Modello di Organizzazione, Gestione e Controllo ai sensi del Decreto Legislativo 231/01 della "S.R.T. - Società pubblica per il recupero ed il trattamento dei rifiuti S.p.a."

- Parte Speciale E -

Altri Reati

(articoli 24-bis, 24–ter, 25-bis, 25-octies, 25-octies.1, 25-decies, 25-septiesdecies e 25-duodevicies del D.lgs. 231/2001)

Approvato con Delibera del Consiglio di Amministrazione in data 25/01/2024

Sommario

Altre tipologie di reati (Artt. 24-bis, 24–ter, 25-bis, 25-octies, 25-octies.1, 25-decies, 25-septiesdecies e 25-duodevicies del D.lgs. 231/2001)

La presente Parte Speciale comprende le sotto elencate altre tipologie di reati presupposto ex D.lgs. 231/2001 non inerenti alle precedenti Parti Speciali, riconducibili alla specifica attività svolta dalla Società:

- ✓ reati informatici e il trattamento illecito dei dati (articolo 24-bis del D.lgs. 231/2001);
- ✓ reati connessi alla criminalità organizzata (articolo 24–ter del D.lgs. 231/2001);
- ✓ reati in tema di falsità in monete, carte di pubblico credito e valori di bollo (articolo 25-bis del D.lgs. 231/2001);
- ✓ i reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio (articolo 25-octies del D.lgs. 231/2001);
- ✓ reati in materia di strumenti di pagamento diversi dai contanti (articolo 25-octies.1 del D.lgs. 231/01);
- ✓ reati contro l'amministrazione della giustizia (articolo 25-decies del D.lgs. 231/2001);
- ✓ reati i contro il patrimonio culturale (articolo 25-septiesdecies del D.lgs. 231/01);
- ✓ reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (articolo 25-duodevicies del D.lgs. 231/01).

Reati informatici e trattamento illecito dei dati. Aree di attività a Rischio e modalità di gestione e controllo.

L'art. 24-bis del D. Lgs. 231/01: "**Delitti informatici e trattamento illecito di dati**", introdotto dalla Legge 18 marzo 2008 n.48 art.7 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno", prevede i seguenti reati presupposto ritenuti applicabili alla Società, rimandando all'allegato Risk Assessment per l'elenco completo dei reati previsti dall'art. 24-bis Decreto.

- **Falsità in un documento informatico pubblico o privato avente efficacia probatoria (art. 491 - bis c.p.).**

Il reato si configura nei casi in cui si riscontrino ipotesi di falsità, materiale o ideologica, commesse su atti pubblici qualora le stesse abbiano ad oggetto un "documento informatico avente efficacia probatoria".
In relazione alla commissione di tali delitti si applica all´ente la sanzione pecuniaria sino a quattrocento quote.

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

Commette il delitto chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.
In relazione alla commissione di tali delitti si applica all´ente la sanzione pecuniaria da cento a cinquecento quote.

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

Commette il delitto chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo.
In relazione alla commissione di tali delitti si applica all´ente la sanzione pecuniaria da cento a cinquecento quote.

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

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
In relazione alla commissione di tali delitti si applica all´ente la sanzione pecuniaria da cento a cinquecento quote.

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

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.
In relazione alla commissione di tali delitti si applica all´ente la sanzione pecuniaria da cento a cinquecento quote.

- **Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies, co.3, c.p.)**

Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.
In relazione alla commissione di tali delitti si applica all´ente la sanzione pecuniaria da cento a cinquecento quote.
L'analisi dei processi aziendali ha consentito di individuare le attività "sensibili" nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24-bis (Delitti informatici e di trattamento illecito di dati) del D.Lgs. n. 231/2001, ritenute rilevanti per la Società:

AREE DI RISCHIO:

A. **Gestione dei profili utente e del processo di autenticazione**: attività relative alla gestione della sicurezza degli accessi agli applicativi ed alle risorse informatiche sia da parte degli utenti della Società in relazione ai ruoli ricoperti dagli stessi sia da parte degli utenti esterni, per i quali è previsto l'utilizzo di meccanismi di autenticazione sicuri e protetti con protocolli di sicurezza. La gestione dei profili utenti è attuata attraverso elementi identificativi (user id e password) e procedure di accesso.

B. **Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio:** modalità operative seguite per la gestione di documenti elettronici aziendali, pubblici o privati, con finalità probatoria in modo che siano monitorati gli stati di utilizzo, modifica ed archiviazione dei documenti.

C. **Gestione e protezione della postazione di lavoro**: attività di gestione, protezione e monitoraggio delle postazioni di lavoro con riferimento alla definizione di regole operative e comportamentali circa le modalità di corretto utilizzo dei beni aziendali, della posta elettronica e della sicurezza informatica.

D. **Gestione degli accessi da e verso l'esterno**: attività di gestione degli accessi agli oggetti (applicazioni, dati, programmi) mediante operazioni (lettura, aggiornamento, esecuzione) da parte degli utenti.

E. **Gestione e protezione delle reti:** attività di definizione e documentazione, monitoraggio e gestione della rete anche con riferimento agli accessi sui server, sui firewall e sui router.

F. **Sicurezza fisica**: attività di gestione e di controllo della sicurezza fisica degli ambienti e delle risorse che vi operano (es. misure per la protezione degli apparati dai furti).

