

## II PARTE SPECIALE

## SEZIONE A) - REATI CONTRO LA P.A.

Il Decreto, agli artt. 24 e 25, prevede i possibili reati, disciplinati dal Codice Penale, che possono compiersi nei confronti e ai danni del patrimonio, dell'imparzialità e del buon andamento della Pubblica Amministrazione. In relazione all'attività svolta dalla Società Cooperativa Fraternità Sistemi (di seguito FS) ed ai rischi nella quale potrebbe incorrere, sono stati ritenuti potenzialmente inerenti per la Società le seguenti fattispecie di reato:

- Concussione (art. 317 c.p.)
- Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318 - 319 c.p.)
- Corruzione in atti giudiziari (art. 319-ter c.p.)
- Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)
- Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)
- Istigazione alla corruzione (art. 322 c.p.)
- Concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.)
- Malversazione a danno dello Stato (art. 316 bis c.p.)
- Indebita percezione di erogazioni a danno dello Stato (art. 316 ter c.p.)
- Truffa in danno allo Stato, di altro ente pubblico o dell'Unione Europea (art. 640, comma 2, n. 1 c.p.)
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.)
- Frode informatica, se il fatto è commesso in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)

L'elemento che caratterizza tale gruppo di fattispecie di reato in esame è l'esistenza di continui rapporti fra la Società e qualsiasi Ente della Pubblica Amministrazione che, nello specifico, si configura prevalentemente nei diversi comuni nei quali la Società opera l'attività di riscossione dei tributi. Deve inoltre segnalarsi che, ai sensi dell'art. 321 c.p., le pene previste dagli artt. 318, 319, 319-bis, 319-ter e 320 sono applicabili anche al soggetto che dà o promette denaro o altra utilità.

In particolare, per la natura stessa dell'attività svolta, la Società FS ha frequenti rapporti con pubblici ufficiali o incaricati di pubblico servizio, ad esempio:

- partecipazione a gare** per concessioni di servizi e/o finanziamenti pubblici;
- gestione dei servizi** erogati (accertamenti, liquidazione, notifica atti, ecc).
- visite ispettive di enti di controllo** (ASL, INAIL, INPS, GdF, Ministero, etc.);
- rendicontazione delle entrate e riversamenti** legati ai singoli tributi gestiti;

A titolo esemplificativo, i Pubblici ufficiali o gli incaricati di pubblico servizio che possono intrattenere rapporti con la Società, nell'ambito delle normali attività da questo svolte, sono: Funzionari Comunali, Provinciali o Regionali, Polizia Municipale, Funzionari dell'ASL, dell'INAIL, dell'INPS, della Guardia di Finanza, dell'Agenzia delle Entrate, Ministero, ecc.

Deve inoltre aggiungersi che il personale stesso della Società, in occasione dello svolgimento di particolari funzioni derivanti dai contratti di servizio stipulati con i Comuni, può trovarsi a svolgere funzioni di incaricato di pubblico servizio, così rivestendo la qualifica funzionale prevista dal Codice Penale per il soggetto attivo delle fattispecie di reato proprio, in esame in questa sezione.

## 1. Elenco delle fattispecie di reato ipotizzabili per processo sensibile

In relazione all'attività svolta dalla Società, si illustrano sinteticamente di seguito le potenziali fattispecie di reato previste dagli artt. 24 e 25 che potrebbero astrattamente verificarsi nell'ambito dei processi ritenuti sensibili e che presentano un livello di rischio critico o rilevante.

Il reato di Concussione (art. 317 c.p.) e di Induzione indebita a dare o promettere utilità (art. 319-quater) potrebbero realizzarsi, ad esempio, in caso di abuso di potere da parte di pubblico ufficiale o incaricato di pubblico servizio che costringa o induca esponenti della Società (dipendenti e non) a dare o promettere denaro o altre utilità (assunzione di un dipendente, stipula di un contratto di consulenza, scelta di un fornitore, ecc...) al fine di:

- agevolare la Società nell'ottenimento di contratti di servizi con enti pubblici, ovvero in relazione alle condizioni contrattuali ivi previste;
- ottenere agevolazioni per l'aggiudicazione di gare pubbliche ovvero di finanziamenti pubblici;
- procurare alla Società trattamenti di favore in caso di accertamento e/o verifiche ispettive da parte delle autorità competenti;
- ottenere un trattamento favorevole in caso di accertamento in materia di sicurezza lavoro, ambiente ovvero in materia di lavoro, fiscale, previdenziale o contributiva, ecc.

Al riguardo deve precisarsi che nei suddetti casi mentre per l'induzione indebita a dare o promettere utilità è prevista la punibilità, ai sensi dell'art. 319 quater, ult. co., c.p. anche del soggetto che dà o promette denaro o altra utilità, nel caso di concussione, invece, non essendo prevista la punibilità del soggetto passivo del reato costretto a dare o promettere utilità, potrebbe ipotizzarsi la responsabilità in capo all'Ente solo nel caso limite e di probabilità residuale in cui l'esponente aziendale avesse agito in concorso di persone nel reato con il soggetto attivo e lo avesse fatto con un connesso o correlato interesse o vantaggio dell'Ente.

I suddetti reati potrebbero inoltre realizzarsi in astratto anche avendo quale soggetto attivo il personale della Fraternalità Sistemi, che rivesta nel caso la qualifica di incaricato di pubblico servizio, e ciò a titolo esemplificativo e in astratto, ove detto personale ponesse in essere condotte che costringano o inducano i contribuenti a dare o promettere denaro o altra utilità a fronte dell'omissione di atti dovuti ovvero di un trattamento più favorevole per esempio in fase di accertamento, ovvero in fase di annullamento o rettifica. In tal caso risulterà comunque necessario, ai fini della configurabilità della rilevanza della condotta nella prospettiva di cui al d.lgs. 231/01, la rigorosa distinzione tra i casi in cui l'azione o l'omissione in questione abbia avuto luogo nell'interesse o a vantaggio dell'Ente (con conseguente responsabilità ex d.lgs. 231 del medesimo) e i diversi casi in cui il dipendente abbia semplicemente agito nell'esclusivo interesse o vantaggio proprio (come potrebbe avvenire con maggior grado di probabilità) connotandosi come dipendente infedele e agendo pertanto in danno dell'Ente.

I reati di Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318-319 c.p.), Corruzione di persona incaricata di un pubblico servizio (art.320 c.p.) e Istigazione alla corruzione (art. 322 c.p.) potrebbero realizzarsi, ad esempio, in caso di offerta o promessa di denaro o altre utilità da parte di esponenti della Società (dipendenti e non) a pubblici ufficiali o incaricati di pubblico servizio al fine di agevolare e far ottenere alla Società, a titolo esemplificativo, i vantaggi di cui sopra.

Anche in tal caso, gli esponenti aziendali possono porre in essere la fattispecie di reato in esame tanto come corruttori (secondo l'esemplificazione sopra riportata) che come corrotti ove, rivestendo la qualifica di incaricato di pubblico servizio nell'espletamento delle funzioni derivanti dai contratti di servizio stipulati con i Comuni, accettino offerta o promessa di denaro o di altra utilità dai contribuenti per far porre in essere un atto del proprio ufficio o un atto contrario ai doveri d'ufficio. 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.

Il reato di Corruzione in atti giudiziari (art. 319 ter) si potrebbe configurare nel caso in cui la Società 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).

Il reato di Malversazione a danno dello Stato o dell'Unione Europea (art. 316-bis c.p.) 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. formazione) e di impiego degli stessi su altri investimenti e/o attività per le quali la Società nutre interesse.

I reati di Indebita percezione di contributi in danno dello Stato o dell'Unione Europea (art. 316-ter c.p.) e Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.) potrebbero realizzarsi, ad esempio, in caso di alterazione da parte del personale di FS 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 la Società.

Il reato di Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea (art. 640, comma 2 n. 1, c.p.) potrebbe realizzarsi, ad esempio, nel caso in cui, per ottenere da un qualsivoglia Comune un maggiore aggio sul riscosso, vengano gonfiati gli accertamenti ovvero vengano inseriti nell'archivio informatico verbali di contravvenzioni inesistenti, mai emessi dalla Polizia Locale, ovvero comunque simulate o rappresentate attività (istruttoria, notifica, ecc...) non poste in essere;

Per quanto riguarda il reato di Concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.), la norma in esame prevede l'applicabilità dei reati ivi previsti (e più precisamente sopra descritti), estendendola ai soggetti citati nella fattispecie stessa.

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

- reclutamento, selezione e gestione del personale;
- rapporti con la pubblica amministrazione;
- Gestione degli adempimenti necessari per l'ottenimento o il rinnovo di autorizzazioni, licenze e/o concessioni da parte della Pubblica Amministrazione (per es. iscrizione all'Albo dei riscossori), nonché per l'emissione di altri provvedimenti occasionali da parte della medesima;
- Effettuazione di adempimenti obbligatori nei confronti della Pubblica Amministrazione o delle Autorità Pubbliche di vigilanza e la gestione dei rapporti con le stesse in occasione di verifiche e controlli;
- contratti pubblici, ivi compresi gli affidamenti di incarichi;
- annullamenti e rettifiche atti di riscossione;
- gestione del contenzioso nelle varie sedi di interesse per la Società;
- ICT e trattamento dati personali dei contribuenti (tutela della riservatezza);
- area economico finanziaria;
- Selezione e gestione rapporti con consulenti e fornitori;
- Gestione Acquisti, Ordini di pagamento e Cassa;

Da specificare che le provviste per la commissione dei reati di corruzione nell'interesse o a vantaggio della società possono, ad esempio, generarsi con la fatturazione di operazioni inesistenti oppure mediante spese di rappresentanza, sponsorizzazione, omaggi e regalie ovvero tramite la voce di rimborsi spese fittizie.

