre, considerata la propensione dell'Ente a favorire l'inserimento lavorativo di persone svantaggiate, giova precisare che anche in tali casi devono comunque essere rispettate le norme di legge e le procedure interne nonché i principi di cui al presente Modello.

5. Principi generali di comportamento e modalità di attuazione

Scopo della presente Parte Speciale è quello di fornire adeguati sistemi comportamentali da adottare per scongiurare la concretizzazione del rischio di commissione del reato di impiego di lavoratori stranieri irregolari, dal quale deriverebbe l'attivazione del sistema sanzionatorio previsto dal Decreto ove venisse accertata la responsabilità dell'Ente.

Tali regole di condotta si applicano a tutti i Destinatari e, in particolare, ai soggetti che svolgono le proprie mansioni nelle aree di rischio segnalate nel paragrafo 2.

La diffusione e l'attuazione di detti sistemi sono rimessi all'Amministratore unico della società, in collaborazione con l'O.d.V..

Tutti i Destinatari sono tenuti a conoscere e rispettare le regole di cui alla presente Parte Speciale, nonché:

- il Codice Etico;

- il sistema disciplinare, incluso quello previsto dal CCNL applicabile;
- le procedure interne per l'assunzione e la formazione del personale;
- il sistema afferente ai criteri utilizzati dall'Azienda per la qualificazione delle imprese con cui intrattenere rapporti di *partnership*;

É fatto espresso divieto a tutti i Destinatari e i collaboratori esterni - debitamente informati mediante apposite clausole contrattuali - di tenere condotte di qualsiasi natura che possano favorire la commissione di reati di cui alla presente Parte Speciale.

È, altresì, vietato:

- utilizzare manodopera di origine straniera senza la preventiva verifica della regolarità del permesso di soggiorno;
- assumere personale senza il rispetto della normativa contrattuale e sindacale in vigore;
- selezionare prestatori di servizi o forniture che si avvalgano di manodopera assunta mediante procedure tali da non garantire il rispetto della normativa in tema di impiego di lavoratori stranieri.

A tutti i Destinatari è imposto di segnalare tempestivamente all'Amministratore unico e all'O.d.V. qualsiasi anomalia riscontrata nella gestione delle procedure di selezione del personale e nelle procedure relative alla scelta di *partners* e fornitori.

Stone Security S.r.l. si impegna a fare sottoscrivere, al momento della conclusione del contratto, apposita dichiarazione con cui *partners* e fornitori confermino di essere a conoscenza della normativa di cui alla presente Parte Speciale.

Infine, l'Amministratore unico della società potrà prevedere ulteriori misure a maggiore tutela delle aree di rischio individuate e ad integrazione dei comportamenti sopra elencati.

PARTE SPECIALE X

1. Delitti con finalità di terrorismo o di eversione dell'ordine democratico

QUALI FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

(Art. 25- *quater*)

L'art 25-*quater* è stato introdotto nel d.lgs. 231/2001 dall'art. 3 della legge 14 gennaio 2003, n. 7.

I delitti che la norma richiama sono i "delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali", nonché dei delitti, diversi da quelli sopra indicati, "che siano comunque stati posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999".

La Convenzione di New York punisce chiunque, illegalmente e dolosamente, fornisce o raccoglie fondi sapendo che gli stessi saranno, anche parzialmente, utilizzati per compiere: (i) atti diretti a causare la morte - o gravi lesioni - di civili, quando l'azione sia finalizzata ad intimidire una popolazione, o coartare un governo o un'organizzazione internazionale; (ii) atti costituenti reato ai sensi delle convenzioni in materia di: sicurezza del volo e della navigazione, tutela del materiale nucleare, protezione di agenti diplomatici, repressione di attentati mediante uso di esplosivi.

La categoria dei "*delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali*" è menzionata dal Legislatore in modo generico, senza indicare le norme specifiche la cui violazione comporterebbe l'applicazione del presente articolo.-

Si possono, in ogni caso, individuare quali principali reati presupposto:

1.1. Art. 270-bis c.p. (Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico)

Tale norma punisce chi promuove, costituisce, organizza, dirige o finanzia associazioni che si propongono il compimento di atti violenti con finalità terroristiche od eversive.

1.2. Art. 270-ter c.p. (Assistenza agli associati)

Tale norma punisce chi dà rifugio o fornisce vitto, ospitalità, mezzi di trasporto, strumenti di comunicazione a taluna delle persona che partecipano alle associazioni con finalità terroristiche od eversive.

2. Aree a rischio

Cod.	**Reati contro la Pubblica Amministrazione**	**Amministratore**	**Delegati – procuratori speciali**
11	Fattispecie selezionate in premessa	Prob. 1 Imp. 3 Rischio: 3	Prob. 1 Imp. 3 Rischio: 3

SISTEMI DI PREVENZIONE:

3. Destinatari

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli operatori nelle aree di attività a rischio, nonché da Collaboratori Esterni e *Partners*, come già definiti nella Parte generale.

Per poter rendere efficace tale sezione, occorre che tutti i Destinatari sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che, quindi, adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

4. Protocolli preventivi

Ferma restando la specificazione operativa resa nel Manuale delle Procedure, si osserva che al fine di prevenire la commissione dei reati contro la Pubblica Amministrazione, STONE SECURITY S.R.L. si è dotata di un sistema organizzativo, formalizzato da organigramma, mansionigramma per le figure chiave, procedure dettagliate, istruzioni e regolamenti in modo tale da garantire:

- **separazione di funzioni**, all'interno di ciascun processo ritenuto sensibile, tra il soggetto che ha il potere decisionale, il soggetto che lo esegue e il soggetto che lo controlla;
- **definizione di ruoli** con particolare riferimento alle responsabilità, rappresentanza e riporto gerarchico;
- **formale conferimento di poteri**, mediante apposita delega ovvero attraverso il rilascio di una specifica procura scritta, a tutti coloro (dipendenti, membri degli organi sociali, collaboratori, consulenti, ecc.) che intrattengono per conto di STONE SECURITY S.R.L. rapporti con la Pubblica Amministrazione;
- **conoscibilità, trasparenza e pubblicità delle responsabilità** attribuite mediante apposite comunicazioni indirizzate al personale interno (ordini di servizio, circolari, ecc.) ovvero rese conoscibili ai terzi interessati, con particolare riguardo ai soggetti appartenenti alla Pubblica Amministrazione;
- **tracciabilità** di contatto personale o documentale rilevante attraverso l'utilizzo di appositi verbali dell'incontro e moduli di report, aventi adeguato livello di formalizzazione;
- **divieto di accettare omaggi o regalie**;

- previsione di specifici **meccanismi di controllo e monitoraggio**, finalizzati alla rilevazione di eventuali anomalie e/o violazioni delle procedure;
- previsione di livelli autorizzativi e **tracciabilità dei processi decisionali**.

