MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI ERP LUCCA SRL

ai sensi del decreto legislativo 8 Giugno 2001 n° 231

PARTE SPECIALE

Stato delle revisioni

Versione	Data	Descrizione	Approvazione
01	*14.12.20215*	Prima emissione	CDA delibera n.90
02	*24.04.20219*	Modifiche alla prima emissione	CDA delibera n.13
03	*31.03.2023*	Seconda emissione	CDA delibera n.15
04	*14.11.2025*	Terza emissione	CDA delibera n.35
05	*15.10.2026*	Quarta emissione	CDA delibera n.24
06	.....	.....	.....

Testo approvato dal C.d.A. con delibera n°24 del 15.10.2026.....

SOMMARIO

A. STRUTTURA DELLA PARTE SPECIALE..... 6

B. FINALITÀ DELLA PARTE SPECIALE..... 6

C. PRINCIPI GENERALI DEL SISTEMA DI CONTROLLO..... 8

C.1. ARTICOLAZIONE DEI POTERI E SISTEMA DELLE DELEGHE 8

C.1.1. Principi ispiratori del sistema di articolazione dei poteri delle deleghe 8

C.1.2. Il sistema dei poteri e delle deleghe 9

C.2. ALTRI PRINCIPI GENERALI DEL SISTEMA DI CONTROLLO 9

D. REATI PREUSPPOSTO DEL D.LGDS. N. 231/01 NON CONTEMPLATI DALLA PARTE SPECIALE..... 10

E. RACCORDO TRA MODELLO 231 E PIANO TRIENNALE PER LA PREVENZIONE DELLA CORRUZIONE (PTPCT) ex LEGE N. 190/12 11

SEZIONE 1: I REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE CORRUZIONE E CONCUSSIONE (ARTT. 24 E 25 DEL D.LGS.N.231/01) 12

1.1. ART. 24 – INDEBITA PERCEZIONE DI EROGAZIONI, TRUFFA IN DANNO DELLO STATO (...) 12

1.2. ART 25 – CONCUSSIONE E CORRUZIONE, INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ 13

1.3. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA 16

1.4. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE 19

1.4.1. Principi 19

1.4.2. Norme generali di comportamento 20

1.4.3. Presidi specifici relativi alla regolamentazione delle attività sensibili 21

1.5. I CONTROLLI DELL'ORGANISMO DI VIGILANZA 23

1.5.1. Flussi informativi verso l'organismo di vigilanza 24

SEZIONE 2: DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (ART. 24-BIS).....25

2. ART. 24-BIS – DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI 25

2.1. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS.N.231/01 25

2.2. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA 26
2.3. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE 29
2.3.1. Principi 29
2.3.2. Norme generali di comportamento 29
2.3.3. Presidi di riferimento specifici relativi alla regolamentazione delle attività sensibili 31
2.4. I CONTROLLI DELL'ORGANISMO DI VIGILANZA 34
2.4.1. Flussi informativi verso l'organismo di vigilanza 35
SEZIONE 3: REATI SOCIETARI (ART. 25-TER) 36
3. ART. 25-TER – REATI SOCIETARI 36
3.1. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS.N.231/01 36
3.2. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA 37
3.3. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE 39
3.3.1. Principi 39
3.3.2. Norme generali di comportamento 41
3.3.3. Presidi di riferimento specifici relativi alla regolamentazione delle attività sensibili 41
3.4. I CONTROLLI DELL'ORGANISMO DI VIGILANZA 42
3.4.1. Flussi informativi verso l'organismo di vigilanza 43
SEZIONE 4: REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME (ART. 25-SEPTIES) 44
4. ART. 25-SEPTIES – REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSI IN VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO 44
4.1. INTRODUZIONE E FUNZIONE DEL REATO DI OMICIDIO COLPOSO E LESIONI COLPOSE COMMESSE CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE 44
4.2. TERMINI E FIGURE RELATIVE ALLE NORME PER LA SALVAGUARDIA DELLA SALUTE E SICUREZZA SUL LAVORO. 47
4.3. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA 50
4.4. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE 51
4.4.1. Principi 51
4.4.2. Norme generali di comportamento 51
4.4.3. Presidi di riferimento specifici relativi alla regolamentazione delle attività sensibili 53
4.5. I CONTROLLI DELL'ORGANISMO DI VIGILANZA 55