G. **Sicurezza logica dei dati:** salvaguardia della riservatezza, integrità e disponibilità di dati e informazioni memorizzati su supporti di varia natura e/o trasmessi attraverso canali di comunicazione.

MODALITA' DI GESTIONE E CONTROLLO:

A. **Gestione dei profili utente e del processo di autenticazione**: con riferimento alle attività relative alla gestione della sicurezza degli accessi agli applicativi ed alle risorse informatiche sia da parte degli utenti della Società in relazione ai ruoli ricoperti dagli stessi sia da parte degli utenti esterni, SRT S.p.A. intende sviluppare idonea procedura che garantisca la piena sicurezza e siano rispettate le seguenti MODALITA' DI GESTIONE E CONTROLLO:

   - utilizzo di meccanismi di autenticazione sicuri e protetti con protocolli di sicurezza.
   - gestione dei profili utenti attraverso elementi identificativi (user id e password) e procedure di accesso.
   - adozione di idonei controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature.

B. **Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio:** modalità operative seguite per la gestione di documenti elettronici aziendali, pubblici o privati, con finalità probatoria in modo che siano monitorati gli stati di utilizzo, modifica ed archiviazione dei documenti. SRT S.p.A. intende sviluppare idonea procedura che garantisca la piena sicurezza e siano rispettate le seguenti MODALITA' DI GESTIONE E CONTROLLO:

   - adozione e attuazione di uno strumento normativo che assicuri la correttezza e la sicurezza dell'operatività dei sistemi informativi.
   - il corretto e sicuro funzionamento degli elaboratori di informazioni;
   - la protezione da software pericoloso;
   - il back-up di informazioni e software;
   - la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;

C. **Gestione e protezione della postazione di lavoro:** attività di gestione, protezione e monitoraggio delle postazioni di lavoro con riferimento alla definizione di regole operative e comportamentali circa le modalità di corretto utilizzo dei beni aziendali, della posta elettronica e della sicurezza informatica. SRT S.p.A. intende sviluppare idonea procedura che garantisca la piena sicurezza e siano rispettate le seguenti MODALITA' DI GESTIONE E CONTROLLO:

- attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;
- destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta.
- adeguata formazione sull'utilizzo della posta elettronica e sulla sicurezza informatica.

D. **Gestione degli accessi da e verso l'esterno:** attività di gestione degli accessi agli oggetti (applicazioni, dati, programmi) mediante operazioni (lettura, aggiornamento, esecuzione) da parte degli utenti. SRT S.p.A. intende sviluppare idonea procedura che garantisca la piena sicurezza e siano rispettate le seguenti MODALITA' DI GESTIONE E CONTROLLO:

   - l'autenticazione individuale degli utenti tramite codice identificativo dell'utente password o altro sistema di autenticazione sicura;

E. **Gestione e protezione delle reti:** attività di definizione e documentazione, monitoraggio e gestione della rete anche con riferimento agli accessi sui server, sui firewall e sui router. SRT S.p.A. intende sviluppare idonea procedura che garantisca la piena sicurezza e siano rispettate le seguenti MODALITA' DI GESTIONE E CONTROLLO:

   - stipula di un contratto con società di provata esperienza per lo svolgimento delle attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso;
   - specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;
   - monitoraggio e gestione della rete anche con riferimento agli accessi sui server, sui firewall e sui router.

F. **Sicurezza fisica**: attività di gestione e di controllo della sicurezza fisica degli ambienti e delle risorse che vi operano (es. misure per la protezione degli apparati dai furti). SRT S.p.A. intende sviluppare idonea procedura che garantisca la piena sicurezza e siano rispettate le seguenti MODALITA' DI GESTIONE E CONTROLLO:

   - stipula di un contratto con società di provata esperienza per l'incarico di videosorveglianza dei beni mobili ed immobili della società.

G. **Sicurezza logica dei dati:** salvaguardia della riservatezza, integrità e disponibilità di dati e informazioni memorizzati su supporti di varia natura e/o trasmessi attraverso canali di comunicazione. SRT S.p.A. intende sviluppare idonea procedura che garantisca la piena sicurezza e siano rispettate le seguenti MODALITA' DI GESTIONE E CONTROLLO:

   - stipula di un contratto con società di provata esperienza per lo svolgimento delle attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso;
   - l'autenticazione individuale degli utenti tramite codice identificativo dell'utente password o altro sistema di autenticazione sicura;
   - attuazione di uno strumento che definisca adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica.