Per quanto strettamente attiene agli **incontri con esponenti delle Pubbliche Amministrazioni** e, più in genere, i Rapporti con la Pubblica Amministrazione, STONE SECURITY S.R.L. si è dotata di una **specifica procedura** con la quale ha previsto, tra l'altro:

- **obbligo di lasciare traccia documentale delle riunioni** intercorse con i Pubblici Ufficiali e gli incaricati di pubblico servizio, contenente, tra l'altro, l'oggetto della riunione, la sede, i partecipanti, la data, l'ora di inizio e fine, indicazione di eventuali anomalie;
- regole di comportamento in occasione di detti incontri;
- partecipazione a detti incontri di almeno due esponenti della società;
- **verbalizzazione/relazione degli incontri più rilevanti**;
- ***report* periodico verso l'O.d.V. degli incontri effettuati** con esponenti della Pubblica Amministrazione
- divieto di promettere e/o offrire e/o corrispondere ai rappresentanti della Pubblica Amministrazione, anche su induzione di questi ultimi e direttamente o tramite terzi, somme di denaro o altre utilità in cambio di favori, compensi o altri vantaggi per la società;
- divieto di effettuare pagamenti o riconoscere altre utilità a collaboratori, o altri soggetti terzi che operino per conto della società, che non trovino adeguata giustificazione nel rapporto contrattuale ovvero nella prassi vigenti;
- divieto di concedere promesse di assunzione a favore di chiunque e, specificatamente, a favore di, rappresentanti della Pubblica Amministrazione, loro parenti e affini e / o soggetti segnalati;
- divieto di distribuire ai rappresentanti della Pubblica Amministrazione italiana e straniera omaggi o regali, salvo che si tratti piccoli omaggi di modico o di simbolico valore, e tali da non compromettere l'integrità e la reputazione delle parti e da non poter essere considerati finalizzati all'acquisizione impropria di benefici. Eventuali richieste esplicite o implicite di benefici da parte di un pubblico ufficiale o di un incaricato di pubblico servizio, salvo omaggi

d'uso commerciale e di modesto valore, debbono essere respinte ed immediatamente riferite al proprio superiore gerarchico;

- divieto di presentare presentare ad organismi pubblici nazionali e stranieri dichiarazioni non veritiere o prive delle informazioni dovute nell'ottenimento di finanziamenti pubblici, ed in ogni caso compiere qualsivoglia atto che possa trarre in inganno l'Ente pubblico nella concessione di erogazioni o effettuazioni di pagamenti di qualsiasi natura;
- divieto di destinare somme ricevute da organismi pubblici nazionali o stranieri a titolo di contributo, sovvenzione o finanziamento a scopi diversi da quelli cui erano destinati;
- divieto di rappresentare, agli Enti finanziatori, informazioni non veritiere e/o non complete o eludere obblighi di legge / normativi, ovvero obbligo di agire nel più assoluto rispetto della legge e delle normative eventualmente applicabili in tutte le fasi del processo, evitando di porre in essere comportamenti scorretti, a titolo esemplificativo, al fine di ottenere il superamento di vincoli o criticità relative alla concessione del finanziamento, in sede di incontro con Funzionari degli Enti finanziatori nel corso dell'istruttoria;
- divieto di ricorrere a forme di pressione, inganno, suggestione o di captazione della benevolenza del pubblico funzionario, tali da influenzare le conclusioni dell'attività amministrativa;
- divieto di omettere gli obblighi ed i presidi di controllo previsti dall'Ente in ambito della gestione dei flussi finanziari (i.e. limite impiego risorse finanziarie, procedura di firma congiunta per determinate tipologie di operazioni, espressa causale impiego di risorse, etc.), in conformità ai principi di correttezza professionale e contabile, al fine di orientare in proprio favore le decisioni in merito all'ottenimento di concessioni, licenze ed autorizzazioni dalla Pubblica Amministrazione.

Per quanto concerne poi il **processo acquisti**, l'Ente

- provvede alla qualificazione dei fornitori (affidabilità) e, in linea di principio, vengono presi in considerazione come parametri i seguenti aspetti, anche in base al Compendio generale delle informazioni documentate SGI vigente di cui la società è già dotata:

  d) Capacità di soddisfare pienamente le specifiche richieste in base ai rapporti contrattuali e alla qualità attesa;

e) Chiarezza e flessibilità nella definizione e nel rispetto dei contratti di fornitura;

f) Eventuali titoli certificativi posseduti dal fornitore o possibilità di esibire attestati di conformità e/o prove documentali di test di verifica già effettuati dallo stesso.

- La qualifica del fornitore, viene esplicitata con un giudizio sul fornitore che può risultare Qualificato, Qualificato con Riserva, Non Qualificato e solo i fornitori che hanno raggiunto la votazione minima, possono essere inseriti nell'Elenco Fornitori Qualificati, ossia costituiranno i **fornitori a cui rivolgersi in via preferenziale**;
- I contratti tra la società ed i consulenti sono definiti per iscritto in tutte le loro condizioni e termini e contengono clausole standard per il rispetto del Codice Etico, del Modello e del d.lgs. 231/2001 ed i relativi provvedimenti in caso di mancato rispetto;
- La corresponsione di onorari o compensi ai collaboratori e consulenti esterni coinvolti nell'erogazione dei servizi è soggetta ad un preventivo controllo volto a valutare la qualità e l'effettiva erogazione della prestazione e la conseguente congruità del corrispettivo richiesto, che deve essere in linea con le tariffe e/o i prezzi di mercato; non è consentito riconoscere compensi in favore dei collaboratori e consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto, che deve in ogni caso essere documentalmente provato e della documentazione comprovante l'effettivo svolgimento dell'incarico deve essere tenuta traccia a cura dell'Ente.

Inoltre Stone Security S.r.l. ha strutturato il **processo relativo agli acquisti** secondo le seguenti modalità idonee alla prevenzione di condotte delittuose:

- l'ufficio che evidenzia il bisogno o, in alternativa, la Vice Presidente o il Consigliere delegato, invia una mail alla Logistica;
- successivamente si procede alla convalida del bisogno da parte del Direttore Amministrativo;
- per i lavori e le manutenzioni si procede con la richiesta di tre o più preventivi;
- delle deliberazioni della commissione viene redatto verbale;
- all'esito, si procede alla sottoscrizione l'ordine di acquisto ed esso viene conservato in duplice copia da parte dell'ufficio acquisti;

- lo stesso ufficio acquisti procede poi alla consegna di una copia alla ragioneria, unitamente alla fattura;
- alla consegna della merce l'ufficio acquisti procede alla verifica della stessa.

5. Principi generali di comportamento e modalità di attuazione

Scopo della presente Parte Speciale è quello di fornire adeguati sistemi comportamentali da adottare per scongiurare la concretizzazione del rischio di commissione dei reati elencati dai quali deriverebbe l'attivazione del sistema sanzionatorio previsto dal Decreto, ove venisse riscontrata la responsabilità dell'Ente.

Tali regole di condotta si applicano a tutti i Destinatari del Modello ed, in particolare, a tutti coloro i quali svolgono le proprie mansioni nelle aree di rischio segnalate nei paragrafi che precedono, inclusi i soggetti esterni alla società.

La diffusione e l'attuazione di detti sistemi sono rimessi all'Amministratore unico della società, in collaborazione con l'O.d.V..

I Destinatari sono tenuti a conoscere e rispettare tutte le regole di cui alla presente Parte Speciale, nonché:

- il Codice Etico;
- il sistema disciplinare;
- le procedure interne adottate per l'assunzione e la formazione del personale nonché per contrastare la verificazione dei reati in oggetto;
- le procedure interne adottate per la gestione dei rapporti e delle comunicazioni adottando un accordo di riservatezza per la protezione e la tutela dei dati trattati nell'ambito dei contratti con clienti identificati come infrastrutture critiche;
- le pratiche conformi ed orientate al soddisfacimento dei requisiti indicati nella Direttiva europea NIs (EU 2016/1148) a tutela delle infrastrutture informatiche nazionali ed europee;
- le procedure interne adottate per la gestione dei rapporti con i fornitori.