4.5.1. Flussi informativi verso l'organismo di vigilanza 56

SEZIONE 5: RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO (ART. 25-OCTIES) 57

5. ART. 25-OCTIES – RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO. 57

5.1. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS.N.231/01 57

5.2. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA 57

5.3. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE 61

5.3.1. Principi 61

5.3.2. Norme generali di comportamento 62

5.3.3. Presidi di riferimento specifici relativi alla regolamentazione delle attività sensibili 63

5.4. I CONTROLLI DELL'ORGANISMO DI VIGILANZA 65

5.4.1. Flussi informativi verso l'organismo di vigilanza 65

SEZIONE 6: REATI AMBIENTALI (ART. 25-UNDECIES 67

6. ART. 25-UNDECIES – REATI AMBIENTALI 67

6.1. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS.N.231/01 67

6.2. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA 69

6.3. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE 75

6.3.1. Principi 75

6.3.2. Norme generali di comportamento 76

6.3.3. Presidi di riferimento specifici relativi alla regolamentazione delle attività sensibili 78

6.4. I CONTROLLI DELL'ORGANISMO DI VIGILANZA 80

6.4.1. Flussi informativi verso l'organismo di vigilanza 82

SEZIONE 7: REATI TRIBUTARI (ART. 25-QUINQUIESDECIES) 84

7. ART. 25-QUINQUIESDECIES – REATI TRIBUTATI 84

7.1. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS.N.231/01 84

7.1.1. Definizioni 84

7.1.2. Le fattispecie di reato 85

7.2. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA 97

7.3. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE 98

7.3.1. Principi 98

7.3.2. Norme generali di comportamento 99

7.3.3. Presidi di riferimento specifici relativi alla regolamentazione delle attività sensibili 102

7.3.3.1. IL SISTEMA DI PREVENZIONE DEI REATI TRIBUTARI 102

7.4. I CONTROLLI DELL'ORGANISMO DI VIGILANZA 104

7.4.1. Flussi informativi verso l'organismo di vigilanza..... 105

A. STRUTTURA DELLA PARTE SPECIALE

La presente Parte Speciale è composta da una parte preliminare dedicata ai principi generali del sistema di controllo e da singole sezioni dedicate alle categorie di reati presi in considerazione dal Decreto considerate sensibili dalla società a seguito di *gap-analisys*, contenenti l'individuazione delle aree di attività a rischio, i presidi per il contenimento del rischio entro soglie di accettabilità e le attività dell'OdV.

Le Sezioni che compongono la presente Parte Speciale sono le seguenti:

SEZIONE "1"	Reati commessi nei rapporti con la pubblica amministrazione, corruzione e concussione
SEZIONE "2"	Delitti informatici e trattamento illecito di dati
SEZIONE "3"	Reati societari
SEZIONE "4"	Reati di omicidio colposo e lesioni colpose gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro
SEZIONE "5"	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita- Autoriciclaggio
SEZIONE "6"	Reati ambientali
SEZIONE "7"	Reati Tributari

B. FINALITÀ DELLA PARTE SPECIALE

La Parte Speciale ha la finalità di definire linee, regole e principi di comportamento che tutti i destinatari del Modello 231 dovranno seguire al fine di prevenire, nell'ambito delle specifiche attività sensibili svolte nella società, la commissione di reati previsti dal Decreto e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Nello specifico, la Parte Speciale del Modello 231 ha lo scopo di:

- Indicare le modalità che gli esponenti aziendali sono chiamati ad osservare ai fini della corretta applicazione del Modello
- Fornire all'organismo di Vigilanza e ai responsabili delle altre funzioni aziendali che cooperano con esso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

- Provvede a fornire, inoltre, indicazioni riferite a ciascuna delle suddette categorie di reati, al fine di facilitare la comprensione delle attività e delle funzioni nell'ambito delle quali possono essere commessi i reati di cui al Decreto

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi ai contenuti dei seguenti documenti:

- Modello 231
- Codice Etico
- Procedure, protocolli e disposizioni
- Procure e deleghe
- Ordini di servizio
- Comunicazioni organizzative
- Sistemi di gestione delle problematiche di sicurezza e ambientali
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto

È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge.
Obiettivo della presente Parte Speciale è che tutti i destinatari adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di **prevenire il verificarsi dei reati in essa considerati**

Il Consiglio di Amministrazione nel definire tale documento, ad ulteriore conferma della volontà aziendale di operare secondo principi "etici" così come già contemplati nella propria regolamentazione interna, intende sensibilizzare tutto il personale a mantenere comportamenti corretti e idonei a prevenire la commissioni di reati.