## 2. Protocolli preventivi adottati

Al fine di mitigare e prevenire la commissione dei reati contro la PA, la Società FS 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 della Società FS rapporti con la P.A.;  
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 ciascun passaggio rilevante attraverso l'utilizzo di appositi moduli, aventi adeguato livello di formalizzazione;  
divieto di accettare omaggi o regalie, eccedenti i 100 €  
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;

Oltre a ciò, per quanto strettamente attiene agli incontri con esponenti delle Pubbliche Amministrazioni, la Società FS e più in genere i **Rapporti P.A.**, la Società 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'ODV degli incontri effettuati con esponenti della PA.

Per quanto concerne poi il **processo di selezione e gestione rapporti con consulenti e fornitori**, la Società si è dotata di specifiche procedure che prevedono i seguenti protocolli preventivi:

- a. Applicazione dei principi di proporzionalità, trasparenza, parità di trattamento e rotazione dell'attività negoziale della Società;
- b. Istituzione Albo Fornitori che risponda ai criteri di cui al capo che precede, e definizione dei requisiti essenziali da possedere per l'iscrizione allo stesso, sia nei casi di forniture e servizi che di lavori;
- c. Pubblicazione della procedura in oggetto e dell'Albo Fornitori sul sito web della Società con facoltà per l'operatore economico di presentare domanda di iscrizione in qualunque momento;
- d. Revisione periodica, almeno annuale e mediante verifiche a campione, dei requisiti dichiarati dagli iscritti all'Albo;
- e. Pubblicazione, con cadenza almeno annuale e mediante apposito avviso reso noto con le modalità idonee ad assicurarne l'adeguata pubblicità, dell'apertura delle iscrizioni nell'Albo;

- f. Agli Operatori Economici ritenuti idonei, viene fornita la comunicazione di avvenuta iscrizione nell'albo così come, in caso di non idoneità, viene comunicato il rigetto dell'iscrizione con evidenza della relativa motivazione;
- g. Standardizzazione della modulistica contrattuale relativa all'incarico, con espressa clausola di adesione al Modello di Organizzazione Gestione e Controllo ex D.Lgs. 231/01 e al Codice Etico di Fraternalità Sistemi, ed espressa previsione di sanzioni per le violazioni fino alla risoluzione del contratto;
- h. Somministrazione di un modulo al conferimento degli incarichi al fine di avere una mappatura degli interessi del soggetto incaricato, della sussistenza/insussistenza di rapporti di parentela/affinità con soggetti politicamente esposti, o con vertici apicali di stazioni appaltanti, o anche soggetti riconducibili alla committenza, nonché una dichiarazione circa gli incarichi ricoperti dagli stessi presso altri enti pubblici;
- i. Applicazione del criterio di rotazione degli operatori economici da invitare alle procedure di selezione, sulla base dell'ordine progressivo di iscrizione, tenendo conto delle eventuali fasce di importo in cui gli operatori sono stati iscritti; è comunque facoltà della Società invitare l'ultimo operatore affidatario di analogo affidamento;
- j. Comunicazione scritta all'Operatore Economico in caso di avvio della procedura di cancellazione dall'Albo, comunicando altresì i fatti addebitati, assegnando un termine di 15 giorni lavorativi per eventuali controdeduzioni e ferma restando la possibilità di ripresentazione della domanda di iscrizione in caso di comprovata riacquisizione dei requisiti;
- k. A conclusione dell'incarico e/o a prodotto consegnato/servizio reso, FS provvede alla qualificazione dei fornitori (affidabilità) e, in linea di principio, vengono presi in considerazione come parametri i seguenti aspetti:
  - Capacità di soddisfare pienamente le specifiche richieste in base ai rapporti contrattuali e alla qualità attesa;
  - Chiarezza e flessibilità nella definizione e nel rispetto dei contratti di fornitura;
  - 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.
- l. 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;
- m. 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;
- n. 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 della Società.;

Per quanto concerne il **processo di relativo agli acquisti** la Società si è dotata di specifiche procedure, prevedendo, tra l'altro, i seguenti protocolli preventivi:

- a. istituzione di un Albo dei Fornitori, suddiviso per categorie merceologiche, aperto o soggetto a revisione con periodicità non superiore a quella annuale, da cui attingere per le richieste di preventivo e le ricerche di mercato;
- b. Definizione di soglie autorizzative per gli acquisti, differenziate in ragione dell'importo della spesa:

1. Fino ad euro 500,00 delibera la spesa il C.D. o altro soggetto munito di apposita procura, previa ricerca di mercato semplificata da parte dell'Ufficio Acquisti;
  2. Oltre euro 500,00 e fino ad euro 20.000,00 delibera la spesa il C.D. previa valutazione comparativa di almeno 3 offerte, listini o preventivi raccolti dall'Ufficio acquisti, scelti tra i soggetti iscritti all'albo dei fornitori, se prevista la corrispondente categoria merceologica, ovvero anche tra soggetti esterni se non disponibili operatori economici in tale numero minimo all'interno dell'albo.
  3. Delibera l'impegno di spesa il CdA su proposta di almeno un consigliere e procede alla valutazione dei preventivi raccolti dall'ufficio acquisti secondo le modalità di cui al punto che precede, eventualmente delegando il C.D. o altro Consigliere alla successiva formalizzazione dell'acquisto;
- c. La scelta del contraente deve avvenire sempre secondo criteri di economicità e/o con riferimento al rapporto qualità/prezzo, ma in ogni caso tale valutazione deve essere motivata e deve esserne tenuta traccia scritta;
  - d. Il pagamento delle fatture avviene da parte dell'Ufficio Contabilità, previa verifica della congruità ed integrità della documentazione e del rispetto delle procedure;
  - e. L'Ufficio contabilità garantisce la conservazione documentale e la tracciabilità dei pagamenti;
  - f. In ogni caso si procede alla valutazione delle rilevazioni dei prezzi di mercato effettuate da amministrazioni o enti a ciò preposti al fine di valutare la congruità dei prezzi presentati in sede di offerta per l'esecuzione dei servizi e l'acquisizione di beni e servizi;
  - g. Periodicamente, e comunque con cadenza almeno annuale, di concerto con il Collegio dei Sindaci, il C.D. predispose il consuntivo degli acquisti e delle consulenze aventi importo maggiore ad euro 10.000,00, IVA esclusa;

Per quanto concerne il processo di **Gestione dei diversi servizi**, la Società si è dotata di specifiche procedure, di seguito elencate:

- PG gestione atti di accertamento in regime di concessione;
- PG adesione atto di accertamento;
- PG insediamento in nuovo comune per attività tributi maggiori;
- PG gestione integrale processo di accertamento ICI/IMU;
- PG Perequazione catastale;
- PG Stime mobiliari, immobiliare e aree;
- PG Insedimento in nuovo comune per l'attività di segnalazioni qualificate compartecipazione Agenzia delle Entrate;
- PG protezione informazioni e segnalazione qualificate agenzia delle entrate;
- PG insediamento in nuovo comune a supporto della gestione delle contravvenzioni e riscossione spontanea e coattiva delle stesse;
- PG avviamento della gestione del servizio di riscossione ed accertamento DPA/ICP/CIMP/TOSAP/COSAP;
- insediamento in un nuovo comune per gestione servizio parcheggi a pagamento senza custodia.

che, nello specifico, prevedono i seguenti protocolli preventivi:

- a. In relazione al **servizio ICI-IMU-TASI, TARSU/TIA/TARES:**
  - i. Verifica posizioni storiche e aggiornamento banca dati dei contribuenti:  
l'attività di verifica tributaria sarà svolta analizzando ogni singola posizione catastale e/o contributiva.  
Per quanto riguarda l'attività di accertamento, sarà creata una banca dati Informatica contenente tutti i dati necessari per una corretta azione di accertamento. I dati di origine saranno forniti dall'ente e/o acquisiti attraverso altre banche dati. In particolare:
    - Denunce ICI/IMU/TASI presentate dai contribuenti;
    - Dati relativi ai pagamenti spontanei ICI/IMU/TASI provenienti dall'Agente della Riscossione;
    - Dati relativi ai pagamenti con bollettino da violazione a seguito di avviso di accertamento;

- Dati relativi agli aggiornamenti catastali (nuove rendite o variazioni di rendita) provenienti dall’Agenzia del Territorio (Catasto).

La nuova banca dati che sarà realizzata a seguito delle attività precedente elencate, sarà quindi bonificata per ottenere la miglior rappresentazione delle situazioni patrimoniali e contributive dei contribuenti e permettere quindi le attività di accertamento.

ii. Accertamenti, valore degli atti emessi, responsabilità della transazione:

Gli accertamenti saranno eseguiti su tutte le fattispecie catastali previste dalla normativa statale e locale. In particolare vengono verificate le posizioni di:

- Fabbricati di tipo D;
- I fabbricati civili;
- Aree fabbricabili;
- terreni agricoli,
- fabbricati rurali.

Il valore di riferimento per determinare la responsabilità di transazione è quello indicato nell’atto di accertamento notificato al contribuente. A titolo di esempio: se un’adesione viene conclusa a 2.000 € ma l’atto di accertamento notificato indicava un valore di 100.000 €, si considera il valore accertato e non transato.

I parametri di riferimento sono:

- Il Direttore di Rete e/o il product manager possono istruire transazioni di qualsiasi valore, anche oltre i 50.000 € accertati. Per importi superiori ai 300.000 € deve preventivamente essere informato il C.D.;
- L’RDOT e/o i tecnici specializzati possono istruire transazioni per accertamenti su un singolo soggetto fino ad un valore di 50.000 € accertati;
- Il responsabile di Commessa può istruire transazioni per accertamenti su un singolo soggetto fino ad un valore di 10.000€ accertati.
- L’operatore può istruire transazioni per accertamenti su un singolo soggetto fino ad un valore di 2.500€ accertati.

iii. Predisposizione dei provvedimenti.

Gli accertamenti ritenuti idonei saranno stampati e consegnati con comunicazione protocollata al Comune sotto forma di elenco riassuntivo degli avvisi, corredato di motivazione sul singolo accertamento.

I provvedimenti di accertamento elaborati da Fraternità Sistemi saranno stampati utilizzando un modello validato dal responsabile dei servizi tributari del Comune.