Stone Security S.r.l. obbliga tutti i destinatari del presente Modello:

- ad osservare tutte le leggi ed il corpo di regolamenti che disciplinano le diverse attività svolte all'interno della società e ad impegnarsi, nei limiti delle rispettive competenze, ad operare affinché sia rispettato quanto previsto dalla normativa in materia;
- nel caso in cui emergano, nell'ambito del rapporto con la Pubblica Amministrazione, criticità di qualsiasi natura o conflitto di interesse deve esserne data, con nota scritta, tempestiva comunicazione all'Organismo di Vigilanza;
- a porre particolare attenzione all'attuazione e al controllo degli adempimenti richiesti e riferire immediatamente al superiore gerarchico e all'Organismo di Vigilanza eventuali situazioni di irregolarità o anomalie nel rispetto delle modalità di segnalazione prescritte;
- a rendere noti tutti i conflitti di interessi, reali o potenziali, e discuterli con la propria Area di afferenza, astenendosi dal prendere parte alle decisioni in cui tali interessi sono coinvolti.

E' fatto espresso **divieto** - per tutti i Destinatari ed i collaboratori esterni (questi ultimi debitamente istruiti con apposite clausole contrattuali) - di:

- adottare comportamenti che, in modo diretto o indiretto, possano integrare le fattispecie di reato indicate in premessa;
- assumere posizioni di palese conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dai delitti sopracitati;
- ostacolare, con violenza o minaccia, il regolare corso della giustizia.

Per quel che riguarda la prevenzione del rischio-reato connesso alla gestione dei rapporti con la Pubblica Amministrazione:

- sono state definite con apposite deleghe i soggetti abilitati alla movimentazione dei conti correnti e delle risorse finanziarie in genere, prevedendone i limiti di utilizzo;
- al fine di assicurare una gestione trasparente dei rapporti con la Pubblica Amministrazione, sono stati previsti da parte dei soggetti a ciò appositamente delegati, puntuali obblighi informativi nei confronti dell'Amministratore unico sull'andamento e sull'esito di ogni pratica in essere;
- è fatto obbligo di respingere ogni tentativo di induzione alla dazione indebita di denaro o altra utilità proveniente da un pubblico ufficiale o un incaricato di pubblico servizio; in tale evenienza,

la persona contattata deve segnalare tempestivamente l'episodio, secondo le modalità stabilite da procedure interne, sia all'amministrazione che all'Organismo di Vigilanza;

- è fatto espresso divieto influenzare o determinare le decisione dei soggetti operanti per nome e per conto della Pubblica Amministrazione con violenza, forza o inganno;
- nel caso di ispezioni da parte della Pubblica Amministrazione (ad es. forze dell'ordine), ci si dovrà far rilasciare dall'Autorità procedente una copia, da conservare presso la società, di ogni provvedimento concernente tale circostanza (ad es. decreto di ispezione, perquisizione e relativi verbali), unitamente alla documentazione del relativo procedimento;
- i fornitori devono essere selezionati in base a criteri di scelta individuati nel rispetto della legislazione regionale, nazionale e comunitaria ed in base alla loro capacità di fornire prodotti o servizi rispondenti per qualità, costo e puntualità;
- gli incarichi di consulenza esterna devono essere conferiti solo in presenza di reali esigenze della società, redatti per iscritto, contenere una descrizione chiara e precisa della prestazione da eseguire ed il relativo compenso. Prima di procedere al conferimento, gli accordi presi devono essere approvati dalla/e figura/e interna/e alla società competente e la relativa documentazione dell'incarico deve essere debitamente archiviata;
- i professionisti esterni sono tenuti ad informare la società e l'Organismo di Vigilanza circa l'esistenza di eventuali criticità riscontrate nell'espletamento dell'attività affidata, soprattutto nelle ipotesi in cui vengano individuati comportamenti che potrebbero favorire, in linea generale, la violazione del Modello e, nello specifico, il verificarsi di una delle ipotesi di reato di cui alla presente Parte Speciale.

Per quel che riguarda la prevenzione del rischio-reato di cui in premessa:

- è stata prevista la separazione di funzioni tra chi svolge le attività di gestione delle procedure informatiche, di controllo degli accessi fisici, logici e della sicurezza del *software* (ad es. responsabile dei sistemi informativi) e chi utilizza le risorse informatiche (utenti);

- è stato previsto l'accesso al sistema informatico attraverso *password* e *login* nominativi, in modo da evitare accessi non autorizzati.

6. Controlli O.d.V.

L'Organismo di Vigilanza verifica periodicamente tramite apposita programmazione degli interventi e con il supporto delle altre funzioni competenti:

- la conduzione di audit interni periodici che coinvolgano tutte le componenti organizzative;
- il mantenimento della certificazione ISO27001, il tracciamento e la corretta gestione degli incidenti informatici;
- il monitoraggio delle attività eseguite dall'azienda in qualità di amministratore di sistema;
- il **sistema di deleghe e procure** in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative, raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al delegato o vi siano altre anomalie;
- le **segnalazioni** eventualmente provenienti, attraverso i canali appositamente predisposti, da tutti coloro che operano per conto dell'Ente in relazione ad eventuali comportamenti delittuosi, quali ad esempio richiesta di indebiti vantaggi o tentativi di concussione compiuti da funzionari della PA o tentativi di corruzione da personale interno;
- i **flussi finanziari della società**, ed in particolare controlla, le riconciliazioni contabili bancarie e di cassa, le uscite di cassa ed il rispetto dei limiti dei pagamenti/incassi in contanti; controlla, inoltre la documentazione della società con particolare riferimento alle fatture passive, liberalità, donazioni e sponsorizzazioni;
- le attività connesse alle Aree a Rischio per verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello, Codice Etico (esistenza e adeguatezza della relativa procura, limiti di spesa, ***reporting*** **verso gli organi deputati**, ecc.);
- le commesse contrattualizzate, verificando a campione i contratti stipulati e le procedure utilizzate per l'acquisizione della commessa, gli eventuali collaboratori utilizzati, verificando per

questi ultimi la contrattualizzazione degli stessi, l'attività concretamente svolta dai medesimi, l'assenza di rapporti con soggetti politicamente esposti, la fatturazione e i flussi finanziari corrispondenti;

- le **procedure di selezione del personale**, anche con specifico riferimento agli inserimenti lavorativi di soggetti svantaggiati, acquisendo, anche a campione, la documentazione delle procedure di selezione suddette;
- le **consulenze affidate**, anche a professionisti esterni, avendo cura di verificare i criteri utilizzati per la scelta del professionista ed il conferimento dell'incarico, l'effettiva prestazione della consulenza, anche mediante acquisizione della relativa documentazione, la congruità del prezzo e l'insussistenza di rapporti con soggetti politicamente esposti, con rappresentanti degli enti clienti ovvero con esponenti della società.

Per lo svolgimento di tali verifiche, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione rilevante.