A tale scopo vengono disciplinati nel presente documento i presidi per il contenimento dei rischi individuati in apposita *gap-analysis* composti da principi e le regole di comportamento generali e specifiche da porre alla base dell'operatività aziendale.

Tali principi e regole richiamano, focalizzandoli ai fini della prevenzione dei reati connessi al Decreto ed eventualmente integrandoli, quelli previsti nel Codice Etico/Codice di Comportamento Interno e nelle procedure aziendali interne attualmente in vigore.

In via generale, a tutto il personale dell'azienda:

- È fatto obbligo di rispettare le regole, i principi e le procedure aziendali previste nel Modello e nei documenti interni della Società richiamati nel Modello e nei quali il medesimo si articola
- È fatto divieto di:

- Porre in essere, dare causa o concorrere alla realizzazione di comportamenti che possano integrare, direttamente o indirettamente, qualsiasi fattispecie di reato disciplinata nella legislazione tempo per tempo vigente e, in particolare, i reati di cui al Decreto
- Violare in tutto o in parte le regole, i principi e le procedure aziendali previste nel Modello e nei documenti interni della società richiamati nel Modello e nei quali il medesimo si articola

La violazione delle norme aziendali e, in particolare, di quelle richiamate nel presente documento, comporta l'applicazione del Codice Sanzionatorio.

I medesimi obblighi e divieti si applicano, per le attività e i comportamenti loro rispettivamente attribuiti o comunque ai quali sono tenuti nell'esercizio dell'ufficio o dell'incarico, ai componenti degli Organi Sociali della società, ai Collaboratori esterni e ai Partner.

C. PRINCIPI GENERALI DEL SISTEMA DI CONTROLLO

C.1. ARTICOLAZIONE DEI POTERI E SISTEMA DELLE DELEGHE

C.1.1. Principi ispiratori del sistema di articolazione dei poteri delle deleghe

Il sistema adottato delle deleghe e dei poteri costituisce parte integrante e sostanziale del Modello 231 aziendale.
Il principio cui l'azienda ispira la propria struttura organizzativa e la propria attività è quello in base al quale solo i soggetti muniti di specifici e formali poteri possono assumere, in suo nome e per suo conto, obbligazioni verso terzi.
I principi ispiratori di tale sistema sono:

- La tempestiva e costante informazione circa la titolarità dei poteri delegati ed i relativi cambiamenti
- La verifica periodica del rispetto dei poteri così come delegati.
- Le dichiarazioni periodiche di cui sia determinata nel Modello 231 la cadenza con le quali coloro che hanno ricevuto deleghe di poteri confermino l'assenza di conflitti di interesse, così come declinata e disciplinata anche nel PTPCT.
- La verifica periodica dell'adeguatezza del sistema delle deleghe.

A tutti i poteri attribuiti mediante delega degli stessi corrispondono esattamente mansioni e responsabilità come riportate nell'organigramma della società.
Il sistema dei poteri e delle deleghe prevede che:

- Ogni destinatario del presente Modello 231 che, per conto dell'azienda intrattiene rapporti negoziali e/o di rappresentanza con l'esterno, deve essere dotato di idonea procura.
- Tutti coloro (ivi compreso anche i dipendenti o gli organi sociali) che intrattengono per conto dell'azienda rapporti con la Pubblica Amministrazione, devono essere dotati di delega formale in tal senso.
- Ciascuna delega definisce in dettaglio i poteri del delegato e del soggetto.

L'Organismo di Vigilanza verifica periodicamente il sistema delle deleghe e delle procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative, raccomandando eventuali modifiche.
Il conferimento della procura è seguito da un flusso informativo all'OdV.