Il Comune ha il diritto di stralciare, modificare, cancellare posizioni dalla lista dei soggetti accertati con atto formale motivato. In tal caso il responsabile del procedimento emetterà un formale atto di annullamento/revoca/parziale revoca, che sarà registrato e annotato nel software tributario e conservato nella cartella del contribuente.

L’avviso di accertamento deve sempre contenere:

- Cognome e nome / ragione sociale, indirizzo;
- codice fiscale;
- Ubicazione degli immobili e relativi identificativi catastali, percentuale di possesso, periodo di possesso;
- Motivazione dell’accertamento;
- Aliquote applicate;
- Indicazione di eventuali detrazioni e/o riduzioni;
- Imposta dovuta, sanzione applicata, interessi;
- Indicazione delle modalità di pagamento, informazioni relative alla definizione agevolata, tempi e modalità per proporre ricorso e nominativo del Responsabile del procedimento.

iv. Istituto dell’adesione.

A norma dell'art. 59, comma 1, lettera m), del D.Lgs. n. 446/97, i comuni possono introdurre l'istituto dell'accertamento con adesione del contribuente (cosiddetto "concordato") sulla base dei criteri stabiliti dal D.Lgs. 19 giugno 1997, n. 218. Il concordato rappresenta una modalità di conciliazione/prevenzione delle vertenze e può essere promosso sia dall'ente locale sia dal contribuente. Nel primo caso, il Comune inoltra al contribuente un "invito a comparire", nel quale sono indicate le annualità d'imposta suscettibili di accertamento, il giorno e il luogo dell'appuntamento, nonché gli elementi rilevanti ai fini dell'accertamento. Nel secondo caso, il contribuente che ha ricevuto un avviso di accertamento attiva la procedura di concordato inviando una domanda in carta libera, con l'indicazione del proprio recapito anche telefonico. L'ufficio, entro quindici giorni dal ricevimento della domanda, invita il contribuente a comparire. L'istituto dell'adesione è regolato con una specifica procedura di gestione "Adesione atto di accertamento" revisionata e aggiornata in base all'evoluzione normativa.

In caso di adesione con conseguente revoca/annullamento/parziale revoca, il responsabile della PA dovrà emettere un formale atto motivato di revoca/annullamento/parziale revoca che giustifichi l'adesione.

v. Fase di trasmissione al comune degli atti di accertamento, notifica, assistenza ai contribuenti e pagamento:

Una volta che l'elenco degli atti d'accertamento è stato approvato dal responsabile della PA, la trasmissione viene effettuata con la seguente modalità:

- Stampa di tutti i provvedimenti emessi;
- Controllo che i provvedimenti emessi corrispondano alla lista approvata dal responsabile;
- Firma da parte del responsabile del procedimento;
- Imbustamento degli atti con eventuali allegati.
- Compilazione raccomandate A/R;
- In alternativa, predisposizione invio a mezzo PEC;
- Trasmissione al contribuente, così come previsto dalla legge, dell'atto di accertamento.

vi. Assistenza ai contribuenti e regime di autotutela:

A seguito della notifica di un accertamento, l'attività di controllo si completa con l'attività di sportello. Essa si tiene in presenza dello stesso Contribuente ove ritenga di intervenire nel procedimento per esporre direttamente le proprie ragioni o giustificazioni. In tale sede possono essere verificati/definiti/stralciati gli atti già notificati. Possono poi essere acquisite nuove informazioni, che consentono l'emissione di nuovi accertamenti contestualmente stampati e notificati.

Nel caso di revoca/annullamento/parziale revoca di atti d'accertamento già emessi, il responsabile dell'Ente locale dovrà emettere un formale atto motivato di revoca/annullamento/parziale revoca che sarà registrato nel software tributario.

vii. Principio di tracciabilità degli atti emessi:

Una volta che l'atto di accertamento è emesso e quindi ha ricevuto un numero univoco di pratica, esso deve poter essere tracciato durante tutto il corso della sua validità amministrativa. Ogni cambio di stato (revoca totale o parziale, annullamento) deve essere motivato con atto formale da parte del funzionario responsabile dell'Ente locale.

Nel caso di erronea emissione (errore formale e/o insussistenza dell'accertamento) e prima che l'atto sia trasmesso alla PA, il suo annullamento nel software tributario è possibile solo con l'autorizzazione del superiore gerarchico del dipendente che ha istruito l'atto e secondo le soglie autorizzative di cui al punto ii. Tale autorizzazione dovrà essere rilasciata per iscritto (mail o altro documento) e motivata menzionando la causa della decisione. L'autorizzazione dovrà essere annotata nel software tributario.

**b. In relazione al servizio DPA:**

- i. ciascun operatore allo sportello, ricevuta la richiesta di affissione, verifica tramite lo scadenziario (il cui accesso è protetto da apposita password soggetta a periodica modifica) la disponibilità degli spazi e comunica al contribuente l'importo dovuto sulla base di quanto previsto dal regolamento per l'applicazione dell'Imposta Comunale sulla Pubblicità e del Diritto sulle Pubbliche Affissioni nonché le modalità di versamento ed i tempi di prenotazione;
- ii. Ricevuto il versamento, l'operatore compila la bolla di pagamento, allegandola al versamento, e la archivia tenendone copia per il contribuente; consegna quindi il registro delle affissioni agli attacchini che, ultimata l'affissione, compilano la Nota delle Affissioni;
- iii. In caso di affissioni abusive, gli attacchini provvedono al loro oscuramento o defissione e compilano la nota delle Defissioni; di tale attività vengono informati mediante comunicazione il Comando della Polizia Locale ed il Servizio Entrate dei Comuni, allegando anche i rilievi fotografici;

**c. In relazione al servizio ICP:**

- i. entro il 31 gennaio di ogni anno, l'operatore allo sportello provvede ad inviare ai contribuenti presenti in banca dati, un avviso bonario contenente il tributo da versare e, una volta ottenuto il pagamento, viene inserito nel programma di gestione comprovandone l'avvenuto inserimento;
- ii. Successivamente l'operatore svolge un'attività di censimento dei contribuenti e consegna una lista degli stessi ai rilevatori che provvedono a verificare, mediante controllo sul territorio, la congruenza dei dati dichiarati con i dati esistenti compilando la "Scheda di rilevazione ICP/TOSAP";
- iii. In caso di difformità, vengono generati gli avvisi di accertamento che sono soggetti a controllo da parte funzionario comunale in caso di affidamento di servizio o dal Responsabile del settore Tributi Minori in caso di concessione, i quali sottoscrivono solo dopo averne verificato la correttezza;
- iv. In seguito alla ricezione dell'avviso di accertamento da parte del contribuente, lo stesso può produrre la documentazione necessaria per ottenere la rettifica o l'annullamento dell'atto; in questo caso viene richiesto dall'operatore allo sportello la compilazione del modulo di "rettifica" ovvero di "annullamento" che vengono sottoscritti, dopo gli opportuni controlli, dal funzionario comunale in caso di affidamento di servizio o dal Responsabile dei settore Tributi Minori in caso di concessione;
- v. In caso di ricorso, il responsabile del Servizio esamina il ricorso, raccoglie la documentazione e la invia al Responsabile della Segreteria Legale e Societaria per le opportune controdeduzioni, unitamente alla "scheda di contenzioso" compilata;

Con riferimento all'**attività di annullamento degli atti**, che fornisce autotutela alla Società nel caso di atti emessi e poi rivelatisi errati a seguito di controlli interni o segnalazioni, la Società ha previsto apposite procedure, avente il fine di garantire i requisiti di trasparenza, tracciabilità e uniformità dell'attività di annullamento degli atti.

Per quanto concerne il **processo di Gestione Risorse Umane** la Società ha adottato apposite procedure inerenti:

- le assunzioni e le dimissioni del personale;
- la formazione e l'addestramento del personale dipendente;
- l'inserimento lavorativo del soggetto svantaggiato;
- il trasferimento in altra zona di competenza.

Secondo tali procedure la Società osserva i seguenti protocolli preventivi:

- A. la definizione dei requisiti minimi e delle qualifiche che deve possedere il personale dell'azienda;
- B. la selezione delle risorse viene effettuata nei limiti di rispetto del budget prestabiliti, previa delibera da parte del CdA e garantendo la tracciabilità e la trasparenza delle valutazioni e delle scelte operate, in particolar modo deve essere garantito:
  - a. la pubblicità dell'avviso di selezione del personale, sempre anche mediante pubblicazione sul sito internet aziendale;
  - b. la parità di trattamento nella fase di selezione e l'assenza di discriminazioni;
  - c. un congruo termine per la presentazione delle candidature e un congruo preavviso per la convocazione alle selezioni;
  - d. la valutazione ad opera di una commissione collegiale, composta da almeno un membro esterno all'azienda, e alla quale non possono prendere parte soggetti coinvolti nei processi di acquisizione o contrattualizzazione delle commesse;
  - e. la verbalizzazione di tutte le fasi di selezione del personale, compresi i colloqui e i giudizi sintetici espressi circa ciascun candidato, e la conservazione di detti verbali;
  - f. il divieto assoluto di ammettere alla selezione soggetti le cui candidature non pervengano attraverso i canali previsti mediante l'avviso pubblicato ovvero che siano stati "segnalati" da clienti o da soggetti politicamente esposti, o comunque da esponenti degli Enti locali e/o stazioni appaltanti;
  - g. anche con specifico riferimento agli inserimenti lavorativi di soggetti svantaggiati la procedura di selezione, pur con gli adeguamenti richiesti dal caso, dovrà avvenire nel rispetto dei principi suddetti e non potrà in nessun caso essere consentita l'indicazione del soggetto da assumere ad opera del committente.
- C. il dimensionamento e la tipologia di organico impiegato deve essere sempre congruo con quanto previsto dalla normativa in materia;
- D. in caso di rimborso spese per viaggi/trasferte ai dipendenti, oltre ad un'autorizzazione preventiva alla trasferta da parte del Consigliere Delegato, è prevista l'approvazione del pagamento da parte dello stesso e da parte del Responsabile del Servizio nel caso di servizi che facciano capo direttamente ad esso, previa verifica di congruenza, completezza e correttezza delle note spese presentate;
- E. i sistemi premiali delle risorse interne sono basati su target di performance misurabili, raggiungibili e concreti.