Per la corretta gestione degli adempimenti relativi ai "Reati informatici e trattamento illecito dei dati" ed alla sicurezza informatica ai fini della *Compliance* 231:

- la Società ha sottoscritto un contratto di assistenza in ambito privacy e sicurezza informatica;
- è stato avviato un processo di adeguamento a quanto previsto dal Regolamento UE 2016/679 (GDPR);

- i controlli che vengono posti in essere sono effettuati secondo gli standard previsti dalle certificazioni ISO 27001 e 27002;
- la Società ha provveduto a nominare un Amministratore di Sistema per implementare il sistema IT;
- è stato adottato un modello di organizzazione della privacy;
- viene effettuata un'analisi annuale dei rischi informatici relativi al trattamento dei dati personali;
- la Società è dotata di un organigramma della privacy e dei Registri delle attività di trattamento;
- vengono effettuati i back up dei dati, nonché le prove di *disaster recovery* e ogni sei mesi viene richiesta la modifica delle password;
- la Società ha istituito delle VPN controllate e distribuito al personale che opera in *smart working* delle policy sul corretto e sicuro utilizzo dei dispositivi informatici;
- viene effettuata periodicamente formazione in materia di sicurezza informatica, sia in presenza che a distanza;
- non si sono verificati incidenti di sicurezza informatica;
- la Società non aveva nominato un DPO in quanto inizialmente non soggetta a tale obbligo. A seguito del mutamento di interpretazione della normativa in materia, che ha individuato quali soggetti tenuti all'obbligo gli "organismi di diritto pubblico", la Società ha provveduto a nominare un DPO, con decorrenza 1/1/2023.

Delitti di criminalità organizzata.
Aree di attività a Rischio e modalità di gestione e controllo.

L'art. 24-ter del D. Lgs. 231/01: "**Delitti di criminalità organizzata**", introdotto dalla Legge 15 luglio 2009, n. 94, art. 2, co. 29: "Disposizioni in materia di sicurezza pubblica", prevede i seguenti reati presupposto ritenuti applicabili alla Società, rimandando all'allegato Risk Assessment per l'elenco completo dei reati previsti dall'art. 24-ter Decreto.

- **Associazione per delinquere (art. 416 c.p.).**

La fattispecie di delitto in esame si realizza quando tre o più persone si associano allo scopo di commettere più delitti. L'art. 416 c.p. punisce coloro che promuovono o costituiscono od organizzano l'associazione con la reclusione da tre a sette anni.
Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni. I capi soggiacciono alla stessa pena stabilita per i promotori.
Se gli associati scorrono in armi le campagne o le pubbliche vie, si applica la reclusione da cinque a quindici anni. La pena è aumentata se il numero degli associati è di dieci o più.

1. In relazione alla commissione di taluno dei delitti di cui agli articoli 416, sesto comma, 416-bis, 416-ter e 630 del codice penale, ai delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-bis ovvero al fine di agevolare l´attività delle associazioni previste dallo stesso articolo, nonché ai delitti previsti dall´articolo74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, si applica la sanzione pecuniaria da quattrocento a mille quote.
2. In relazione alla commissione di taluno dei delitti di cui all´articolo 416 del codice penale, ad esclusione del sesto comma, ovvero di cui all´articolo 407, comma 2, lettera a), numero 5), del codice di procedura penale, si applicala sanzione pecuniaria da trecento a ottocento quote.
3. Nei casi di condanna per uno dei delitti indicati nei commi 1 e 2, si applicano le sanzioni interdittive previste dall´articolo 9, comma 2, per una durata non inferiore ad un anno.
4. Se l´ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati nei commi 1 e 2, si applica la sanzione dell´interdizione definitiva dall´esercizio dell´attività ai sensi dell´articolo 16, comma 3.

L'analisi dei processi aziendali, ha consentito di individuare le attività "sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24-ter (Delitti di criminalità organizzata) del D.Lgs. n. 231/2001, ritenute rilevanti per la Società:

AREE DI RISCHIO:

A. Gestione dei rapporti societari o di impresa con interlocutori terzi pubblici e/o privati nel processo di gestione della società.

MODALITA' DI GESTIONE E CONTROLLO:

Con riferimento alle attività relative alla gestione dei rapporti societari o di impresa con interlocutori terzi pubblici e/o privati nel processo di gestione della società, poiché il rischio si ritiene applicabile a tutte le attività della società e coinvolge tutte le funzioni aziendali, le MODALITA' DI GESTIONE E CONTROLLO si sostanziano nell'attuazione da parte di tutti gli esponenti aziendali, ciascuno per gli aspetti di propria competenza, di comportamenti conformi al contenuto dei seguenti protocolli di prevenzione adottati dalla società:

- Principi di comportamento individuati nel Codice Etico;
- Procedure aziendali per l'accesso ai servizi di trattamento, recupero e smaltimento dei rifiuti;
- Sistema di Gestione Ambiente e Qualità;
- "Regolamento riguardante le modalità di svolgimento del servizio di smaltimento, trattamento e recupero dei rifiuti";
- "Regolamento interno per il reclutamento e le progressioni di carriera del personale";
- "Linee Guida per l'affidamento dei lavori, delle forniture e dei servizi inferiori alla soglia di rilevanza comunitaria";
- Ordini di Servizio specifici;
- Definizione di poteri e responsabilità già riconosciuti all'interno dell'organizzazione, in coerenza con le responsabilità organizzative assegnate ed attuazione del principio della segregazione delle funzioni.

Reati di falso nummario.
Aree di attività a Rischio e modalità di gestione e controllo.

L'art. 25-bis del D. Lgs. 231/01: "**Reati di falso nummario**", ossia "Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento." In relazione alla commissione dei delitti previsti dal c.p. in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento... ...come modificato dalla L. 99/2009, art.15, co.7 "Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia", prevede i seguenti reati presupposto ritenuti applicabili alla Società, rimandando all'allegato Risk Assessment per l'elenco completo dei reati previsti dall'art. 25-bis Decreto.