PARTE SPECIALE XI

DELITTI TRIBUTARI

QUALI FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

(Art. 25- *quinquiesdecies*)

1. . Delitti tributari di cui al D.lgs. 10 marzo 2000, n. 74

Con il D.L. n. 124/2019, convertito con modificazioni dalla L. n. 157/2019, il legislatore è intervenuto inserendo alcuni delitti tributari nel novero dei reati presupposto del D.Lgs. 231/01 così ampliando la responsabilità amministrativa degli enti. Tale intervento si inserisce in un contesto di implementazione che ha altresì determinato: *(i)* modifica di talune soglie di punibilità e delle cornici edittali di pena delle fattispecie delittuose di cui agli artt. 2, 3, 4, 5, 8 e 10, D.Lgs. n. 74/2000; *(ii)* introduzione, per alcuni reati tributari, della misura patrimoniale della c.d. "confisca allargata".

Le fattispecie – presupposto di cui trattasi sono ora inserite nell'art. 25-quinquiesdecies, secondo quanto segue:

"*In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, si applicano all'ente le seguenti sanzioni pecuniarie:*

a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 1, la sanzione pecuniaria fino a cinquecento quote;

b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 2, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;

c) per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote;

d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, la sanzione pecuniaria fino a cinquecento quote; e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;

f) per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote;

g) per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote.

2. Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

3. Nei casi previsti dai commi 1 e 2, si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e).".

1.1. Art. 2 – (Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti)

1. È punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.

2. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

2 -bis. Se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

1.2. Art. 3 – (Dichiarazione fraudolenta mediante altri artifici)

1. Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica 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, quando, congiuntamente:

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

b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento 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 cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

2. Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

3. Ai fini dell'applicazione della disposizione del comma 1, non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

1.3. Art. 8 - (Emissione di fatture o altri documenti per operazioni inesistenti)

1. È punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

2. Ai fini dell'applicazione della disposizione prevista dal comma 1, l'emissione o il rilascio di più fatture o documenti per operazioni

inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

2 -bis. Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

1.4. Art. 10 – (Occultamento o distruzione di documenti contabili)

1. Salvo che il fatto costituisca più grave reato, è punito con la reclusione da tre a sette anni 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.

1.5. Art. 11 – (Sottrazione fraudolenta al pagamento di imposte)

1. E' punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

2. E' punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

(1) Articolo così sostituito dall'art. 29, comma 4, D.L. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla L. 30 luglio 2010, n. 122.

2. Aree a Rischio

Cod.	Reati contro la Pubblica Amministrazione	Amministratore	Delegati – procuratori speciali
1	Fattispecie selezionate in premessa	Prob. 1 Imp. 3 Rischio: 3	Prob. 1 Imp. 3 Rischio: 3

SISTEMI DI PREVENZIONE:

3. Destinatari

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli operatori nelle aree di attività a rischio, nonché da Collaboratori Esterni e *Partners*, come già definiti nella Parte generale.

Per poter rendere efficace tale sezione, occorre che tutti i Destinatari sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che, quindi, adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

4. Protocolli preventivi

Ferma restando la specificazione operativa resa nel Manuale delle Procedure, si osserva che al fine di prevenire la commissione dei reati contro la Pubblica Amministrazione, STONE SECURITY S.R.L. si è dotata di un sistema organizzativo, formalizzato da organigramma, mansionigramma per le figure chiave, procedure dettagliate, istruzioni e regolamenti in modo tale da garantire:

- **separazione di funzioni**, all'interno di ciascun processo ritenuto sensibile, tra il soggetto che ha il potere decisionale, il soggetto che lo esegue e il soggetto che lo controlla;
- **definizione di ruoli** con particolare riferimento alle responsabilità, rappresentanza e riporto gerarchico;
- **formale conferimento di poteri**, mediante apposita delega ovvero attraverso il rilascio di una specifica procura scritta, a tutti coloro (dipendenti, membri degli organi sociali, collaboratori, consulenti, ecc.) che intrattengono per conto di STONE SECURITY S.R.L. rapporti con i fornitori;
- **conoscibilità, trasparenza e pubblicità delle responsabilità** attribuite mediante apposite comunicazioni indirizzate al personale interno (ordini di servizio, circolari, ecc.) ovvero rese conoscibili ai terzi interessati, con particolare riguardo ai soggetti fornitori;
- previsione di specifici **meccanismi di controllo e monitoraggio**, finalizzati alla rilevazione di eventuali anomalie e/o violazioni delle procedure;
- previsione di livelli autorizzativi e **tracciabilità dei processi decisionali sugli acquisti**.

Per quanto concerne poi il **processo acquisti**, l'Ente

- provvede alla qualificazione dei fornitori (affidabilità) e, in linea di principio, vengono presi in considerazione come parametri i seguenti aspetti, anche in base al Compendio generale delle informazioni documentate SGI vigente di cui la società è già dotata:

  g) Capacità di soddisfare pienamente le specifiche richieste in base ai rapporti contrattuali e alla qualità attesa;

  h) Chiarezza e flessibilità nella definizione e nel rispetto dei contratti di fornitura;

  i) Eventuali titoli certificativi posseduti dal fornitore o possibilità di esibire attestati di conformità e/o prove documentali di test di verifica già effettuati dallo stesso.

- La qualifica del fornitore, viene esplicitata con un giudizio sul fornitore che può risultare Qualificato, Qualificato con Riserva, Non Qualificato e solo i fornitori che hanno raggiunto la votazione minima, possono essere inseriti nell'Elenco Fornitori Qualificati, ossia costituiranno i **fornitori a cui rivolgersi in via preferenziale**;

- I contratti tra la società ed i consulenti sono definiti per iscritto in tutte le loro condizioni e termini e contengono clausole standard per il rispetto del Codice Etico, del Modello e del d.lgs. 231/2001 ed i relativi provvedimenti in caso di mancato rispetto;
- La corresponsione di onorari o compensi ai collaboratori e consulenti esterni coinvolti nell'erogazione dei servizi è soggetta ad un preventivo controllo volto a valutare la qualità e l'effettiva erogazione della prestazione e la conseguente congruità del corrispettivo richiesto, che deve essere in linea con le tariffe e/o i prezzi di mercato; non è consentito riconoscere compensi in favore dei collaboratori e consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto, che deve in ogni caso essere documentalmente provato e della documentazione comprovante l'effettivo svolgimento dell'incarico deve essere tenuta traccia a cura dell'Ente.

Inoltre Stone Security S.r.l. ha strutturato il **processo relativo agli acquisti** secondo le seguenti modalità idonee alla prevenzione di condotte delittuose:

- l'ufficio che evidenzia il bisogno o, in alternativa, la Vice Presidente o il Consigliere delegato, invia una mail alla Logistica;
- successivamente si procede alla convalida del bisogno da parte del Direttore Amministrativo;
- per i lavori e le manutenzioni si procede con la richiesta di tre o più preventivi;
- delle deliberazioni della commissione viene redatto verbale;
- all'esito, si procede alla sottoscrizione l'ordine di acquisto ed esso viene conservato in duplice copia da parte dell'ufficio acquisti;
- lo stesso ufficio acquisti procede poi alla consegna di una copia alla ragioneria, unitamente alla fattura;
- alla consegna della merce l'ufficio acquisti procede alla verifica della stessa.

5. Principi generali di comportamento e modalità di attuazione

Scopo della presente Parte Speciale è quello di fornire adeguati sistemi comportamentali da adottare per scongiurare la concretizzazione del rischio di commissione dei reati elencati dai quali deriverebbe l'attivazione del sistema sanzionatorio previsto dal Decreto, ove venisse riscontrata la responsabilità dell'Ente.

Tali regole di condotta si applicano a tutti i Destinatari del Modello ed, in particolare, a tutti coloro i quali svolgono le proprie mansioni nelle aree di rischio segnalate nei paragrafi che precedono, inclusi i soggetti esterni alla società.