### 3. Principi e regole di comportamento

Relativamente ai Rapporti con la PA, nell'ambito della categoria dei reati in trattazione, la Società impone:

- a. l'OBBLIGO di:

osservare tutte le leggi e regolamenti che disciplinano le diverse attività svolte all'interno della Società ed impegnarsi, nei limiti delle rispettive competenze, ad operare affinché sia rispettato quanto previsto dalla normativa in materia;

instaurare e mantenere rapporti con la PA basati su criteri di massima correttezza e trasparenza;

nel caso in cui emergano, nell'ambito del rapporto con la PA, criticità di qualsiasi natura o conflitto di interesse deve esserne data, con nota scritta, tempestiva comunicazione all'Organismo di Vigilanza;

porre particolare attenzione all'attuazione e al controllo degli adempimenti richiesti dalla PA e riferire immediatamente al superiore gerarchico e all'Organismo di Vigilanza eventuali situazioni di irregolarità o anomalie nel rispetto delle modalità di segnalazione prescritte;

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 FS 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'OdV qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della PA o di un incaricato di pubblico servizio o di episodi di tentativi di corruzione di cui si dovesse essere destinatari o semplicemente venirne a conoscenza; nel caso la segnalazione sia stata effettuata al superiore gerarchico, lo stesso deve trasmettere tempestivamente la segnalazione ricevuta all'OdV;

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.

b. il DIVIETO di:

effettuare elargizioni in danaro a pubblici funzionari;

accettare elargizioni in danaro o regalie;

promettere, offrire o consegnare denaro, omaggi, regalie altre utilità o accordare vantaggi di qualsiasi natura, anche per interposta persona, in favore di pubblici funzionari o di soggetti ad essi legati da un vincolo familiare;

ricevere danaro, doni o qualsiasi altra utilità ovvero accettarne la promessa, da chiunque sia o intenda entrare in rapporto con la Società e voglia conseguire indebitamente un trattamento in violazione della normativa o delle disposizioni impartite o, comunque, un trattamento più favorevole rispetto a quello dovuto;

influenzare o determinare le decisioni dei soggetti operanti per nome e per conto della PA con violenza, forza o inganno;

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 la Società 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 della Società;

presentare dichiarazioni non veritiere a enti pubblici nazionali e/o comunitari al fine di conseguire o far conseguire erogazioni, contributi o finanziamenti agevolati;

destinare eventuali somme ricevute da enti pubblici nazionali e/o comunitari per scopi diversi da quelli a cui originariamente erano destinati;

impedire, occultare dati, documenti e informazioni in occasione di visite ispettive da parte degli enti di controllo al fine di influenzarne impropriamente l'esito.

## 4. Controlli dell'Organismo di Vigilanza

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 della Società 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 aziendali, 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 aziendale 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 e del 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 aziendali;

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 committenti ovvero con esponenti aziendali;

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

## SEZIONE B) - REATI SOCIETARI e REATI DI ABUSO DI MERCATO

Gli artt. 25-ter e 25-sexies del Decreto contemplano i cosiddetti reati societari e i reati di abuso di mercato. Di questi rischi di reati solo alcuni sono stati ritenuti inerenti per la Società, ovvero:

- Impedito controllo (art 2625 c.c.)
- Indebita restituzione dei conferimenti (art. 2626 c.c.)
- Illegale ripartizione di utili e riserve (art.2627 c.c.)
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
- Formazione fittizia del capitale (art. 2632 c.c.)
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)
- Corruzione tra privati (art. 2635, comma 3 c.c.)
- Illecita influenza sull'assemblea (art. 2636 c.c.)
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)
- False comunicazioni sociali e fatti di lieve entità (artt. 2621 e 2621-bis e c.c.)
- Aggiotaggio (art. 2637 c.c.)
- Abuso di informazioni privilegiate (art. 184 TUF)
- Manipolazione del mercato (art. 185 TUF)

Si può osservare come l'interesse del legislatore sia volto ad assicurare la trasparenza nei documenti contabili e nella gestione societaria e, più in generale, la corretta informazione ai terzi.

### 1. Elenco delle fattispecie di reato ipotizzabili per processo sensibile

In considerazione della *ratio* normativa volta alla tutela dei soci e dei terzi, il processo che risulta presentare una sensibilità diretta ai rischi di reato in esame è quello relativo alla **Approvazione del Bilancio di Esercizio** da parte dell'Assemblea e pertanto si illustrano sinteticamente di seguito le potenziali fattispecie di reato previste dagli artt. 24 e 25 che potrebbero astrattamente verificarsi.

Il reato di Impedito controllo (art. 2625 c.c.) potrebbe realizzarsi, ad esempio, in caso di occultamento di documenti amministrativo-contabili, da parte del personale degli uffici amministrativi, per ostacolare lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali.

Il reato di Indebita restituzione dei conferimenti (art. 2626 c.c.) potrebbe realizzarsi, ad esempio, nel caso in cui gli amministratori restituiscano anche simulatamente i conferimenti ai soci, ovvero li liberino dall'obbligo di eseguirli.

I reati di Illegale ripartizione di utili e riserve (art. 2627 c.c.) nel caso in cui, ad esempio, gli amministratori ripartiscano utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartiscano riserve, anche non costituite con utili, che non possono per legge essere distribuite.

Il reato di Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.) nel caso in cui, ad esempio, la società acquisti o sottoscriva proprie quote sociali o quote della società controllante cagionando una lesione dell'integrità del capitale sociale o delle riserve non distribuibili per legge.

I reati di Operazioni in pregiudizio dei creditori (art. 2629 c.c.) nel caso in cui gli amministratori, in violazione delle disposizioni di legge a tutela dei creditori, effettuino riduzioni del capitale sociale o fusioni con altra società o scissioni cagionando danno ai creditori.

Il reato di Formazione fittizia del capitale (art. 2632 c.c.) potrebbe configurarsi nel caso in cui gli amministratori e i soci conferenti formino o aumentino fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, mediante sottoscrizione reciproca di azioni o quote, altresì attraverso una sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

Il reato di Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.) potrebbe configurarsi nel caso in cui la Società fosse posta in liquidazione, ovvero mediante concorso in caso di altra Società posta in liquidazione, laddove fossero poste in essere operazioni che cagionino danno ai creditori, mediante ripartizione di beni sociali tra i soci prima di avere estinto più obbligazioni verso i creditori o di avere accantonato le somme necessarie a soddisfarli.

Il reato di Corruzione tra privati (art. 2635 c.c.) potrebbe verificarsi nel caso in cui un soggetto, al fine di far conseguire un interesse o un vantaggio alla Società FS, ma anche semplicemente in virtù della sua qualità di incaricato di pubblico servizio, dia o prometta denaro, beni o altre utilità ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori di un'altra società affinché gli stessi compiano od omettano atti in danno alla società presso la quale rivestono la carica.

Il reato di Illecita influenza sull'assemblea (art. 2636 c.c.) potrebbe verificarsi nel caso in cui gli amministratori determinino fraudolentemente la maggioranza in assemblea allo scopo di procurare un profitto per la Società o comunque assumendo una deliberazione che vada a vantaggio della Società, per esempio al fine di garantire la continuità aziendale.

Il reato di Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.) potrebbe realizzarsi, ad esempio, nel caso in cui, al fine di ostacolare l'esercizio delle funzioni delle autorità pubbliche di vigilanza, si espongono atti materiali non rispondenti al vero sulla situazione economica, patrimoniale o finanziaria ovvero occultano con altri mezzi fraudolenti, in tutto o in parte, fatti, concernenti la situazione medesima, che sarebbero dovuti essere oggetto di comunicazione alle autorità di vigilanza.

Il reato di False comunicazioni sociali (art. 2621 c.c.) e di Fatti di lieve entità (art. 2621-bis c.c.) potrebbero realizzarsi, ad esempio, in cui gli amministratori o comunque di esponenti della Società (personale amministrativo-contabile e non) esponano nelle comunicazioni sociali previste dalla legge dei fatti non corrispondenti al vero al fine di indurre in errore soci o terzi circa la situazione economica, patrimoniale e finanziaria, al fine di trarre un ingiusto profitto per la Società.

A titolo esemplificativo, tra i modi più ricorrenti di realizzazione dei rischi di reato in esame, si segnalano tutte quelle forme dirette a modificare i dati contabili presenti sul sistema informatico, per fornire una falsa rappresentazione della situazione patrimoniale, economica e finanziaria attraverso l'inserimento di voci di bilancio inesistenti o di valori difformi da quelli reali.

Il reato di Aggiotaggio (art. 2637 c.c.) potrebbe realizzarsi allorché si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

Il reato di Abuso di informazioni privilegiate (art. 184 TUF) potrebbe configurarsi nel caso in cui il soggetto, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di

amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:

- a) acquista, vende o compie altre operazioni, direttamente od indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;
- b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;
- c) raccomanda od induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a)

Il reato di Manipolazione del mercato (art. 185 TUF) potrebbe realizzarsi, ad esempio, nel caso in cui un dipendente della Società, nell'esercizio delle funzioni, diffondesse false notizie, ponesse in essere operazioni simulate o altri artifici tali da provocare una alterazione sensibile del prezzo di strumenti finanziari, allo scopo di favorire l'ente.

I processi maggiormente a rischio, in ordine ai reati sopra elencati, sono:

- Processo di approvazione del bilancio;
- Processo Acquisti;
- Processo Gestione Risorse Umane.