- **Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.)**

Le disposizioni degli articoli 453, 455 e 457 del c.p. si applicano anche alla contraffazione o alterazione di valori di bollo e alla introduzione nel territorio dello Stato, o all'acquisto, detenzione e messa in circolazione di valori di bollo contraffatti; ma le pene sono ridotte di un terzo.
Agli effetti della legge penale, s'intendono per valori di bollo la carta bollata, le marche da bollo, i francobolli e gli altri valori equiparati a questi da leggi speciali.

- **Uso di valori di bollo contraffatti o alterati (art. 464, co. 1 e 2, c.p.).**

Chiunque, non essendo concorso nella contraffazione o nell'alterazione, fa uso di valori di bollo [459] contraffatti o alterati, è punito con la reclusione fino a tre anni e con la multa fino a euro 516.

Se i valori sono stati ricevuti in buona fede, si applica la pena stabilita nell'articolo 457, ridotta di un terzo.
L'analisi dei processi aziendali, ha consentito di individuare le attività "sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25-bis (Falsità in monete, carte di pubblico credito e valori di bollo) del D.Lgs. n. 231/2001, ritenute rilevanti per la Società:

AREE DI RISCHIO:

A. Gestione delle attività che prevedono l'acquisto e la gestione di valori bollati nei processi aziendali.

MODALITA' DI GESTIONE E CONTROLLO:

In relazione alle attività che prevedono l'acquisto e la gestione di valori bollati nei processi aziendali, SRT prevede le seguenti MODALITA' di GESTIONE e CONTROLLO:

1. l'acquisto e la gestione di valori bollati nei processi aziendali è affidata Responsabile Ufficio Contabilità - Bilancio – Cassa (RUB) tramite la Gestione del servizio di cassa;
2. gli acquisti dei valori bollati vengono effettuati previa predisposizione di apposita distinta che viene timbrata e sottoscritta dal rivenditore ed annotata sul registro di cassa; l'utilizzo dei valori bollati viene debitamente motivato allegando il relativo giustificativo;
3. la relativa spesa viene approvata e liquidata dal Direttore Generale e rendicontata mensilmente al Consiglio di Amministrazione.

Reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio. Aree di attività a Rischio e modalità di gestione e controllo.

L'art. 25-octies del D. Lgs. 231/01: "**Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita**", ...introdotto dal D.Lgs. 21 novembre 2007, n. 231 art.63 "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione e successive modificazioni e integrazioni", prevede i seguenti reati presupposto ritenuti applicabili alla Società, rimandando all'allegato Risk Assessment per l'elenco completo dei reati previsti dall'art. 25- octies del Decreto.

- **Ricettazione (art. 648 c.p.)**

L'art. 648 c.p. incrimina chi, al fine di procurare a sé o ad altri un profitto, "fuori dei casi di concorso nel reato, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare".
Per acquisto dovrebbe intendersi l'effetto di un'attività negoziale, a titolo gratuito od oneroso, mediante la quale l'agente consegue il possesso del bene.
Il termine ricevere starebbe ad indicare ogni forma di conseguimento del possesso del bene proveniente dal delitto, anche se solo temporaneamente o per mera compiacenza.
Per occultamento dovrebbe intendersi il nascondimento del bene, dopo averlo ricevuto, proveniente dal delitto.
La ricettazione può realizzarsi anche mediante l'intromissione nell'acquisto, nella ricezione o nell'occultamento della cosa. Tale condotta si esteriorizza in ogni attività di mediazione, da non intendersi in senso civilistico (come precisato dalla giurisprudenza), tra l'autore del reato principale e il terzo acquirente.

L'ultimo comma dell'art. 648 c.p. estende la punibilità "anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto".
Lo scopo dell'incriminazione della ricettazione è quello di impedire il perpetrarsi della lesione di interessi patrimoniali iniziata con la consumazione del reato principale. Ulteriore obiettivo della incriminazione consiste nell'evitare la commissione dei reati principali, come conseguenza dei limiti posti alla circolazione dei beni provenienti dai reati medesimi.

- **Riciclaggio (art. 648-bis c.p.)**

Tale reato consiste nel fatto di chiunque "fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa". Il delitto in esame sussiste anche quando l'autore del delitto da cui il denaro o le cose provengono, sia non imputabile o non punibile, o quando manchi una condizione di procedibilità riferita a tale delitto. È necessario che antecedentemente ad esso sia stato commesso un delitto non colposo al quale, però, il riciclatore non abbia partecipato a titolo di concorso.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale ed è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni.

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

È il reato commesso da "chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli artt. 648 c.p. (Ricettazione) e 648-bis c.p. (Riciclaggio), impiega in attività economiche o finanziarie denaro o beni o altre utilità provenienti da delitto".

Anche in questa fattispecie, è prevista la circostanza aggravante dell'esercizio di un'attività professionale ed è esteso ai soggetti l'ultimo comma dell'art. 648, ma la pena è diminuita se il fatto è di particolare tenuità.

Il riferimento specifico al termine "impiegare", di accezione più ampia rispetto a "investire" che suppone un impiego finalizzato a particolari obiettivi, esprime il significato di "usare comunque". Il richiamo al concetto di "attività" per indicare il settore di investimento (economia o finanza) consente viceversa di escludere gli impieghi di denaro od altre utilità che abbiano carattere occasionale o sporadico.