C.1.2. Il sistema dei poteri e delle deleghe

Il principio della segregazione delle responsabilità è applicato in azienda in linea con quanto consentito dalla normativa vigente.
I poteri di firma e di rappresentanza sono rilasciati dall'Organo Amministrativo o dall'Amministratore che ne è titolare per delega e sono revocabili in qualsiasi momento attraverso una semplice notifica a seguito della decisione della società.
Il sistema dei poteri e delle deleghe prevede l'attribuzione dei poteri di rappresentanza sia agli amministratori che a procuratori esterni con procura speciale (come consulenti esterni, dipendenti, etc.,).

C.2. ALTRI PRINCIPI GENERALI DEL SISTEMA DI CONTROLLO

Gli organi sociali, gli amministratori, i dipendenti ed i procuratori aziendali nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nello svolgimento delle attività a rischio hanno l'espresso obbligo di perseguire altresì i seguenti principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi di controllo specifici:

- **Segregazione delle attività:** Si richiede l'applicazione del principio di separazione delle attività e dei ruoli che intervengono nelle attività chiave dei processi operativi esposti a rischio, tra chi autorizza, chi esegue e chi controlla; in particolare, deve sussistere separazione dei ruoli di gestione di un processo e di controllo dello stesso.

- **Esistenza di procedure**: devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire i principi di comportamento e le modalità operative per lo svolgimento delle attività sensibili. Le procedure devono definire formalmente le responsabilità e i ruoli all'interno del processo e le disposizioni operative e relativi controlli posti a presidio nelle attività.

- **Poteri autorizzativi e di firma**: definire livelli autorizzativi da associarsi alle attività critiche dei processi operativi esposti a rischio. Inoltre i poteri autorizzativi e di firma devono: essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese e essere chiaramente definiti e conosciuti all'interno della società.

- **Tracciabilità**: tracciabilità delle attività svolte nell'ambito dei processi esposti a rischio; ogni operazione relativa alle attività sensibili deve essere adeguatamente registrata. Il processo di

decisione, autorizzazione e svolgimento dell'attività sensibile deve verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

- **Gestione delle segnalazioni:** raccolta, analisi e gestione delle segnalazioni di fattispecie a rischio per i reati ambientali rilevati da soggetti interni e esterni all'ente.

- **Riporto all'OdV (Organismo di Vigilanza):** riferire prontamente all'OdV eventuali situazioni di irregolarità.

D. REATI PREUSPPOSTO DEL D.LGDS. N. 231/01 NON CONTEMPLATI DALLA PARTE SPECIALE

Per quanto riguarda i reati presupposto previsti dal D.lgs. n. 231/01 non contemplati nella presente Parte speciale ad esito della *gap analysis*, così come individuati **nell'allegato al Modello 231 intitolato "elenco reati presupposto"**, al fine di prevenire comunque il rischio che vengano perpetrati nel contesto aziendale, è fatto espresso divieto a tutti i soggetti destinatari del Modello di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui al D.Lgs.n.231/01, nonché di porre in essere comportamenti in violazione delle procedure/protocolli/prescrizioni aziendali e del Codice etico.

È da considerarsi vietato qualsiasi comportamento che possa integrare una condotta rilevante di una qualsivoglia fattispecie di reato contemplata dal D.Lgs.n.231/01.

In generale, la prevenzione di tutti i reati previsti dal D.lgs. n. 231/01, oltre che con l'applicazione dei principi generali di controllo sopra riportati, è attuata almeno attraverso l'applicazione dei seguenti strumenti di rilevanza trasversale:

- Codice Etico.
- Idoneo sistema disciplinare e sanzionatorio applicabile a carico dei dipendenti (o altri destinatari del Modello) che violino i sistemi di controllo preventivi o le indicazioni comportamentali presenti nel Modello e in tutta la documentazione societaria esistente e ad esso afferente.
- Predisposizione di programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti dalla commissione dei reati previsti dal D.Lgs.n.231/01

Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Parte Speciale, in linea generale e al fine di perseguire la prevenzione dei reati ambientali è fatto espresso divieto a tutti i soggetti destinatari del Modello di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui al D.Lgs.n.231/01.