## 2. Protocolli preventivi adottati

Le modalità operative, l'iter approvativo e le tempistiche di svolgimento delle singole attività legate al processo individuato al paragrafo precedente garantiscono la tracciabilità e la verificabilità delle transazioni attraverso adeguati supporti documentali, disponibili negli archivi della Società. I diversi responsabili, infatti, sono tenuti a garantire la coerenza, congruità, correttezza e veridicità delle operazioni effettuate, la corretta archiviazione e conservazione della documentazione elaborata, anche in via telematica o elettronica, inerente alla esecuzione delle attività e degli adempimenti di competenza al fine di consentirne la ricostruzione delle responsabilità e delle motivazioni che hanno condotto alle scelte effettuate.

Per ciascuna area organizzativa è infatti identificato il personale preposto alla trasmissione tempestiva di tutta la documentazione richiesta dagli Organi Sociali, dai membri del Collegio sindacale, dalla società di revisione e dall'OdV nell'ambito della propria attività.

Sono previste, inoltre, riunioni periodiche, secondo un calendario prestabilito e condiviso tra CD, Collegio Sindacale e OdV per verificare l'osservanza della normativa di riferimento e la corretta applicazione dei principi contabili e, in caso di condotte delittuose o non conformi alle procedure, per prevedere azioni correttive o disciplinari da intraprendere nel rispetto del sistema sanzionatorio vigente. Al termine di tali riunioni viene redatto un apposito verbale.

Per quanto concerne il processo di **Approvazione del bilancio d'esercizio** che, come già evidenziato, rappresenta il processo principale per la possibile commissione dei reati in oggetto, la Società si è dotata dei seguenti protocolli preventivi:

- a. Obbligo per tutti i dipendenti coinvolti nelle attività di formazione del bilancio o degli altri documenti similari di tenere un comportamento corretto e di massima collaborazione verso tutti gli organi sociali e di vigilanza preposti;
- b. attività di formazione continua dei dipendenti che operano in contabilità sulle principali nozioni di bilancio (principi contabili, norme di legge, sanzioni, ecc.);

- c. tracciabilità delle operazioni e dei passaggi di inserimento dati, registrazione/cancellazione di scritture contabili, ecc., nonché identificazione dei soggetti che ne sono stati gli autori, così da consentire un controllo costante e garantire l'individuazione di eventuali operazioni sospette o inusuali;
- d. il bilancio è soggetto al controllo del Collegio Sindacale e della Società di Revisione che rispondono a requisiti di indipendenza, autonomia, onorabilità e professionalità con cui si intrattengono rapporti improntati su principi di trasparenza e correttezza; i dirigenti delle funzioni coinvolte nell'elaborazione della bozza di bilancio, o di altre comunicazioni sociali, sono responsabili della veridicità e completezza dei dati e delle informazioni trasmesse;
- e. svolgimento di una riunione collegiale tra OdV, Collegio Sindacale e C.D.prima dell'approvazione del bilancio e dopo la predisposizione del progetto di Bilancio al fine di verificare l'effettiva applicazione delle procedure;
- f. definizione dei ruoli e delle responsabilità relativamente alla tenuta, conservazione e aggiornamento della documentazione contabile e del fascicolo di bilancio.

I documenti del bilancio di esercizio devono essere redatti rispettando requisiti di chiarezza, completezza, e che permettano la tracciatura delle operazioni e dei soggetti responsabili dell'inserimento dei dati nel sistema.

Per quanto concerne **Processo Acquisti** e il **Processo Gestione Risorse Umane** si richiamano i protocolli preventivi già dettagliati nella precedente Sezione A).

### 3. Principi e regole di comportamento

In tutte le operazioni e attività sensibili ai Reati Societari la Società impone ai soggetti coinvolti:

- a. l'OBBLIGO di:
  - conoscere e rispettare la normativa di riferimento e le norme inerenti al sistema amministrativo, contabile e finanziario della Società nonché di tutte le disposizioni di legge a tutela della trasparenza, dell'informazione e dell'integrità del Capitale;
  - tenere un comportamento corretto, trasparente e collaborativo nel rispetto delle norme di legge e delle procedure/istruzioni interne in tutte le attività finalizzate o collegate alla formazione del bilancio e delle altre comunicazioni sociali allo scopo di fornire a terzi informazioni veritiere e corrette sulla situazione economica, patrimoniale e finanziaria della Società;
  - effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge, agevolando e collaborando all'esercizio delle attività di verifica degli enti pubblici di controllo;
  - conoscere e rispettare le norme inerenti il sistema amministrativo, contabile e finanziario della Società, nonché di tutte le disposizioni di legge a tutela della trasparenza, dell'informazione, dell'integrità del Capitale;
  - mantenere comportamenti improntati alla massima correttezza e trasparenza nel caso in cui vi sia stata una richiesta di produzione di documenti o di informazioni da parte dell'Organismo di Vigilanza, del Collegio Sindacale o della società di revisione e non ostacolare in alcun modo le attività di controllo;
  - rendere disponibili i dati ed i documenti richiesti in modo puntuale ed in un linguaggio chiaro, oggettivo ed esaustivo in modo da fornire informazioni accurate, complete e veritiere;
  - eseguire gli incassi ed i pagamenti secondo le istruzioni e le modalità di controllo interne;
  - comunicare con tempestività all'OdV eventuali operazioni esposte a situazioni di conflitto di interesse;
  - comunicare all'OdV eventuali ulteriori incarichi conferiti ai membri del Collegio Sindacale o alla società di revisione;

trasmettere al Collegio Sindacale, con congruo anticipo, tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'Assemblea o sui quali esso debba esprimere un parere ai sensi di legge.

b. Il DIVIETO di:

Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato considerate ai sensi dell'art. 25 ter del D. Lgs. 231/2001;

Violare i principi e le procedure/istruzioni interne esistenti previste;

Esercitare, con qualsiasi mezzo o per interposta persona, "*illecita influenza*" sull'operato e sulle decisioni dell'Assemblea dei soci;

Compiere illecite ripartizioni degli utili e operazioni fraudolente sulle azioni o quote sociali;

rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni, documenti, comunicazioni e dati, anche risultanti da valutazioni estimative, falsi, imprecisi, lacunosi, erronei o, comunque, non rispondenti alla reale situazione economica, patrimoniale e finanziaria della Società;

omettere od alterare dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società ovvero destinati ad essere utilizzati in prospetti informativi;

tenere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo o di revisione della gestione da parte del Collegio Sindacale o della società di revisione;

omettere di effettuare, con la dovuta completezza, accuratezza, diligenza e tempestività, le segnalazioni periodiche previste dalle leggi e dai regolamenti nonché omettere di dar corso con sollecitudine all'invio dei dati e della documentazione prevista dalla normativa;

esporre nelle predette comunicazioni fatti non rispondenti al vero, ovvero occultare fatti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;

porre in essere condotte tali che siano di ostacolo all'esercizio delle funzioni di vigilanza da parte delle Autorità competenti cui è sottoposta la Società (ad es. espressa opposizione, rifiuti ingiustificati, ritardi nella trasmissione o nella consegna di documenti).

## 4. Controlli dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, lo stesso effettua periodicamente controlli a campione sulle attività della Società potenzialmente a rischio di reati societari diretti a verificare la corretta esplicazione delle stesse in relazione alle regole contenute nel presente Modello ed alle procedure/istruzioni operative adottate e vigenti (quali ad es. redazione bilancio e adempimenti tributari e fiscali).

L'Organismo di Vigilanza, oltre a mantenere traccia delle informazioni ricevute ed inviate, deve conservare agli atti evidenza di tutte le verifiche effettuate. A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Inoltre, l'OdV deve tracciare tramite appositi verbali tutte le riunioni periodiche con il CdA, con il C.D., con il Collegio Sindacale e la Società di revisione, durante i quali vengono effettuati approfondimenti ed analisi documentali.

In ogni caso, l'ODV si incontra con il C.D. e il Collegio Sindacale almeno una volta l'anno per l'esame del progetto di bilancio prima della sua approvazione.

L'OdV, in caso di eventuali situazioni di conflitto di interesse che si venissero a creare all'interno della Società, ha il compito di indicare le modalità operative più adeguate per la loro risoluzione.

## SEZIONE C) – DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO, DELITTI INFORMATICI, TRATTAMENTO ILLECITO DI DATI E VIOLAZIONE DEL DIRITTO D'AUTORE

L'art. 24 bis del Decreto prevede alcune fattispecie di reato la cui commissione può originare la responsabilità amministrativa della Società. In particolare, sono contemplate le fattispecie delittuose qui di seguito elencate:

- Falsità in documenti informatici (art. 491-bis c.p.)
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 - quater c.p.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 615 quinquies c.p.)
- Danneggiamento di informazioni, dati e programmi informatici (Art. 635-bis c.p.)
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (Art. 635-ter c.p.)
- Danneggiamento di sistemi informatici o telematici (Art. 635-quater c.p.)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635-quinquies c.p.)

Inoltre, l'art. 25 novies del D.Lgs. 231/01 prevede alcune fattispecie inerenti la violazione del diritto d'autore, tra le quali sono da considerarsi rilevanti in relazione all'attività svolta da Fraternalità Sistemi le seguenti:

- Turbata libertà dell'industria o del commercio (art. 513 c.p.)
- Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.)
- 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)
- 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)
- Riproduzione o trasferimento su un altro supporto, distribuzione, presentazione in pubblico del contenuto di una banca dati (art. 171-ter, L. 633/1941)
- Delitti in materia di violazione del diritto d'autore (artt. 171 septies e octies, L. 633/1941)

### 1. Elenco delle fattispecie di reato ipotizzabili per processo sensibile

In relazione all'attività svolta dalla Società, si illustrano sinteticamente di seguito le potenziali fattispecie di reato previste dagli artt. 24-bis e 25 novies che potrebbero astrattamente verificarsi nell'ambito dei processi ritenuti sensibili e che presentano un livello di rischio critico o rilevante.

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 (art. 482 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.); Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.).

Il reato di Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) potrebbe configurarsi laddove un dipendente della Società, 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.

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 dipendente fornisca a terzi non autorizzati credenziali di accesso a sistemi informatici gestiti da FS, ovvero consentano a terzi di continuare ad utilizzare le predette credenziali pur non avendone più titolo, al fine di procurarsi un profitto eventualmente derivante dalla relazione con i terzi.