La diffusione e l'attuazione di detti sistemi sono rimessi all'Amministratore unico della società, in collaborazione con l'O.d.V..

I Destinatari sono tenuti a conoscere e rispettare tutte le regole di cui alla presente Parte Speciale, nonché:

- il Codice Etico;
- il sistema disciplinare;
- le procedure interne adottate per l'assunzione e la formazione del personale nonché per contrastare la verificazione dei reati in oggetto;
- le procedure interne adottate per la gestione dei rapporti e delle comunicazioni con la Pubblica Amministrazione;
- le procedure interne adottate per la gestione dei rapporti con i fornitori.

Stone Security S.r.l. obbliga tutti i destinatari del presente Modello:

- ad osservare tutte le leggi ed il corpo di regolamenti che disciplinano le diverse attività svolte all'interno della società e ad impegnarsi, nei limiti delle rispettive competenze, ad operare affinché sia rispettato quanto previsto dalla normativa in materia;
- ad instaurare e mantenere rapporti con la Pubblica Amministrazione basati su criteri di massima correttezza e trasparenza;

- nel caso in cui emergano, nell'ambito del rapporto con la Pubblica Amministrazione, criticità di qualsiasi natura o conflitto di interesse deve esserne data, con nota scritta, tempestiva comunicazione all'Organismo di Vigilanza;

- a porre particolare attenzione all'attuazione e al controllo degli adempimenti richiesti dalla Pubblica Amministrazione e riferire immediatamente al superiore gerarchico e all'Organismo di Vigilanza eventuali situazioni di irregolarità o anomalie nel rispetto delle modalità di segnalazione prescritte;

- a tracciare tutti i contatti, anche attraverso annotazioni nelle relative pratiche, con i funzionari pubblici. Redigere un verbale delle riunioni intercorse con i Pubblici Ufficiali e gli incaricati di pubblico servizio, contenente, tra l'altro, l'oggetto della riunione, la sede, i partecipanti, la data, l'ora di inizio e fine. Nel caso di riunioni rilevanti per l'attività di Stone Security S.r.l. ovvero di particolari criticità ai fini del rischio *ex* d.lgs. 231/01, provvedere a trasmettere un apposito verbale all'Organismo di Vigilanza per informarlo dei fatti intercorsi; segnalare immediatamente all'O.d.V. qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione o di un incaricato di pubblico servizio o di episodi di tentativi di corruzione di cui si dovesse essere destinatario o semplicemente venirne a conoscenza; nel caso la segnalazione sia stata effettuata al Responsabile, lo stesso deve trasmettere tempestivamente la segnalazione ricevuta all'O.d.V.;

- a rendere noti tutti i conflitti di interessi, reali o potenziali, e discuterli con la propria Area di afferenza, astenendosi dal prendere parte alle decisioni in cui tali interessi sono coinvolti.

E' fatto espresso **divieto** - per tutti i Destinatari ed i collaboratori esterni (questi ultimi debitamente istruiti con apposite clausole contrattuali) - di:

- adottare comportamenti che, in modo diretto o indiretto, possano integrare le fattispecie di reato di cui agli artt. 24, 25 e 25 *decies* del Decreto;

- assumere posizioni di palese conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dai delitti sopracitati;

- ostacolare, con violenza o minaccia, il regolare corso della giustizia.

In particolare, **è assolutamente proibito**:

- emettere fatture per prestazioni non realmente erogate;

- effettuare pagamenti in contanti o in natura, fatta eccezione per procedure di piccola cassa;

- ricevere e/o erogare denaro o altra utilità - sia volontariamente che su sollecitazione, direttamente o per interposta persona - nei confronti di pubblici ufficiali o incaricati di pubblico servizio, a loro coniugi ovvero discendenti, fratelli, sorelle o a persone da loro indicate, salvo che il fatto si verifichi (in conformità con quanto previsto anche dal Codice di comportamento dei dipendenti pubblici) in occasione di festività in cui sia tradizione lo scambio di doni o, comunque, questi siano di tenue valore, o si riferisca a contribuzioni, nei limiti consentiti dalla legge, in occasione di campagne elettorali;

- distribuire e/o ricevere regali o accordare vantaggi di qualsiasi natura - di propria iniziativa o su sollecitazione - a pubblici ufficiali o incaricati di pubblico servizio che possano influenzare la terzietà o l'indipendenza di giudizio, ovvero indurre a fornire specifici vantaggi alla società;

- pagare o promettere denaro o altra utilità a seguito di una attività di induzione posta in essere da un pubblico ufficiale o un incaricato di pubblico servizio;

- assumere pubblici ufficiali ed incaricati di pubblico servizio ovvero *ex* impiegati della Pubblica Amministrazione, anche delle Comunità europee, nei due anni successivi al compimento di un atto discrezionale, di competenza di uno dei predetti soggetti, da cui sia derivato un vantaggio per la società. Il divieto sussiste anche per le ipotesi di omissione o ritardo di un atto con effetti svantaggiosi per la società;

- rilasciare promesse di assunzioni che non siano basate su criteri di merito, competenza, professionalità ma, diversamente, consistano in veri e propri favoritismi o forme clientelari privilegiate;

- attribuire compensi o prestazioni a soggetti esterni (ad es. consulenti, revisori o altri professionisti) che non trovino giustificazione in alcun tipo di incarico affidato, nonché versare compensi per prestazioni mai svolte;

- presentare dichiarazioni materialmente alterate, o dal contenuto mendace, ad organismi pubblici nazionali o appartenenti all'ordinamento comunitario, al fine di conseguire contributi o finanziamenti agevolati;

- distrarre eventuali erogazioni concesse dallo Stato, dagli Enti pubblici o dalla Comunità Europea per scopi diversi rispetto a quelli a cui erano destinati.

Per quel che riguarda la prevenzione del rischio-reato connesso alla gestione dei rapporti con la Pubblica Amministrazione:

- sono state definite con apposite deleghe i soggetti abilitati alla movimentazione dei conti correnti e delle risorse finanziarie in genere, prevedendone i limiti di utilizzo;
- al fine di assicurare una gestione trasparente dei rapporti con la Pubblica Amministrazione, sono stati previsti da parte dei soggetti a ciò appositamente delegati, puntuali obblighi informativi nei confronti dell'Amministratore unico sull'andamento e sull'esito di ogni pratica in essere;
- è fatto obbligo di respingere ogni tentativo di induzione alla dazione indebita di denaro o altra utilità proveniente da un pubblico ufficiale o un incaricato di pubblico servizio; in tale evenienza, la persona contattata deve segnalare tempestivamente l'episodio, secondo le modalità stabilite da procedure interne, sia all'amministrazione che all'Organismo di Vigilanza;
- è fatto espresso divieto influenzare o determinare le decisione dei soggetti operanti per nome e per conto della Pubblica Amministrazione con violenza, forza o inganno;
- nel caso di ispezioni da parte della Pubblica Amministrazione (ad es. forze dell'ordine), ci si dovrà far rilasciare dall'Autorità procedente una copia, da conservare presso la società, di ogni provvedimento concernente tale circostanza (ad es. decreto di ispezione, perquisizione e relativi verbali), unitamente alla documentazione del relativo procedimento;
- i fornitori devono essere selezionati in base a criteri di scelta individuati nel rispetto della legislazione regionale, nazionale e comunitaria ed in base alla loro capacità di fornire prodotti o servizi rispondenti per qualità, costo e puntualità;
- gli incarichi di consulenza esterna devono essere conferiti solo in presenza di reali esigenze della società, redatti per iscritto, contenere una descrizione chiara e precisa della prestazione da eseguire ed il relativo compenso. Prima di procedere al conferimento, gli accordi presi devono essere approvati dalla/e figura/e interna/e alla società competente e la relativa documentazione dell'incarico deve essere debitamente archiviata;
- i professionisti esterni sono tenuti ad informare la società e l'Organismo di Vigilanza circa l'esistenza di eventuali criticità riscontrate nell'espletamento dell'attività affidata, soprattutto nelle ipotesi in cui vengano individuati comportamenti che potrebbero favorire, in linea generale, la

violazione del Modello e, nello specifico, il verificarsi di una delle ipotesi di reato di cui alla presente Parte Speciale.