È da considerarsi vietato qualsiasi comportamento che possa integrare una condotta rilevante di una qualsivoglia fattispecie di reato contemplata dall'Art.25-undecies del D.Lgs.n.231/01

In generale, la prevenzione dei reati ambientali è svolta attraverso adeguate misure organizzative e normative e in particolare almeno attraverso l'applicazione dei seguenti controlli di carattere generale:

- Previsione nel Codice Etico e relativa appendice applicativa di specifiche indicazioni volte a impedire la commissione dei reati previsti dall'Art.25-undecies del D.Lgs.n.231/01
- Previsione di un idoneo sistema di sanzioni disciplinari (o vincoli contrattuali nel caso di terze parti) a carico dei dipendenti (o altri destinatari del Modello) che violino i sistemi di controllo preventivi o le indicazioni comportamentali presenti nel Modello e in tutta la documentazione societaria esistente e ad esso afferente
- Predisposizione di adeguati strumenti organizzativi e normativi atti a prevenire e/o impedire la realizzazione dei reati previsti dall'Art. 25-undecies del D.Lgs.n.231/01 da parte dei dipendenti e in particolare di quelli appartenenti alle strutture della società ritenute più esposte al rischio
- Predisposizione di programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti dalla commissione dei reati previsti dall'Art. 25-undecies del D.Lgs.n.231/01

E. RACCORDO TRA MODELLO 231 E PIANO TRIENNALE PER LA PREVENZIONE DELLA CORRUZIONE (PTPCT) ex LEGE N. 190/12

La Società ha adottato e aggiorna annualmente il proprio Piano per la prevenzione della corruzione e per la trasparenza (PTPCT) ai sensi della Legge n. 190/12 che contiene le misure integrative a quelle derivate dall'attuazione del Modello 231 per il presidio dei rischi di *maladministration* e conseguentemente (ma non solo) anche di commissione di reati che possono astrattamente recare un danno all'Ente e non solo di quelli da cui può scaturire un interesse o un vantaggio per quest'ultimo. Detto PTPCT rappresenta una parte integrante e sostanziale del Modello 231 ed in particolare della presente Parte speciale per i reati di cui agli art.li 24, 25 e 25-ter (con riferimento alla corruzione tra privati).

Ulteriori presìdi preventivi si ravvisano in adeguati percorsi formativi, programmati su base annuale in materia di prevenzione della corruzione in materia di gestione dei finanziamenti pubblici a carico delle funzioni aziendali interessate, nelle attività che coinvolgono l'Organismo di Vigilanza nello svolgimento dei controlli di competenza e per lo scambio di informazioni (e segnalazioni) con le funzioni competenti, il tutto in stretto coordinamento con il RPCT come previsto dalla Delibera Anac n. 1134/17 e dal PNA ed infine nella previsione nel Codice Etico e nel Codice Sanzionatorio dei profili di condotta vietati e del relativo apparato sanzionatorio.

SEZIONE 1:

REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE CORRUZIONE E CONCUSSIONE

(ARTT. 24 E 25 DEL D.LGS.N.231/01)

1. I REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE CORRUZIONE E CONCUSSIONE (ARTT. 24 E 25 DEL D.LGS.N.231/01)

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex Art. 5 del D.Lgs.n.231/2001 è collegato il regime di responsabilità a carico della società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi del D.Lgs.n.231/2001, si riporta, qui di seguito, una breve descrizione dei reati richiamati dall' Art. 24 (Indebita percezione di erogazioni, truffa in danno dello stato o di un ente pubblico o dell'Unione Europea per il conseguimento di erogazioni pubbliche e frode informatica in danno dello stato o di un ente pubblico e frode nelle pubbliche forniture) e dall'Art.25 (Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio) del D.Lgs.n.231/01.