Il reato di Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.) potrebbe configurarsi laddove dipendenti della Società, per interessi connessi allo svolgimento dell'attività, producano, si procurino, diffondano apparecchiature, dispositivi, o programmi informatici (ad esempio i cosiddetti virus), allo scopo di danneggiare un sistema informatico o telematico, o i dati in esso contenuti, di un terzo.

Il reato di Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) potrebbe configurarsi laddove un dipendente della Società impedisca o interrompa comunicazioni informatiche o telematiche, ovvero ne rilevi il contenuto, mediante qualsiasi mezzo di informazione al pubblico. Tale processo potrebbe realizzarsi, in concreto, anche in caso di illecito controllo delle comunicazioni dei dipendenti.

Il reato di Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 615 quinquies c.p.) potrebbe configurarsi laddove soggetti della società installino apparecchiature atte ad intercettare. Tale reato potrebbe in concreto realizzarsi anche nel caso di installazione di apparecchiature atte a intercettare le comunicazioni telematiche o informatiche dei dipendenti.

Il reato di Danneggiamento di informazioni, dati e programmi informatici (Art. 635-bis c.p.) potrebbe configurarsi laddove dipendenti della Società ponggano in essere attività di distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici, e ciò eventualmente anche al fine di agevolare o coprire una propria condotta illecita.

Il reato di 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.) potrebbe configurarsi laddove i dipendenti della Società ponessero in essere attività di distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici, utilizzati dallo Stato o da altro ente pubblico, e ciò eventualmente anche al fine di agevolare o coprire una propria condotta illecita.

Il reato di Danneggiamento di sistemi informatici o telematici (Art. 635-quater c.p.) laddove dipendenti della Società ponessero in essere attività di distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici, rendendo in tutto o in parte inservibili tali sistemi informatici o telematici, e ciò eventualmente anche al fine di agevolare o coprire una propria condotta illecita

Il reato di Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635-quinquies c.p.) potrebbe configurarsi laddove dipendenti della Società ponessero in essere attività di distruzione,

deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici utilizzati dallo Stato o comunque di pubblica utilità, rendendo in tutto o in parte inservibili tali sistemi informatici o telematici, e ciò eventualmente anche al fine di agevolare o coprire una propria condotta illecita. Tali condotte sarebbero aggravate laddove realizzate su sistemi informatici sui quali la Società o gli addetti della Società rivestano la qualifica di "operatori di sistema"

Con riferimento al secondo 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 turbata libertà dell'industria o del commercio (art. 513 c.p.) potrebbe astrattamente realizzarsi laddove un dipendente della Società impedisse o turbasse, nell'interesse della Società medesima, l'esercizio di un'attività di un terzo adoperando violenza sulle cose o mediante l'uso di mezzi fraudolenti.

La fattispecie di illecita concorrenza con minaccia o violenza (art. 513-bis c.p.) si potrebbe verificare laddove un dipendente della Società commettesse atti di concorrenza usando violenza o rivolgendo minacce al fine di ottenere un vantaggio per la Società medesima.

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 laddove la Società, per la realizzazione delle proprie attività, 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 laddove la Società, per la realizzazione delle proprie attività, 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 laddove la Società, per lo svolgimento delle proprie attività, 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.

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.

\*\*\*\*\*

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 FS, tutti i processi aziendali sono astrattamente esposti al rischio di commissione di tali reati.

In particolare, con riferimento a tutti i processi di gestione dei singoli tributi, risulta particolarmente sensibile l'attività di Verifica e bonifica banca dati 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 misure minime di profilazione utente per gli accessi ai diversi programmi e database gestiti dalla Società, 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 la Società.

I reati in esame potrebbero essere commessi da chiunque abbia accesso ai sistemi informatici dell'ente 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.

## 2. Protocolli preventivi adottati

Al fine di prevenire il presentarsi delle fattispecie delittuose sopra menzionate, la Società si è dotata di specifici protocolli preventivi:

- 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;
- 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;
- 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 della Società;
- 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;
- l'accesso alla rete informatica aziendale, per la consultazione e l'elaborazione di dati, documenti e informazioni da comunicare o ricevuti dalla PA, 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;
- la 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 impegnano al corretto utilizzo delle risorse informatiche aziendali;
- formazione ed informazione di 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 aziendali ed organizzate procedure per la garanzia della sicurezza nei trattamenti dei dati.

### 3. Principi e regole di comportamento

La Società 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.

a. l'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);  
non divulgare informazioni relative ai sistemi informatici della Società;  
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.

b. il 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 dalla Società 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 dalla Società, al fine di acquisire informazioni riservate, alterarle e/o cancellarle;

divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, 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 della Società, 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 della Società, 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 della Società, di clienti o di terze parti;

comunicare a persone non autorizzate, interne o esterne alla Società, 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 aziendale un software che possa impedire/interrompere o danneggiare le comunicazioni all'interno della Società 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.

#### 4. Controlli dell'Organismo di Vigilanza

In riferimento ai reati in esame, l'OdV 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'OdV condurrà quindi controlli a campione diretti a verificare le procedure/istruzioni interne ed i protocolli contenuti nel presente Modello nonché l'adeguatezza delle prescrizioni a prevenire i rischi di reato potenziali.

## SEZIONE D) - RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA E AUTORICICLAGGIO

L'art. 25-octies del Decreto contempla i cosiddetti reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio:

1. Ricettazione (art. 648 c.p.)
2. Riciclaggio (art. 648-bis c.p.)
3. Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)
4. Autoriciclaggio (art. 648-ter.1 c.p.)

### 1. Elenco delle fattispecie di reato ipotizzabili per processo sensibile

Di seguito si riporta una esemplificazione delle possibili modalità di commissione dei reati in esame all'interno della Società evidenziando una peculiare rischiosità a tal fine del processo Acquisti.

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 della Società, al fine di procurare per la stessa Società un profitto, acquistasse, ricevesse od occultasse denaro o cose provenienti da un qualunque delitto ovvero si intromettesse a tal fine.

### 2. Protocolli preventivi adottati

La Società, 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 700,00. 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 sociali e all'OdV;

monitoraggio dei flussi finanziari aziendali 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 dalla Società 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.

In aggiunta con specifico riferimento al **processo acquisti** vengono specificamente richiamati i protocolli preventivi previsti alla Sezione A).

### 3. Principi e regole di comportamento

I soggetti coinvolti nelle aree ritenute a rischio di commissione dei reati in esame tenuti, nell'ambito dei propri compiti e responsabilità, al rispetto delle norme di comportamento di seguito indicate:

a. **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.

b. **DIVIETO** di:

compiere atti o agevolare attività e operazioni contrarie alle prescrizioni normative;  
utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;  
mantenere comportamenti che siano in contrasto con il Codice Etico, il presente Modello e le procedure interne che disciplinano le attività della Società;  
intrattenere rapporti commerciali con fornitori, consulenti e partner che compiono o si sospetti che possano compiere attività contrarie alle normative vigenti;  
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.

## 4. Controlli dell'Organismo di Vigilanza

In riferimento ai reati in esame, l'OdV 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'OdV 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 aziendale rilevante.

## SEZIONE E) - REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI E GRAVISSIME

La **legge 3 agosto 2007, n. 123** è intervenuta inserendo l'art. 25-septies, disposizione che estende il regime del D.Lgs. 231/2001 alle ipotesi di:

**omicidio colposo** (art. 589 c.p.)

**lesioni colpose gravi o gravissime** (art. 590, co. 3, c.p.)

commessi in violazione o attraverso la mancata applicazione delle norme in materia di igiene, sicurezza e salute sul lavoro.

La punibilità degli Enti riguarda sia i delitti perseguibili a **titolo doloso**, in cui vi sia coscienza e volontarietà dell'azione criminosa, sia i **delitti colposi**, in cui si ravvisa la mancanza di volontarietà nella realizzazione dell'evento giuridico rilevante.

Le sanzioni previste dal Decreto vengono applicate esclusivamente qualora gli stessi siano stati commessi nell'interesse o a vantaggio dell'ente anche potenziale, ovvero quando la **violazione o la mancata applicazione delle norme antinfortunistiche** sia finalizzata ad un risparmio economico o anche semplicemente di tempo per la Società.

Restano pertanto **esclusi dalla responsabilità della Società gli infortuni derivanti dal c.d. rischio elettivo**, ossia il rischio diverso da quello a cui il lavoratore sarebbe ordinariamente esposto per esigenze lavorative e, quindi, **imprevedibile e incontrollabile per l'Ente in quanto derivante da una scelta arbitraria del lavoratore** che decide di mettersi in **condizioni di pericolo esorbitanti** rispetto alla normale operatività per soddisfare esigenze personali estranee ai processi della Società.

### 1. Elenco delle fattispecie di reato ipotizzabili per processo sensibile

Le aree e i processi sensibili riferibili ai reati in esame 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, non trascurando, tuttavia, la tutela del personale che opera stabilmente presso la sede della Fraternità Sistemi, nonché 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.

I reati di **Omicidio colposo** (art. 589 c.p.) e **Lesioni colpose gravi e gravissime** (art. 590 co. 3 c.p.) potrebbero realizzarsi in particolare nell'ambito dei servizi resi agli enti locali. 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.

## 2. Protocolli preventivi adottati

Il presente paragrafo contempla i principi generali e specifici di comportamento, nonché i protocolli adottati, che tutti i soggetti coinvolti (Dipendenti, membri degli Organi Sociali, 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.