Per quel che riguarda la prevenzione del rischio-reato connesso alle attività di erogazione/gestione dei finanziamenti pubblici:

- sono stati previsti appositi sistemi di controllo volti a garantire la veridicità delle dichiarazioni rilasciate alla Pubblica Amministrazione, o ad organismi pubblici comunitari, anche per ottenere finanziamenti;
- si è garantita una separazione tra le attività di coloro che istruiscono e decidono delle pratiche di finanziamento e coloro che sono preposti ad attività di controllo sui pagamenti, ovvero sulla destinazione dei contributi erogati, prevedendo l'immediata segnalazione all'Organismo di Vigilanza in caso di riscontro di eventuali irregolarità.

Per quel che riguarda la prevenzione del rischio-reato di frodi informatiche:

- è stata prevista la separazione di funzioni tra chi svolge le attività di gestione delle procedure informatiche, di controllo degli accessi fisici, logici e della sicurezza del *software* (ad es. responsabile dei sistemi informativi) e chi utilizza le risorse informatiche (utenti);
- è stato previsto l'accesso al sistema informatico attraverso *password* e *login* nominativi, in modo da evitare accessi non autorizzati.

Per quel che riguarda la prevenzione del rischio-reato di induzione a rendere dichiarazioni mendaci innanzi all'Autorità giudiziaria o estera:

- ogni qual volta si abbia notizia di un procedimento penale dal quale possa derivare un coinvolgimento dell'Ente, si diffida ciascun Destinatario del Modello dal porre in essere violenza o minaccia, ovvero dal dare o promettere denaro o utilità, affinché il soggetto indagato/imputato renda dichiarazioni menzognere, o eserciti la propria facoltà di non rispondere, potendo invece esporre liberamente la propria rappresentazione dei fatti.

6. Controlli O.d.V.

L'Organismo di Vigilanza verifica periodicamente tramite apposita programmazione degli interventi e con il supporto delle altre funzioni competenti:

- il **sistema di deleghe e procure** in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative, raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al delegato o vi siano altre anomalie;
- le **segnalazioni** eventualmente provenienti, attraverso i canali appositamente predisposti, da tutti coloro che operano per conto dell'Ente in relazione ad eventuali comportamenti delittuosi, quali ad esempio richiesta di indebiti vantaggi o tentativi di concussione compiuti da funzionari della PA o tentativi di corruzione da personale interno;
- i **flussi finanziari della società**, ed in particolare controlla, le riconciliazioni contabili bancarie e di cassa, le uscite di cassa ed il rispetto dei limiti dei pagamenti/incassi in contanti; controlla, inoltre la documentazione della società con particolare riferimento alle fatture passive, liberalità, donazioni e sponsorizzazioni;
- le attività connesse alle Aree a Rischio per verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello, Codice Etico (esistenza e adeguatezza della relativa procura, limiti di spesa, ***reporting*** **verso gli organi deputati**, ecc.);
- le commesse contrattualizzate, verificando a campione i contratti stipulati e le procedure utilizzate per l'acquisizione della commessa, gli eventuali collaboratori utilizzati, verificando per questi ultimi la contrattualizzazione degli stessi, l'attività concretamente svolta dai medesimi, l'assenza di rapporti con soggetti politicamente esposti, la fatturazione e i flussi finanziari corrispondenti;
- le **procedure di selezione del personale**, anche con specifico riferimento agli inserimenti lavorativi di soggetti svantaggiati, acquisendo, anche a campione, la documentazione delle procedure di selezione suddette;
- gli **acquisti di beni o servizi**, avendo cura di verificare, anche a campione, l'effettiva prestazione del servizio o consegna del bene da parte del fornitore, la congruità del prezzo e l'insussistenza di rapporti con soggetti politicamente esposti, con rappresentanti degli enti clienti ovvero con esponenti della società;

- le **consulenze affidate**, anche a professionisti esterni, avendo cura di verificare i criteri utilizzati per la scelta del professionista ed il conferimento dell'incarico, l'effettiva prestazione della consulenza, anche mediante acquisizione della relativa documentazione, la congruità del prezzo e l'insussistenza di rapporti con soggetti politicamente esposti, con rappresentanti degli enti clienti ovvero con esponenti della società.

Per lo svolgimento di tali verifiche, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione rilevante.

PARTE SPECIALE XII

DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

QUALI FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

Il D.Lgs. 184/2021 ha dato attuazione alla Direttiva UE 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e con la sua entrata in vigore il 14 dicembre 2021 ha comportato sia modifiche al codice penale che l'introduzione del nuovo articolo 25-octies.1 nel D.Lgs. 231/01. Il nuovo articolo 25-octies.1 "Delitti in materia di strumenti di pagamento diversi dai contanti" prevede sanzioni diverse a seconda che il reato presupposto commesso sia quello previsto da art. 493-ter c.p. o art. 493-quater c.p. o art. 640-ter c.p. (per tale ultimo reato nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale) oppure, come previsto al comma 2, sia un delitto contro la fede pubblica, il patrimonio o che comunque offende il patrimonio quando ha ad oggetto strumenti di pagamento diversi dai contanti.

Il sistema delle sanzioni è invece così articolato e prevede che possano essere comminate le seguenti sanzioni: a) sanzione pecuniaria da 300 a 800 quote per il delitto di cui all'art. 493-ter; b) sanzione pecuniaria sino a 500 quote per i delitti di cui all' art. 493-quater o all'art. 640-ter sempre nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale. Per inciso giova ricordare che l'art. 640-ter risulta già essere reato presupposto con a previsione delle relative sanzioni amministrative quando alla frode informatica sia commessa se commessa ai danni dello Stato o di altro Ente pubblico.

Nell'ipotesi invece in cui il delitto commesso sia un reato contro la fede pubblica o il patrimonio o che comunque offende il patrimonio può essere ravvisata una responsabilità in capo all'ente solo qualora il fatto non integri un altro illecito amministrativo sanzionato più gravemente. Le sanzioni amministrative previste in questo possono essere la sanzione pecuniaria fino a 500 quote, se il delitto è punito con la pena della reclusione inferiore a dieci anni; e la sanzione pecuniaria da 300 a 800 quote, se il delitto è punito con la pena della reclusione non inferiore a dieci anni.

Per tutte le fattispecie di reato presupposto in caso di condanna si applicano le sanzioni interdittive previste dall'art. 9, co. 2 D.Lgs. 231/01.

Art. 493-* ter *c.p. "Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti"

"Chiunque 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 è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace 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".