La specificità del reato rispetto a quello di riciclaggio risiede nella finalità di far perdere le tracce della provenienza illecita di denaro, beni o altre utilità, perseguita mediante l'impiego di dette risorse in attività economiche o finanziarie.

Il legislatore ha inteso punire quelle attività mediate che, a differenza del riciclaggio, non sostituiscono immediatamente i beni provenienti da delitto, ma che comunque contribuiscono alla "ripulitura" dei capitali illeciti.

- **Autoriciclaggio (art. 648-ter.1 c.p.)**

Questo reato del C.P., entrato in vigore il 01/01/2015, ha lo scopo di perseguire le attività di chiunque interagisca per "pulire" danaro, beni o altra utilità provenienti da attività delittuose non colpose, trasformandole in lecite, per rendere difficile la conoscenza della loro origine illecita.

Costituisce quindi di fatto una ulteriore e altra attività successiva alla commissione del delitto non colposo, ancorché a questo collegato e strumentale. Trattasi di reato comune, infatti può essere commesso da chiunque, il quale, oltre ad aver commesso il delitto doloso, svolge l'ulteriore attività di "pulire" il profitto illecito per occultarne "concretamente" la provenienza.

La fattispecie del reato prevede dunque il reimpiego in attività economiche o finanziarie del denaro, dei beni e delle utilità provenienti da delitto.

Si ritiene che le condotte previste dal reato precedentemente presentato che siano in astratto realizzabili nell'ambito della Società, vista la natura "in house", in quanto qualsiasi risorsa che derivi dalla commissione di un eventuale delitto nell'attività della società non può che essere reimpiegato nell'attività della società stessa.

La prevenzione del reato specifico di autoriciclaggio si realizza mediante la prevenzione dei reati che possano generare risorse illecite e quindi attuando le misure già previste per gli altri reati presupposto.

L'analisi dei processi aziendali, ha consentito di individuare le attività "sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25-octies (Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita) del D.Lgs. n. 231/2001, ritenute rilevanti per la Società:

AREE DI RISCHIO:

A. **Gestione della fiscalità aziendale:** attività relative alla gestione degli adempimenti connessi ad imposte dirette e imposte indirette con particolare riferimento alle seguenti:
   a) monitoraggio della normativa fiscale rilevante;
   b) compilazione, tenuta e conservazione dei registri rilevanti ai fini fiscali e degli altri documenti di cui è obbligatoria la conservazione;
   c) monitoraggio delle scadenze fiscali;
   d) predisposizione di dichiarazioni e comunicazioni fiscali, liquidazione e versamento delle imposte.

B. Tenuta della contabilità, redazione del bilancio di esercizio, di relazioni e comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori in base alla normativa vigente: attività finalizzate alla rilevazione, registrazione e rappresentazione dell'attività d'impresa nelle scritture contabili, alla redazione ed all'emissione del bilancio civilistico della Società, delle relazioni e di qualsiasi altro prospetto relativo alla situazione economica, patrimoniale e finanziaria della Società richiesto da disposizioni di legge, con particolare riferimento alle attività di:
   a) gestione dei rapporti amministrativi con i terzi (clienti, fornitori) e relativa gestione contabile delle partite di debito/credito;
   b) gestione amministrativa e contabile delle partecipazioni, dei cespiti e delle ulteriori immobilizzazioni;
   c) accertamenti di tutti gli altri fatti amministrativi in corso d'anno (costi del personale, penalità contrattuali, finanziamenti attivi e passivi e relativi interessi, ecc.);
   d) processi estimativi, quantificazione delle poste valutative e fondi rischi e oneri;
   e) documentazione, archiviazione e conservazione delle scritture contabili e dell'ulteriore documentazione relativa all'attività di impresa di cui è obbligatoria la conservazione in adempimento alle normative vigenti.

C. Gestione degli approvvigionamenti e delle consulenze: ossia l'attività di selezione e di gestione in generale del processo di *procurement* relativamente a beni e servizi, consulenze e prestazioni professionali.

MODALITA' DI GESTIONE E CONTROLLO:

A. Gestione della fiscalità aziendale: con riferimento alla gestione della fiscalità aziendale, l'attività sensibile in esame viene svolta nel rispetto degli standard di controllo previsti per l'attività sensibile "*Gestione dei rapporti con funzionari pubblici nell'ambito delle attività di verifica ispettiva e di controllo effettuate dalla Pubblica Amministrazione*" individuati nella "Parte Speciale B - Reati Societari" alla quale si rimanda.

Valgono inoltre i seguenti principi comportamentali a presidio dei rischi in oggetto:

a) il personale a qualsiasi titolo coinvolto negli adempimenti fiscali è tenuto a:
   - garantire l'attuazione del principio di segregazione dei ruoli tra le attività di gestione delle contabilità aziendale e la successiva trasposizione nelle dichiarazioni tributarie, tra le attività di determinazione delle imposte, effettuazione delle scritture contabili e versamento delle imposte dovute;
   - custodire in modo corretto ed ordinato le scritture contabili e gli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali;
   - rispettare i termini e le modalità previsti dalla normativa applicabile per la predisposizione delle dichiarazioni/ certificazioni e il conseguente versamento all'Agenzia delle Entrate.

b) si applicano inoltre i seguenti divieti nello svolgimento delle attività in oggetto:
   - omettere di presentare le dichiarazioni previste dalla normativa di riferimento;
   - indicare nelle dichiarazioni elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi, avvalendosi a titolo esemplificativo di fatture o altri documenti per operazioni inesistenti;
   - omettere il versamento delle imposte dovute;
   - occultare o distruggere le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi, del volume di affari o di altri elementi economico / patrimoniali rilevanti ai fini della determinazione delle imposte.