1.1. ART. 24 – INDEBITA PERCEZIONE DI EROGAZIONI, TRUFFA IN DANNO DELLO STATO (...)

Le fattispecie di reato di cui all'Art. 24 D.Lgs. 231/2001 sono le seguenti:

Reato	Esempio di condotta
- Malversazione a danno dello Stato o di altro ente pubblico (art. 316-bis c.p.).	I dipendenti dell'azienda, cui sia stata affidata la gestione di un finanziamento pubblico, utilizzano i fondi per scopi diversi da quelli per i quali il finanziamento è stato erogato (ad esempio, fondi ricevuti per scopi di formazione del personale dipendente vengono utilizzati per coprire le spese di corsi già effettuati autonomamente dalla società)
- Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico o delle Comunità europee (art. 316-ter c.p.).	Un funzionario aziendale rilascia, in violazione della procedura aziendale adottata, una garanzia fideiussoria necessaria per l'ottenimento di un finanziamento pubblico da parte di un proprio Cliente, pur essendo a conoscenza che il garantito non possiede i requisiti di legge per l'ottenimento dell'erogazione pubblica.
- Frode nelle pubbliche forniture (Art. 356 c.p.) inserito dal D.Lgs.n.75 del 14 luglio 2020.	lavori di adeguamento degli impianti di un edificio pubblico eseguiti in difformità rispetto alla normativa e al contenuto dell'appalto; consegna di un prodotto o

	servizio diverso da quello pattuito nell'esecuzione di un contratto
- Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art. 640, co. 2, n.1, c.p.).	Nella predisposizione di documenti o dati per la partecipazione a procedure di gara, la società fornisce alla Pubblica Amministrazione informazioni non veritiere
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.).	A titolo esemplificativo, si veda il caso precedente di cui all'art. 640 c.p.: la finalità deve consistere nell'ottenimento di un finanziamento o contributo pubblico.
- Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.).	In concreto, può integrarsi il reato in esame qualora, una volta ottenuto un finanziamento, l'azienda violasse il sistema informatico della Pubblica Amministrazione al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.
- Frode nelle pubbliche forniture (art. 356 c.p.) [introdotto dal D.Lgs. n. 75/2020] - Frode ai danni del Fondo europeo agricolo (art. 2. L. 23/12/1986, n.898) [introdotto dal D.Lgs. n. 75/2020]	Fornitura di servizi non conformi: Una società di pulizie che si aggiudica il servizio per un ospedale pubblico. Il contratto prevede l'uso di specifici disinfettanti e sanificanti professionali, ma l'impresa, per risparmiare, utilizza normali detergenti da supermercato, meno efficaci e non idonei per un ambiente sanitario.
- Turbata libertà degli incanti (art. 353 c.p.) [articolo introdotto dalla L. n. 137/2023] - Turbata libertà del procedimento di scelta del contraente (art. 353-bis) [articolo introdotto dalla L. n. 137/2023]	Promesse o doni a un membro della commissione: Un imprenditore promette un viaggio o una somma di denaro a un membro della commissione di gara in cambio di informazioni riservate sulle offerte degli altri concorrenti, in modo da poter calibrare la propria offerta e vincere.

1.2. ART 25 – CONCUSSIONE E CORRUZIONE, INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ

Le fattispecie di reato di cui all'Art. 25 D.Lgs. 231/2001 sono le seguenti:

Reato	Esempio di condotta
- Peculato (art. 314 c.p.).	Un incaricato di pubblico servizio utilizza la carta di credito aziendale per ragioni private.
- Concussione (Art. 317 c.p.)	Un dipendente, nell'esercizio delle proprie funzioni, costringe un soggetto a versare una somma maggiore rispetto a quella dovuta, procurando un vantaggio all'azienda. Tuttavia, sembra più plausibile un'ipotesi di concorso in concussione.