Nella definizione dei compiti organizzativi ed operativi, la Società **ha esplicitato e resi noti le responsabilità ed i compiti di ispezione, verifica e sorveglianza** in materia di salute e sicurezza sul lavoro, in particolare:

il **Datore di lavoro**, ha il compito di:

- **nominare, previa verifica del possesso dei requisiti previsti dalla legge di riferimento, il RSPP, il Medico competente, i lavoratori 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;
- **fornire ai Lavoratori i necessari ed idonei dispositivi di protezione individuale**, sentito il RSPP ed il Medico Competente;
- **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;
- **garantire il rispetto degli obblighi** di informazione, formazione ed addestramento;
- **garantire l'aggiornamento delle misure di prevenzione in relazione ai mutamenti organizzativi** che hanno rilevanza ai fini della salute e sicurezza del lavoro;
- **garantire la sicurezza dei locali, attrezzature e macchinari** ai quali i lavoratori 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 all'interno della Società;
- 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 Lavoratori;
- a partecipare alle consultazioni con i Lavoratori 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 Lavoratori 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 il Datore di Lavoro 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 Lavoratori, 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, avendo cura, nell'osservanza delle specifiche disposizioni di legge, di verificare anche la idoneità all'utilizzo degli autoveicoli da parte dei soggetti applicati a funzioni esterne;
- istituire, aggiornare e custodire sotto la propria responsabilità una cartella sanitaria e di rischio per ogni lavoratore sottoposto a sorveglianza sanitaria;

- fornire informazioni ai Lavoratori sul significato degli accertamenti sanitari a cui sono sottoposti ed informandoli sui relativi risultati;
- comunicare per iscritto, in occasione della riunione periodica di cui all'art. 35 del D. Lgs. 81/2008, 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 dei Lavoratori;
- 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 Lavoratori, 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.

Il **Datore di lavoro** definisce e comunica a tutto il personale la **Politica della Sicurezza** adottata dalla Società, gli obiettivi da perseguire nel campo della salute e sicurezza sul lavoro e l'impegno al miglioramento delle prestazioni relative alla prevenzione degli infortuni e alla tutela dei lavoratori, **anche tramite i dirigenti o responsabili** delegati. 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, il Datore di lavoro, 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 aziendale 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 i Lavoratori 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 della Società 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 della Società significative ai fini della sicurezza e della salute dei Lavoratori.

### 3. 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 aziendali 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 la struttura aziendale**, a tutti i livelli, 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'OdV;

**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 Direzione, dai Responsabili 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'OdV 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 (disponibile sul sistema informativo aziendale) 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 Società 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 assolutamente VIETATO:**

**mettere in atto comportamenti tali da esporre l'azienda** 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.

## 4. 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**, ovvero il Datore di Lavoro, 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 protocolli 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 protocolli, dall'altro l'effettiva adeguatezza delle prescrizioni in essi contenute a prevenire i reati potenzialmente commessibili.

## SEZIONE F) – I REATI DI FALSO NUMMARIO

Il D.Lgs 231/01, come integrato dall'art. 15 della l. 99/2009, all'art. 25bis prevede i reati, disciplinati dal Codice Penale, in ordine alla falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento. In relazione all'attività svolta da Fraternità Sistemi. ed ai rischi nei quali potrebbe incorrere, sono stati ritenuti potenzialmente inerenti per la Società le seguenti fattispecie di reato:

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.)
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.)
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.)
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.)
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.)

### 1. Elenco delle fattispecie di reato ipotizzabili per processo sensibile

Sono fattispecie di reato che consistono nella contraffazione, alterazione di monete genuine, nazionali o straniere, o carte di pubblico credito, nonché nella spendita delle stesse ancorché ricevute in buona fede.

L'area considerata più a rischio, in ordine alla commissione dei reati afferenti a questa categoria, oltre a quella della gestione degli incassi dei tributi per contanti, è quella riguardante la Gestione Acquisti della Società. Sono entrambe aree particolarmente sensibili in quanto potrebbero costituire le circostanze in cui un apicale o un eterodiretto di Fraternità Sistemi riesca più facilmente ad utilizzare monete che siano state falsificate o anche solamente di cui sia a qualsiasi titolo entrato nel possesso.

Ipotesi di configurazione di alcuni dei predetti reati possono individuarsi, a titolo meramente esemplificativo, nei seguenti casi:

Il reato di Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.) potrebbe verificarsi laddove la Società, eventualmente anche al fine di compiacere un soggetto terzo dal quale poter trarre una diversa utilità, si prestasse per spendere e/o mettere in circolazione monete contraffatte o alterate, ovvero al fine di mettere in circolazione le acquistasse o comunque ricevesse dai terzi.

Il reato di Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.) potrebbe configurarsi nel caso in cui la Società, eventualmente anche al fine di compiacere un soggetto terzo dal quale poter trarre una diversa utilità, acquistasse o detenesse monete contraffatte o alterate al fine di metterle in circolazione, fuori dalle ipotesi di cui all'articolo 453 c.p.

Il reato di Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.) potrebbe configurarsi nel caso in cui la Società spendesse o mettesse in circolazione monete contraffatte o alterate, ricevute in buona fede, in via esemplificativa ma non esaustiva negli incassi per tributi, al fine di non sopportare il pregiudizio economico conseguente alla loro distruzione.

Il reato di Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.) potrebbe configurarsi nel caso in cui la Società falsificasse valori di bollo, o introducesse nello Stato, o acquistasse o detenesse o mettesse in circolazione valori di bollo falsificati, anche conseguendo il vantaggio derivante dal conseguente risparmio.

Il reato di Uso di valori di bollo contraffatti o alterati (art. 464 c.p.) potrebbe verificarsi laddove la Società facesse uso di valori bollati contraffatti o alterati, ricevuti in buona fede, al fine di non sopportare il pregiudizio economico conseguente alla loro distruzione.

## 2. Protocolli preventivi adottati e Principi e regole di comportamento

Al fine di mitigare e prevenire la commissione dei reati di falso in nummario, la Società si è dotata di un **sistema organizzativo**, formalizzato da **organigramma**, **sistema qualità certificato**, **procedure e istruzioni operative interne** emanate con apposite **circolari** strutturato in modo da garantire:

- a) La **separazione dei compiti** fra i soggetti che procedono all'attivazione e conduzione dei processi ritenuti sensibili in relazione alla famiglia dei reati in esame ed i soggetti che procedono allo svolgimento dei controlli previsti dalle procedure aziendali di riferimento;
- b) La **tracciabilità delle operazioni** rilevanti all'interno dei processi sensibili, con garanzia della formalizzazione dei controlli effettuati;
- c) Riduzione, nei limiti del possibile, della circolazione di denaro contante, fornendo ai contribuenti, nella gestione ordinaria della riscossione, la possibilità di effettuare pagamenti telematici e tracciati, anche mediante l'utilizzo dei P.O.S. e limitando tutti i pagamenti e incassi in contanti entro la soglia massima di euro 700,00;
- d) Formalizzazione di criteri per il riconoscimento di denaro contante falso e dei comportamenti da adottare ad opera del personale che vi entra in contatto durante l'attività di riscossione ordinaria, o di qualunque altra attività nella quali si configuri un rischio di tale specie, nonché ad opera del personale addetto alla cassa centrale quale, a titolo esemplificativo, l'utilizzo di strumenti idonei al riconoscimento delle banconote contraffatte e la previsione di utilizzo obbligatorio di tali strumenti per le banconote di taglio pari o superiore a 50€. In caso di identificazione di una banconota falsa è tenuta traccia della provenienza e ne è dato immediato avviso sia all'autorità competente che all'OdV;
- e) **Controlli periodici** prescritti dalle procedure di produzione descritte dal manuale qualità.

## 3. Controlli dell'Organismo di Vigilanza

L'OdV, al fine di verificare il rispetto del modello e delle procedure adottate dalla Società, analizza le segnalazioni di presunte violazioni eventualmente ricevute, soprattutto con specifico riferimento al rinvenimento di banconote o bolli falsi. In tal caso l'OdV effettuerà un'ulteriore verifica circa la provenienza di dette banconote o bolli, redigendo apposito verbale e/o *report* di verifica. Può inoltre effettuare controlli a campione con riferimento alla gestione della cassa.

A tal fine all'OdV viene garantito libero accesso a tutta la documentazione aziendale necessaria allo svolgimento delle verifiche.

## SEZIONE G) - ALTRI REATI

### I. REATI CONTRO L'AMMINISTRAZIONE DELLA GIUSTIZIA

Il Decreto, all'art. 25-decies, inserisce fra i reati presupposto per i quali è ipotizzabile la responsabilità dell'Ente il reato di:

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

#### 1. Elenco delle fattispecie di reato ipotizzabili per processo sensibile

Tale reato può essere posto in essere da qualunque esponente della Società (dipendente e non) che, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, anche connessa alla carriera del dipendente o alla posizione del fornitore o dell'esponente dell'ente committente, induca a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata dinnanzi alla autorità giudiziaria a testimoniare nell'ambito di un procedimento penale o civile così da influenzarne il comportamento e ostacolare o turbare la ricerca della verità nel processo.

#### 2. Protocolli preventivi e Principi e regole di comportamento

Al fine di prevenire il verificarsi della fattispecie delittuosa sopra menzionata, oltre a quanto già descritto nella Parte Speciale relativa ai Reati contro la PA (Sezione A), in particolare con riferimento al **Processo Gestione Risorse Umane** e al **Processo Acquisti**, i cui protocolli preventivi sono da intendersi qua richiamati, la Società prevede per gli organi sociali, i dipendenti ed i collaboratori l'obbligo di:

evitare tassativamente contatti con soggetti che abbiano la veste di testimoni in cui è coinvolto la Società;

in evitare qualsiasi comportamento che abbia lo scopo o l'effetto di indurre un soggetto terzo a rilasciare false dichiarazioni, ovvero a non rilasciare dichiarazioni nell'ambito di un procedimento penale di competenza dell'Autorità Giudiziaria italiana o straniera;

mantenere un comportamento corretto, chiaro, trasparente, diligente e collaborativo con le Autorità Giudiziarie, alle quali devono essere tempestivamente comunicate tutte le informazioni, i dati e le notizie richiesti;

segnalare all'OdV, nel rispetto degli obblighi di riservatezza e dei divieti di divulgazione previsti dalle norme, la richiesta dell'Autorità Giudiziaria, italiana o straniera, di rendere o produrre dichiarazioni utilizzabili in un procedimento penale relative all'esercizio delle proprie funzioni.