Infine, per ulteriore indicazione degli standard di controllo applicabili, si rimanda a quanto previsto nella "Parte Speciale B - Reati Tributari" alla quale si rimanda.

B. Tenuta della contabilità, redazione del bilancio di esercizio, di relazioni e comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori in base alla normativa vigente. L'attività sensibile in esame viene svolta nel rispetto degli standard di controllo previsti per l'attività sensibile "*Tenuta della contabilità, redazione del bilancio di esercizio, di relazioni e comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori in base alla normativa vigente*" individuati nella "Parte Speciale B - Reati societari" alla quale si rimanda.

C. Gestione degli approvvigionamenti e delle consulenze L'attività sensibile in esame viene svolta nel rispetto degli standard di controllo previsti per l'attività sensibile "*Gestione degli approvvigionamenti e delle consulenze*" individuati nella "Parte Speciale A - Reati nei rapporti con la Pubblica Amministrazione" alla quale si rimanda.

Reati in materia di strumenti di pagamento diversi dai contanti. Aree di attività a Rischio e modalità di gestione e controllo.

L'art. 25-octies.1 del D. Lgs. 231/01: "Delitti in materia di strumenti di pagamento diversi dai contanti", introdotto dal D.Lgs. 8 novembre 2021, n. 184 "*Attuazione della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti*", e dalla Legge 9 ottobre 2023, n. 137 "*Conversione in legge, con modificazioni, del decreto-legge 10 agosto 2023, n. 105, recante disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonchè in materia di personale della magistratura e della pubblica amministrazione*", prevede i seguenti reati presupposto, allocati in posizione di immediata contiguità e prosecuzione funzionale all'art. 25 octies, ritenuti applicabili alla Società, rimandando all'allegato Risk Assessment per l'elenco completo dei reati previsti dall'art. 25-octies.1 del Decreto.

- **Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (Art. 493-ter c.p.)**

Chiunque al fine di trarne profitto per sé o per altri**, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento**, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi o comunque ogni altro strumento di pagamento diverso dai contanti, è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. (sanzione pecuniaria tra 300 e 800 quote).

- **Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (Art. 493-quater c.p.)**

Salvo che il fatto costituisca più grave reato, chiunque, **al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici** che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo, è punito con la reclusione sino a due anni e la multa sino a 1000 euro (sanzione pecuniaria sino a 500 quote).

- **Frode informatica (Art. 640-ter c.p.)**

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da € 51 a € 1,032. La pena è della reclusione da uno a cinque anni e della multa da € 309 a € 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza prevista dall'art. 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età. (articolo modificato dal D.Lgs. 4/10/2022, n. 156).

- **Trasferimento fraudolento di valori (art. 512-bis c.p.)**

L'articolo 512-bis del codice penale, sanziona chi "attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648-bis e 648-ter", cioè dei delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita. La condotta sanzionata dall'articolo 512-bis è punita con la reclusione da due a sei anni.

Si ritiene che le condotte previste dal reato precedentemente presentato non siano neppure astrattamente realizzabili nell'ambito della Società e pertanto tale reato presupposto non verrà successivamente analizzato.

AREE DI RISCHIO:

A. **Gestione diretta o indiretta, degli strumenti di pagamento e dei movimenti monetari:** attività relative alla riscossione o al pagamento mediante strumenti di pagamento diversi dai contanti, come le quelle effettuate tramite i punti vendita che utilizzano dispositivi elettronici che consentono di effettuare pagamenti mediante moneta elettronica, carte di credito, di debito o prepagate.

B. **Falsificazione o utilizzo indebito di un dispositivo diverso dalla moneta a corso legale**, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali. Vi possono rientrare, ad esempio, monete elettroniche, valute virtuali, cripto valute, ma anche carte di credito/debito aziendali.

MODALITA' DI GESTIONE E CONTROLLO:

Valgono i seguenti principi comportamentali a presidio dei rischi in oggetto:

Il personale a qualsiasi titolo coinvolto nella gestione delle suddette attività è tenuto a:

- garantire l'attuazione del principio di segregazione dei ruoli tra le attività di gestione delle riscossioni e dei pagamenti;
- custodire i dispositivi di pagamento elettronico ed i relativi codici di accesso per la gestione delle transazioni;
- custodire in modo tracciabile e trasparente le relative scritture contabili e gli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali.

Reati contro l'amministrazione della giustizia. Aree di attività a Rischio e modalità di gestione e controllo.