In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è ordinata la confisca delle cose che servirono o furono destinate a commettere il reato, nonchè del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.

Gli strumenti sequestrati ai fini della confisca di cui al secondo comma, nel corso delle operazioni di polizia giudiziaria, sono affidati dall'autorità giudiziaria agli organi di polizia che ne facciano richiesta."

Art. 493-quater "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti"

"Salvo che il fatto costituisca più grave reato, 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 sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo, è punito con la reclusione sino a due anni e la multa sino a 1000 euro.

In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è sempre ordinata la confisca delle apparecchiature, dei dispositivi o dei programmi informatici predetti, nonché la confisca del profitto o del prodotto del reato ovvero, quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto."

Art. 640-ter "Frode informatica"

Sebbene già previsto pur in termini parziali e nella versione prescrittrice antecedente alla modifica del D.Lgs. 184/2021, era già presupposta dall'art. 24. punisce "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, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni.

La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 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 taluna delle circostanze previste dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età, e numero 7."

Delitti in materia di strumenti di pagamento diversi dai contanti

Per quanto concerne la presente Parte Speciale, si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati.

Le frodi e le falsificazioni dei mezzi di pagamento diversi dai contanti hanno assunto una notevole dimensione transfrontaliera, accentuata dalla loro natura sempre più digitale, donde la necessità degli Stati membri di garantire un approccio coerente, facilitare lo scambio di informazioni e la cooperazione tra autorità competenti.

Si tratta di reati in parte connotati dall'uso illegittimo degli strumenti finalizzati al pagamento diversi dai contanti.

Quanto alle locuzioni è importante sottolineare come debba intendersi per «**strumento di pagamento diverso dai contanti**» (un dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali) ; per «**dispositivo, oggetto o record protetto**» (un dispositivo oggetto o record protetto contro le imitazioni o l'utilizzazione fraudolenta, per esempio mediante disegno, codice o firma) «mezzo di scambio digitale» (qualsiasi moneta elettronica definita all'articolo 1, comma 2, lettera h-ter, del decreto legislativo 1° settembre 1993, n. 385, e la valuta virtuale); per **«valuta virtuale**» (una rappresentazione di valore digitale che non e' emessa o garantita da una banca centrale o da un ente pubblico, non e' legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma e' accettata da persone fisiche o giuridiche come mezzo di scambio, e che puo' essere trasferita, memorizzata e scambiata elettronicamente.

Aree a rischio

Il rischio di commissione dei reati in materia di strumenti di pagamento diversi dai contanti è particolarmente rilevante per la natura delle attività poste in essere dall'Azienda.

In considerazione della *ratio* normativa, i processi che presentano una sensibilità diretta ai rischi di reato sono tutti quelli che presuppongono l'utilizzo di una rete di dispositivi per i pagamenti diversi dalla

moneta corrente, dunque, tenuto conto delle attività svolte da STONE SECURITY S.R.L. , **specialmente i processi legati ai pagamenti effettuati possono essere esposti a tale rischio di reato.**

In particolare, con riferimento a tutti i processi di gestione dei singoli pagamenti, risulta particolarmente sensibile l'attività di verifica e bonifica dell'utilizzo degli strumenti finalizzati al pagamento diversi dai contanti. Questi, tuttavia, sono abilitati solo per soggetti all'uopo individuati.

Pertanto, tali reati potrebbero realizzarsi nell'ambito del più ampio processo relativo alla gestione dei pagamenti nel caso, ad esempio, in cui non siano previste o attivate le misure minime di accesso in sicurezza e profilazione utente per gli accessi ai diversi programmi e *database* gestiti dall'Ente finalizzato al pagamento, con conseguente possibile manipolazione o alterazione illegittima sugli stessi dati, informazioni e programmi con l'obiettivo di conseguire un profitto per sé o per altri.

I reati in esame possono essere commessi da soggetti con significativa dimestichezza informatica o da coloro che fraudolentemente o mediante un accesso pregresso al dispositivo previsto per il pagamento.

I processi ritenuti maggiormente sensibili per tale fattispecie delittuosa sono i seguenti:

- Gestione delle risorse economiche e finanziarie;
- Gestione risorse umane.

A titolo esemplificativo si indicano possibili modalità di commissione del reato nella realtà dell'Ente:

- indebito utilizzo (non essendone titolare) di 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;

- accesso abusivo ai sistemi che elaborano e gestiscono i pagamenti;

- accesso abusivo ai sistemi che realizzano i pagamenti per alterare le informazioni o la destinazione al fine di realizzare un profitto illecito.

- accesso o alterazione di apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati in materia si strumenti di pagamento diversi dai contanti;

Di seguito è stata riportata la **matrice dei rischi** nella quale è espressa la correlazione tra la probabilità di verificazione del reato presupposto e l'impatto che lo stesso avrebbe per STONE SECURITY S.R.L. (a tal proposito si rinvia alla nota metodologica, relativa alla mappatura dei processi e delle attività sensibili e dei rischi ad essi relativi, di cui al paragrafo 10 della Parte generale del presente Modello.

Cod.	Reati in materia si strumenti di pagamento diversi dai contanti	**Amministr. unico**	**Direttore Amm.vo - Commerciale**	**Personale tecnico amm.vo preposto alla funzione amministrativa**
4	Fattispecie selezionate in premessa	Prob. 1 Imp. 3 Rischio: 3	Prob. 1 Imp. 3 Rischio: 3	

SISTEMI DI PREVENZIONE:

Destinatari

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli operanti nelle aree di attività a rischio, come già definiti nella Parte generale.

Per poter rendere efficace tale sezione, occorre che tutti i Destinatari sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che adottino, pertanto, regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

1 Protocolli preventivi

Al fine di prevenire il presentarsi delle fattispecie delittuose sopra menzionate, STONE SECURITY S.R.L. si è dotata di specifici Procedure preventive:

- la distribuzione dei compiti e delle responsabilità nell'ambito dei soggetti preposti alla gestione dei pagamenti;
- l'analisi dei rischi che incombono sui dispositivi abilitanti ai pagamenti;
- la definizione delle misure da adottare per garantire la sicurezza delle apparecchiature, dispositivi o programmi informatici finalizzati al pagamento nonché l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la previsione di interventi formativi degli autorizzati alle diverse procedure di pagamento;
- la definizione di un procedimento di autenticazione degli utenti mediante *username* e *password* o la conservazione e l'utilizzo delle stesse a cui corrisponde un accesso limitato in relazione a compiti e responsabilità ricoperte all'interno dell'Ente;
- la disattivazione, al momento delle dimissioni/licenziamento dell'utente, di ogni apparecchiatura, dispositivo o credenziali di accesso a programmi informatici finalizzati al pagamento;
- accesso alla rete informatica della società, per la consultazione e l'elaborazione di dati, documenti e informazioni da comunicare o ricevuti dalla Pubblica Amministrazione, ovvero per qualunque intervento sui programmi destinati ad elaborarli, avviene attraverso l'utilizzo di ***id*** **e** ***password*** **personali**;
- protezione **del *server* e dei dati attraverso l'utilizzo di sistemi anti-intrusione, di *software* antivirus costantemente aggiornati ed attività di *back up*;**
- limitazioni **agli accessi alla rete informatica dall'esterno**, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei destinatari;
- limitare l'accesso a apparecchiature, dispositivi o programmi informatici finalizzati al pagamento ai soli soggetti abilitati alla funzione;
- impostazione dei sistemi informatici stessi in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
- limitare l'accesso alle aree ed ai siti internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti capaci di danneggiare o distruggere sistemi

informatici o dati in questi contenuti; predisposizione ed aggiornamento annuale del Documento Programmatico di Sicurezza (DPS), nel quale sono analizzate le situazioni ed organizzate procedure per la garanzia della sicurezza nei trattamenti dei dati.