#### 3. Controlli dell'Organismo di Vigilanza

In relazione all'osservanza del modello per quanto concerne le prescrizioni di cui alla presente sezione, l'OdV 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'OdV è garantito libero accesso a tutta la documentazione aziendale necessaria allo svolgimento delle verifiche, ivi compresa la documentazione relativa ai procedimenti giudiziari di cui l'Ente o gli esponenti dello stesso siano parte.

## II. DELITTI DI CRIMINALITA' ORGANIZZATA

L'art. 24-ter del D.Lgs 231/01 inserisce, tra i reati presupposto che concretano la responsabilità penale degli Enti, il reato di:

- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso (art. 416-bis c.p.)
- Scambio elettorale politico mafioso (art. 416-ter c.p.)

### 1. Elenco delle fattispecie di reato ipotizzabili per processo sensibile

Il reato di Associazione per delinquere (art. 416 c.p.) potrebbe configurarsi nel caso in cui tre o più persone si associno allo scopo di commettere più delitti, tra quelli mappati dalla presente matrice, rilevanti ai fini del D.Lgs. 231/01, ovvero anche al fine di commettere reati che non siano ricompresi nel catalogo dei reati presupposto dal D.Lgs. 231/01.

Il reato di Associazione di tipo mafioso (art. 416-bis c.p.) potrebbe configurarsi laddove dipendenti o soggetti apicali della Società, anche in concorso, si riuniscano in un'associazione che presenti le caratteristiche tipiche dell'associazione mafiosa e perciò la forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva, e in secondo luogo per ciò che concerne le finalità: il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici allo scopo di realizzare profitti ingiusti per la Società o per altri, ovvero al fine di impedire o ostacolare il libero esercizio del voto o di procurarne a sé o ad altri.

Il reato di Scambio elettorale politico mafioso (art. 416-ter c.p.) potrebbe configurarsi laddove dipendenti o soggetti apicali della Società accettino o promettano di procurare voti con le modalità di cui all'art. 416-bis c.p. e meglio esplicate nel punto che precede.

L'elemento che caratterizza le suddette fattispecie di reato è la creazione di un'organizzazione dotata di un vincolo associativo e di un programma criminoso. L'organizzazione ha come requisito indispensabile un vincolo continuativo, scaturente dalla consapevolezza di ciascun associato di far parte di un sodalizio criminale, e di un programma criminale duraturo.

L'associazione per delinquere si distingue dal concorso di persone nel reato continuato proprio per il modo di svolgersi dell'accordo criminoso, che nell'ipotesi in questione non avviene in via occasionale e limitata, bensì, essendo diretto all'attuazione di un vasto programma di criminalità, deve assumere un carattere permanente.

È da rilevare come tale delitto può realizzarsi in tutti i casi in cui tre o più persone si associno allo scopo di commettere più delitti, tra quelli mappati dalla presente matrice, rilevanti ai fini del D.Lgs. 231/01, ovvero

anche al fine di commettere reati che non siano ricompresi nel catalogo dei reati presupposto dal D.Lgs. 231/01.

Conseguentemente a quanto appena detto, appare chiaro come il rischio del verificarsi di tale fattispecie di reato possa configurarsi in tutti i processi e sottoprocessi aziendali, essendo sufficiente un'associazione di tre o più persone finalizzata allo scopo di commettere più delitti che comprendono la totalità di quelli mappati in matrice.

Non va trascurata anche l'ipotesi in cui l'organizzazione criminale sia composta solo in parte da apicali o dipendenti della Società (in ipotesi anche uno solo) e per la restante parte da soggetti esterni alla stessa.

## 2. Protocolli preventivi adottati

La Società, 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;
- Controlli sul rispetto delle procedure e delle deleghe;
- Formazione continua al personale;
- Previsione di regole di comportamento nel Codice Etico e verifica del rispetto delle stesse;
- 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 previa verifica dell'onorabilità degli stessi e secondo una comparazione obiettiva e trasparente delle offerte basata su criteri oggettivi documentabili.

## 3. Principi e regole di comportamento

Al fine di prevenire la commissione dei reati in trattazione, la Società impone:

a. l'OBBLIGO di:

osservare tutte le leggi e regolamenti che disciplinano le diverse attività svolte all'interno della Società 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.

b. il DIVIETO di:

ricevere danaro, doni o qualsiasi altra utilità ovvero accettarne la promessa, da chiunque sia o intenda entrare in rapporto con la Società 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 la Società 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 della Società.

#### 4. Controlli dell'Organismo di Vigilanza

In relazione all'osservanza del modello per quanto concerne le prescrizioni di cui alla presente sezione, l'OdV procede a:

- 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'OdV è garantito libero accesso a tutta la documentazione aziendale necessaria allo svolgimento delle verifiche, ivi compresa la documentazione relativa ai procedimenti giudiziari di cui l'Ente o gli esponenti dello stesso siano parte.

### III. REATI TRANSNAZIONALI

Lo stesso reato di cui al punto II. rileva ai fini 231 anche per quanto riguarda quel tipo di reati, i Reati transnazionali, nel compimento dei quali sono coinvolti soggetti operanti in più Stati. Tra di essi, disciplinati dall'art. 10 della l. 146/2006, rientrano:

- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso (art. 416-bis c.p.)
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377bis c.p.)
- Favoreggiamento personale (art. 378 c.p.)

#### 1. Elenco delle fattispecie di reato ipotizzabili per processo sensibile

Il reato di Associazione per delinquere (art. 416 c.p.), come già precedentemente analizzato, potrebbe configurarsi nel caso in cui tre o più persone si associno allo scopo di commettere più delitti, tra quelli mappati dalla presente matrice, rilevanti ai fini del D.Lgs. 231/01, ovvero anche al fine di commettere reati che non siano ricompresi nel catalogo dei reati presupposto dal D.Lgs. 231/01.

Il reato di Associazione di tipo mafioso (art. 416-bis c.p.) potrebbe configurarsi laddove dipendenti o soggetti apicali della Società, anche in concorso, si riuniscano in un'associazione che presenti le caratteristiche tipiche dell'associazione mafiosa e perciò la forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva, e in secondo luogo per ciò che concerne le finalità: il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici allo scopo di realizzare profitti ingiusti per la Società o per altri, ovvero al fine di impedire o ostacolare il libero esercizio del voto o di procurarne a sé o ad altri.

Il reato di Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377bis c.p.), come già precedentemente analizzato, può essere posto in essere da qualunque esponente della Società (dipendente e non) che, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induca a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata dinnanzi alla autorità giudiziaria a testimoniare nell'ambito di un procedimento penale o civile così da influenzarne il comportamento e ostacolare o turbare la ricerca della verità nel processo;

Il reato di Favoreggiamento personale (art. 378 c.p.) potrebbe configurarsi nel caso in cui un dipendente o qualunque esponente della Società aiuti taluno a eludere le investigazioni delle Autorità o a sottrarsi alle ricerche della stessa, nei casi in cui fu commesso un delitto per il quale sia previsto l'ergastolo o la reclusione.

## 2. Protocolli preventivi

Presupposto necessario per la responsabilità della Società è che i suindicati reati vengano commessi in un contesto internazionale. Se ciò, in considerazione dell'attività svolta da Fraternità Sistemi, 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 protocolli preventivi debbano sostanzialmente coincidere con quelli previsti per le stesse fattispecie di reato commesse in ambito nazionale, cui si rimanda.

## 3. Principi e regole di comportamento

In base a quanto sostenuto poc'anzi, 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 societarie e del Codice Etico di Fraternità Sistemi.

## 4. Controlli dell'Organismo di Vigilanza

Anche con riferimento ai controlli da parte dell'OdV, 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'OdV è garantito libero accesso a tutta la documentazione aziendale necessaria allo svolgimento delle verifiche, ivi compresa la documentazione relativa ai procedimenti giudiziari di cui l'Ente o gli esponenti dello stesso siano parte.

## IV. IMPIEGO DI LAVORATORI IRREGOLARI

L'art. 25-duodecies del D.Lgs. 231/01 inserisce, tra i reati presupposto che concretano la responsabilità penale degli Enti e delle Società, il reato di:

- Impiego di lavoratori irregolari (art. 22, c. 12-bis, D.Lgs. 286/1998)

### 1. Elenco delle fattispecie di reato ipotizzabili per processo sensibile

Il reato di Impiego di lavoratori irregolari (art. 22, c. 12-bis, D.Lgs. 286/1998) potrebbe in concreto configurarsi laddove la Società 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 della Società, ma che potrebbero rivendicare l'accertamento e/o la costituzione del rapporto di lavoro (ad es. somministrazioni irregolari e altre ipotesi previste dalla legge).

### 2. Protocolli preventivi adottati e Principi e regole di comportamento

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 della Società in osservanza dei protocolli preventivi in materia di Gestione delle Risorse Umane previsti alla Sezione A), a cui si rinvia;

nell'ambito delle stesse procedure di cui al punto che precede, verificare la regolarità della documentazione dei candidati;

laddove la Società impieghi personale straniero, verificare all'atto dell'assunzione e con cadenza almeno annuale il possesso di titolo in corso di validità per l'ingresso o la permanenza sul territorio

dello Stato e laddove il dipendente si rifiuti di fornire tale documentazione procedere alla risoluzione del rapporto;  
acquisire da parte delle ditte appaltatrici di FS apposita dichiarazione e documentazione comprovante il possesso da parte dei dipendenti di queste che operano sulla commessa di FS, di valido titolo per la permanenza sul territorio dello Stato.

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 della Società 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 aziendali nonché i principi di cui al presente Modello.

### **3. Controlli dell'Organismo di Vigilanza**

L'OdV, nell'ambito delle attività di verifica finalizzate alla prevenzione del reato di cui alla presente sezione promuove una serie di verifiche a campione anche mediante sopralluoghi presso la sede della Società, e verifica documentale a campione dei titoli legittimanti il soggiorno sul territorio dello Stato dei dipendenti di FS ed ha accesso a tutta la documentazione aziendale necessaria.