L'art. 25-decies del D. Lgs. 231/01: "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" ...introdotto dalla Legge 3 agosto 2009, n. 116 art. 4 "Ratifica ed esecuzione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione, adottata dalla Assemblea generale dell'ONU il 31 ottobre 2003 con risoluzione n. 58/4, firmata dallo Stato italiano il 9 dicembre 2003, nonché norme di adeguamento interno e modifiche al codice penale e al codice di procedura penale", come sostituito dall'art. 2, comma 1, D.Lgs 7 luglio 2001, n. 121, prevede i seguenti reati presupposto ritenuti applicabili alla Società, rimandando all'allegato Risk Assessment per l'elenco completo dei reati previsti dall'art. 25-decies del Decreto.

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

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

L'analisi dei processi aziendali, ha consentito di individuare le attività "sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25-decies (Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria) del D.Lgs. n. 231/2001, ritenute rilevanti per la Società:

AREE DI RISCHIO:

A. Gestione dei rapporti con amministratori, dipendenti o terzi coinvolti in procedimenti giudiziari: attività inerenti la gestione dei rapporti e delle informazioni riguardanti amministratori, dipendenti o terzi coinvolti in procedimenti giudiziari in atto.

MODALITA' DI GESTIONE E CONTROLLO:

L'attività sensibile in esame rientra nel più ampio processo di gestione dei contenziosi giudiziali e stragiudiziali, ne consegue, pertanto, che viene svolta nel rispetto degli standard di controllo previsti per l'attività sensibile "Gestione dei contenziosi giudiziali e stragiudiziali" individuati nella "Parte Speciale A - Reati nei rapporti con la Pubblica Amministrazione" alla quale si rimanda.

A. **Gestione dei rapporti con amministratori, dipendenti o terzi coinvolti in procedimenti giudiziari:** Nella gestione delle attività inerenti la gestione dei rapporti e delle informazioni riguardanti amministratori, dipendenti o terzi coinvolti in procedimenti giudiziari in atto, SRT S.p.A. richiede ai Destinatari il rispetto delle seguenti MODALITA' DI GESTIONE E CONTROLLO:

- evadere con tempestività, correttezza e buona fede tutte le richieste provenienti dagli organi di polizia giudiziaria e dall'autorità giudiziaria inquirente e giudicante, fornendo tutte le informazioni, i dati e le notizie eventualmente utili;
- mantenere, nei confronti degli organi di polizia giudiziaria e dell'autorità giudiziaria un comportamento disponibile e collaborativo;
- garantire che la gestione dei rapporti con i Pubblici Ufficiali, ed in particolare con le autorità giudiziarie di qualsiasi ordine o grado, avvenga da parte dei soggetti responsabili identificati in possesso di una procura conferita dalla Società.

Reati contro il patrimonio culturale.
Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici.
Aree di attività a Rischio e modalità di gestione e controllo.

La Legge 9 marzo 2022 n. 22 “Disposizioni in materia di reati contro il patrimonio culturale” che inserisce all’interno del Codice Penale il Titolo VIIIbis “Dei delitti contro il patrimonio culturale”, ritenuti applicabili alla Società, rimandando all’allegato Risk Assessment per l’elenco completo dei reati previsti dagli artt. 25-septiesdecies (reati i contro il patrimonio culturale) e 25-duodevicies (reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici) del Decreto.

L’articolo 25-septiesdecies: “**Delitti contro il patrimonio culturale”** prevede in relazione:

- all’articolo 518-ter (appropriazione indebita di beni culturali), all’articolo 518-decies (importazione illecita di beni culturali) e all’articolo 518-undecies (uscita o esportazione illecite di beni culturali) l’applicazione della sanzione amministrativa pecuniaria da duecento a cinquecento quote;
- all’articolo 518-sexies c.p. (riciclaggio di beni culturali) l’applicazione della sanzione amministrativa pecuniaria da cinquecento a mille quote;
- all’articolo 518-duodecies (distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali e paesaggistici) e all’articolo 518-qua terdecies c.p. (contraffazione di opere d’arte) l’applicazione della sanzione amministrativa pecuniaria da trecento a settecento quote;
- all’articolo 518-bis (furto di beni culturali), all’articolo 518-quater (ricettazione di beni culturali) e all’articolo 518-octies (falsificazione in scrittura privata relativa a beni culturali) l’applicazione della sanzione amministrativa pecuniaria da quattro cento a novecento quote.

Nel caso di condanna per i delitti su elencati la nuova disposizione prevede l’applicazione all’ente delle sanzioni interdittive per una durata non superiore a due anni.

L’art. 25-duodevicies: “Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici”, che prevede in relazione:

- all’articolo 518-sexies (delitti di riciclaggio di beni culturali) e all’articolo 518--terdecies (devastazione e saccheggio di beni culturali e paesaggistici) l’applicazione all’ente della sanzione pecuniaria da cinquecento a mille quote. Nel caso in cui l’ente, o una sua unità organizzativa, venga stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di tali delitti, si applica la sanzione dell’interdizione definitiva dall’esercizio dell’attività (art 16, comma 3).

AREE DI RISCHIO:

A. Possibili rinvenimenti di beni culturali da parte del personale operativo nell’ambito delle attività inerenti la gestione ordinaria degli impianti di smaltimento e di valorizzazione dei rifiuti.

B. Attività di scavi e movimentazione terreno per la realizzazione di vasche di smaltimento o di altre opere pubbliche. Si rileva che la discarica di Tortona è situata nel “Parco naturale dello Scrivia”.