2 Principi generali di comportamento

STONE SECURITY S.R.L. prescrive una serie di regole comportamentali, di seguito indicate, che devono essere obbligatoriamente seguite dai propri dipendenti, collaboratori, consulenti, membri degli organi sociali e di controllo nonché da soggetti terzi con cui intrattiene relazioni.

È anzitutto fatto obbligo di

- rispettare le leggi e i regolamenti applicabili alla materia della protezione e sicurezza dei dati personali e dei sistemi informatici (Reg. UE 2016/679 e Codice della Privacy così come modificato dal D.lgs n°101/2018), unitamente alle Policy di sicurezza informatica definita all'interno del sistema di gestione aziendale;
- non divulgare informazioni relative ai sistemi informatici e di pagamento dell'Ente;
- utilizzare le informazioni, i programmi e le apparecchiature aziendali esclusivamente per motivi di ufficio o connessi all'attività lavorativa;
- non prestare o cedere a terzi apparecchiature informatiche o carte di credito finalizzate al pagamento senza la preventiva autorizzazione da parte dell'Amministratore; in caso di smarrimento o furto, informare tempestivamente l'Amministratore e presentare denuncia presso l'Autorità Giudiziaria preposta;
- garantire ed agevolare ogni forma di controllo interno e di supervisione sulla adozione delle misure di sicurezza implementate;
- adottare misure di sicurezza, organizzative, fisiche e logistiche per il trattamento dei dati personali;
- in mancanza di specifica autorizzazione, astenersi dall'effettuare copie di dati e di software.

È fatto divieto di:

- rappresentare, alle autorità pubbliche e agli organismi di vigilanza, situazioni non veritiere o comunicare dati falsi, lacunosi o, comunque, non rispondenti alla realtà, per influenzarle indebitamente;

- modificare in qualunque modo la configurazione delle postazioni di lavoro fisse o mobili assegnate, installando o utilizzando *software* e *hardware* non approvati dall'Ente e non correlati con l'attività professionale ricoperta;
- acquisire, possedere o utilizzare strumenti *software* e/o *hardware* che potrebbero essere adoperati per compromettere la sicurezza dei sistemi informatici o telematici anche finalizzati al pagamento (sistemi per individuare le password, decifrare i file criptati, intercettare il traffico in transito, ecc.), a meno che non sia esplicitamente contemplato nei propri compiti lavorativi;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o *software* allo scopo di danneggiare il sistema informatico o telematico di soggetti, pubblici o privati, al fine di danneggiare le informazioni, i dati o i programmi in esso contenuti oppure di favorire l'interruzione totale o parziale o l'interruzione del suo funzionamento;
- ottenere abusivamente credenziali di accesso e di utilizzo di strumenti finalizzati al pagamento diversi dai contanti, al fine di ottenere un profitto o un vantaggio per sé o per altri;
- divulgare, cedere o condividere con personale interno o esterno all'Ente le credenziali di accesso ai sistemi e alla rete, anche di clienti o di terze parti;
- accedere abusivamente al sistema al fine di alterare e/o cancellare dati e/o informazioni o ottenere o modificare dati di pagamento;
- effettuare prove o tentare di compromettere i controlli di sicurezza di strumenti finalizzati al pagamento diversi dai contanti dell'Ente;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dell'Ente, di clienti o di terze parti;
- distorcere, oscurare, sostituire la propria identità e inviare e-mail riportanti false generalità;
- installare nella rete di ateneo un *software* che possa impedire, interrompere o danneggiare le comunicazioni all'interno dell'Ente o verso l'esterno o che possa rallentare o bloccare l'intera rete informatica;
- installare nella rete aziendale o sui singoli pc, ovvero utilizzare, duplicare un software in violazione della normativa sul diritto d'autore.

Sono indicate nel prosieguo anche procedure generali di verifica degli accessi, di visibilità e modificabilità dei dati, nonché di conservazione dei medesimi.

- l'uso dei *computers* disponibili nella rete della società o di strumenti finalizzati al pagamento diversi dai contanti è concesso previa autorizzazione dell'amministratore o del personale preposto e solo per fondati motivi di lavoro;
- l'utilizzo di ogni elaboratore (di seguito PC) è riservato e protetto da *password*;
- ogni PC deve disporre di *username* e *password* (che il sistema informatico impone di modificare periodicamente).
- l'accesso ai programmi di contabilità, gestione ed amministrazione della società è concesso, secondo le necessità e con diverse autorizzazioni a seconda della funzione.
- l'utilizzo di *internet* è parimenti strettamente regolamentato.
- il personale non ha accesso alla rete se non previa autorizzazione del proprio diretto superiore gerarchico concessa solo per comprovate ragioni lavorative.

Ogni violazione delle procedure interne enucleate ed *enucleande* per l'utilizzo di strumenti finalizzati al pagamento diversi dai contanti deve essere tempestivamente comunicata all'Organismo di Vigilanza.

3.Principi di attuazione dei comportamenti prescritti

3.1 Modalità di accesso ai singoli strumenti finalizzati al pagamento diversi dai contanti

Ogni singolo strumento prevede che l'utente utilizzi codici e password. Pertanto l'utente abilitato al pagamento deve procedere all'autenticazione ogni volta che si richiede l'accesso al dispositivo stesso.

Le *password* sono personalizzate e non devono essere mai cedute a nessun altro soggetto.

A ciascun utente sono stati forniti i relativi privilegi di accesso a seconda della mansione/attività strumento predisposto per il pagamento.

È fatto divieto di divulgare, cedere o condividere con personale interno o esterno alla società le credenziali di accesso e di utilizzo dei sistemi.

In caso di assenze del titolare, deve essere regolamentato il passaggio di consegne in ordine ad eventuali scadenze di legge aventi ad oggetto adempimenti o pagamenti telematici, con previsione delle modalità per la sostituzione.

3.2Modalità di utilizzo delle carte di credito /carte di credito ricaricabili

I dipendenti hanno la possibilità di utilizzare carte di credito o carte ricaricabili dell'Ente, solo se previamente autorizzato dall'Amministratore e per esigenze lavorative. L'utilizzo è circoscritto ad un arco di tempo predeterminato e per specifiche attività.

3.3 Controlli O.d.V.

In riferimento ai reati in esame, l'O.d.V. ha il compito di monitorare il rispetto degli obblighi e dei divieti impartiti al personale interno effettuando verifiche periodiche, anche a campione:

- sulla gestione dei profili autorizzativi degli strumenti finalizzati al pagamento diversi dai contanti
    - sul rispetto delle politiche di autenticazione in ordine all'accesso ai dispositibi abilitati al pagamento;
    - L'O.d.V. condurrà quindi controlli a campione diretti a verificare le procedure/istruzioni interne ed i Procedure contenuti nel presente Modello nonché l'adeguatezza delle prescrizioni a prevenire i rischi di reato potenziali.

Stonesecurity s.r.l.

Font: Garamond, 12

Interlinea: 1,5

Paragrafo: prima=0, dopo=6 (non aggiungere)

stile: giustificato