- Corruzione per un atto d'ufficio – Corruzione per un atto contrario ai doveri d'ufficio – Circostanze aggravanti-Induzione indebita a dare o promettere utilità-Corruzione di persona incaricata di pubblico servizio, Pene per il corruttore (Artt. 318 modificato da L.3 del 9 gennaio 2019, 319, 319-bis, e 320 c.p. modificati da L.69 del 27 maggio 2015 e 319-quater c.p. modificato dal D.Lgs.n.75 del 14 luglio 2020, Art. 321 c.p.)	RUP che agevola appalti in favore dei cari o agevola l'affidamento degli appalti in favore delle persone a lui più vicine
- Corruzione in atti giudiziari (Art. 319-ter c.p.)	Un dirigente versa denaro ad un cancelliere del Tribunale affinché accetti, seppur fuori termine, delle memorie o delle produzioni documentali, consentendo quindi di superare i limiti temporali previsti dal codice di procedura penale a tutto vantaggio della propria difesa.
- Istigazione alla corruzione (Art. 322 c.p.)	Si veda il caso enunciato relativamente al reato di corruzione per un atto d'ufficio o contrario ai doveri d'ufficio con conseguente rifiuto dell'offerta del dipendente da parte del pubblico ufficiale.
- Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilita', corruzione [Articolo modificato dalla L. n. 190/2012, dalla Legge n. 3 del 9 gennaio 2019 dal D.Lgs.n.75 del 14 luglio 2020 e dalla Legge n.112 dell'8 agosto 2024]	Si faccia riferimento alle singole fattispecie delittuose considerate sopra.
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.) [articolo introdotto dalla L. n. 112/2024]	**Fondi vincolati dirottati:** l'azienda riceve un fondo di 100.000 euro con un vincolo di legge specifico: manutenzione immobili. L'azienda, invece, utilizza una parte di quei soldi (es. 30.000 euro) per pagare gli straordinari al personale amministrativo. Non si appropria del denaro, ma lo distrae dalla finalità obbligatoria per legge per un vantaggio non patrimoniale che genera un vantaggio patrimoniale per i dipendenti.
- Traffico di influenze illecite (Art.346-bis c.p. modificato da L.3 del 9 gennaio 2019)	Tale previsione è volta a punire condotte di accordi corruttivi: essa punisce chi si offre di mettere in contatto un soggetto con un pubblico ufficiale al fine di porre in essere un accordo illecito, in cambio di promessa o della dazione di denaro.

I reati elencati nell'articolo 24 e 25 del decreto legislativo n. 231/2001, appartengono alla categoria dei delitti dei pubblici ufficiali contro la pubblica amministrazione.

Tale categoria di reati è stata ulteriormente rivista a seguito dell'entrata in vigore della L. 27 maggio 2015, n. 69 "Disposizioni in materia di delitti contro la pubblica amministrazione, di associazioni di tipo mafioso e di falso in bilancio", la quale interviene nel senso di estendere le pene edittali previste dal c.p. in caso di commissione di alcune fattispecie di reato (artt. 318, 319, 319-ter e quater) ed inoltre modificando l'articolo 317 del c.p., ampliando la categoria di quanti possono commettere il reato proprio di concussione. Al pubblico ufficiale viene infatti aggiunto anche l'incaricato di un pubblico servizio.

Soggetti attivi possono essere i pubblici ufficiali e gli incaricati di pubblico servizio, intesi come coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di questa ultima (deliberativi, autoritativi, certificativi), e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale (articolo 358 c.p.).

Anche in questo caso la norma accoglie una concezione oggettiva di pubblico servizio: ciò che rileva è solo il concreto esercizio di un pubblico servizio, a prescindere dal rapporto di impiego con lo Stato o altro ente pubblico o privato.

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

Il legislatore puntualizza la nozione di "pubblico servizio" attraverso due ordini di criteri, uno positivo ed uno negativo. Il "servizio", affinché possa definirsi pubblico, deve essere disciplinato – del pari alla "pubblica funzione" - da norme di diritto pubblico ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

Il legislatore ha inoltre precisato che non può mai costituire "servizio pubblico" lo svolgimento di "semplici mansioni di ordine" né la "prestazione di opera meramente materiale". Con riferimento alle attività che vengono svolte da soggetti privati in base ad un rapporto concessorio con un soggetto pubblico, si ritiene che ai fini della definizione come pubblico servizio dell'intera attività svolta nell'ambito di tale rapporto concessorio non è sufficiente l'esistenza di un atto autoritativo di investitura soggettiva del pubblico servizio, ma è necessario accertare se le singole attività che vengono in questione siano a loro volta soggette a una disciplina di tipo pubblicistico.

La giurisprudenza ha individuato la categoria degli incaricati di un pubblico servizio, ponendo l'accento sul carattere della strumentalità ed accessorietà delle attività rispetto a quella pubblica in senso stretto.