C. Ordinaria gestione degli impianti di smaltimento e di valorizzazione dei rifiuti.

MODALITA' DI GESTIONE E CONTROLLO:

A. **Delitti contro il patrimonio culturale derivanti da possibili rinvenimenti di beni culturali da parte del personale operativo erroneamente smaltiti o provenienti da delitti:** L'attività sensibile in esame rientra nel processo di gestione ordinaria degli impianti di smaltimento e di valorizzazione dei rifiuti. Nel rispetto degli standard di controllo previsti per l'attività sensibile "Reati contro il patrimonio culturale". Nella gestione delle suddette attività richiede ai Destinatari il rispetto delle seguenti MODALITA' DI GESTIONE E CONTROLLO:

- adeguata formazione al personale operativo addetto alla selezione e movimentazione dei rifiuti relativa al rinvenimento di potenziali beni culturali;
- rispetto delle prescrizioni contenute nelle autorizzazioni integrate ambientali;
- previsione, in fase di progettazione, della verifica preventiva dell'interesse archeologico, ai sensi dell'art. 25 del D.Lgs. n. 50/2016.

B. **Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici:** L'attività sensibile in esame rientra nel processo di gestione ordinaria e di realizzazione degli impianti di smaltimento dei rifiuti e di altre opera pubbliche. Nel rispetto degli standard di controllo previsti per l'attività sensibile "Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici". Nella gestione delle suddette attività richiede ai Destinatari il rispetto delle seguenti MODALITA' DI GESTIONE E CONTROLLO:

- adeguata formazione al personale operativo addetto alla selezione e movimentazione dei rifiuti relativa al rinvenimento di potenziali beni culturali;
- rispetto delle prescrizioni contenute nelle autorizzazioni integrate ambientali;
- previsione, in fase di progettazione, della verifica preventiva dell'interesse archeologico, ai sensi dell'art. 25 del D.Lgs. n. 50/2016.

Attraverso l'esecuzione di un processo di analisi e valutazione dei diversi fattori di rischio, si è ritenuto che la specifica attività svolta dalla Società non presenti profili di rischio tali da rendere ragionevolmente fondata la possibilità della commissione, nell'interesse o a vantaggio della stessa, dei seguenti reati:

- ✓ reati contro l'industria ed il commercio (articolo 25-bis.1 del D.lgs. 231/2001);
- ✓ i reati con finalità di terrorismo o di eversione dell'ordine democratico (articolo 25-quater del D.lgs. 231/2001);
- ✓ i reati consistenti in pratiche di mutilazione degli organi genitali femminili (articolo 25-quater.1 del D.lgs. 231/2001);
- ✓ i reati contro la personalità individuale (articolo 25-quinquies del D.lgs. 231/2001);
- ✓ i reati di abuso di informazioni privilegiate e manipolazione del mercato (articolo 25-sexies del D.lgs. 231/2001);
- ✓ reati in materia di violazione del diritto di autore (articolo 25-novies del D.lgs. 231/2001);
- ✓ reati in materia di immigrazione e condizione dello straniero (articolo 25–duodecies, del D.lgs. 231/01);
- ✓ reati di razzismo e xenofobia (articolo 25–terdecies, del D.lgs. 231/01);
- ✓ reato di contrabbando (articolo 25–sexiesdecies, del D.lgs. 231/01);
- ✓ reati commessi all'estero (c.d. transnazionali) (articolo 4, del D.lgs. 231/01).

Destinatari della Parte Speciale E

La presente Parte Speciale si riferisce a comportamenti posti in essere da amministratori, dirigenti e dipendenti ("Esponenti Aziendali") della Società operanti nelle aree di attività a rischio, nonché da Collaboratori Esterni e Partner, come già definiti nella Parte Generale (qui di seguito, tutti definiti i "Destinatari").

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

Principi generali di comportamento

I predetti Destinatari devono osservare, ciascuno per gli aspetti di propria competenza, i comportamenti conformi al contenuto dei seguenti protocolli di prevenzione adottati dalla società:

- Principi di comportamento individuati nel Codice Etico;
- Procedure aziendali per l'accesso ai servizi di trattamento, recupero e smaltimento dei rifiuti;
- Sistema di Gestione Ambiente e Qualità;
- "Regolamento riguardante le modalità di svolgimento del servizio di smaltimento, trattamento e recupero dei rifiuti";
- "Regolamento interno per il reclutamento e le progressioni di carriera del personale";
- "Linee Guida per l'affidamento dei lavori, delle forniture e dei servizi inferiori alla soglia di rilevanza comunitaria";
- Ordini di Servizio specifici;
- Definizione di poteri e responsabilità già riconosciuti all'interno dell'organizzazione, in coerenza con le responsabilità organizzative assegnate ed attuazione del principio della segregazione delle funzioni.

E' fatto espresso divieto a carico dei predetti Destinatari 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 previste di cui alla presente Parte Speciale E;
- espletare qualsiasi attività, anche tramite interposta persona, diretta ad influenzare l'indipendenza di giudizio o assicurare un qualsiasi vantaggio alla Società. In nessun caso il perseguimento dell'interesse o del vantaggio della Società può giustificare una condotta non onesta.