Essa ha quindi indicato una serie di "indici rivelatori" del carattere pubblicistico dell'ente, per i quali è emblematica la casistica in tema di società per azioni in controllo pubblico. In particolare, si fa riferimento ai seguenti indici:

- La sottoposizione ad un'attività di controllo e di indirizzo a fini sociali, nonché ad un potere di nomina e revoca degli amministratori da parte dello Stato o di altri enti pubblici
- La presenza di una convenzione e/o concessione con la pubblica amministrazione
- L'apporto finanziario da parte dello Stato
- L'immanenza dell'interesse pubblico in seno all'attività economica

Sulla base di quanto sopra riportato, si potrebbe ritenere che l'elemento discriminante per indicare se un soggetto rivesta o meno la qualifica di "incaricato di un pubblico servizio" è rappresentato, non dalla natura giuridica assunta o detenuta dall'ente, ma dalle funzioni affidate al soggetto le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale

È importante, dunque, tenere a mente che, ad esempio, allorché una banca svolga l'attività di concessionaria per la riscossione delle imposte, in quella veste essa è incaricata di pubblico servizio. Bisogna perciò sempre esaminare con attenzione il tipo di rapporto che si instaura con un ente terzo e nel caso di dubbio sulla natura giuridica, rivolgersi immediatamente alla funzione specifica per approfondimenti e chiarimenti.

1.3. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA

Molti dei reati compresi negli art. 24 e 25 del D.Lgs. 231/01 sono, in astratto, configurabili al contesto di ERP LUCCA.

Tali reati, infatti, sono riconducibili alle attività svolte per la richiesta di contributi/finanziamenti a soggetti pubblici (come Comunità Europea, Regioni, Provincia, Comuni, etc.) sia per attività rientranti nelle proprie competenze statutarie (progettazione e realizzazione di alloggi di E.R.P.), sia per attività collaterali relative ad es. alla ricerca & sviluppo (ad es. progetti di innovazione), alla formazione del personale (fondi interprofessionali), all'ottenimento di misure di sostegno pubblico in genere.

In particolare i reati di cui all'articolo 24 del D.Lgs. 231/2001, nel contesto specifico, possono comportare rischi significativi in quanto ERP LUCCA si configura quale stazione appaltante con il ricorso a finanziamenti pubblici per le attività di nuova costruzione, recupero e manutenzione straordinaria ed opera quasi esclusivamente ricorrendo a finanziamenti pubblici.

Le aree aziendali principalmente a rischio per tali reati sono quella Tecnica, relativamente alle attività di Progettazione e Direzione Lavori e quella Amministrativa per quanto riguarda la gestione della contabilità relativa ai contributi ricevuti e alla relativa rendicontazione.

ERP LUCCA svolge un'attività di interesse pubblico per la quale propri dipendenti possono assumere il ruolo di pubblico ufficiale e di incaricato di pubblico servizio.

Inoltre, lo svolgimento delle proprie funzioni presuppone il frequente contatto con soggetti appartenenti alla Pubblica Amministrazione tra i quali funzionari della Regione e dei Comuni, sindaci ed assessori comunali, funzionari di organi di controllo (ASL, ARPA, Vigili del Fuoco, ecc.).

Complessivamente, in relazione ai reati di cui all'art.25 del decreto, appare in astratto plausibile l'ipotesi che soggetti apicali, o loro sottoposti, possano commettere atti di corruzione nell'interesse della Società promettendo o attribuendo qualche utilità a pubblici ufficiali o incaricati di pubblico servizio, detentori del potere di assumere decisioni o di svolgere attività rilevanti per l'azienda (es. autorizzazioni, concessione di finanziamenti, verifiche, controlli, ispezioni, etc.).

Allo stesso tempo il dipendente dell'ERP LUCCA con qualifica di pubblico ufficiale o incaricato di pubblico servizio può essere soggetto attivo dei reati previsti ad es. inducendo taluno a dare o promettere per sé o ad un terzo indebitamente denaro o altre utilità (art. 319-quater c.p.) o costringendo taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli (art. 317 c.p.).

In questi casi, pur ravvisando una maggiore probabilità che il reato possa essere commesso a vantaggio e nell'interesse personale e non in quello della Società, non si escludono forme di vantaggio o interesse (anche indiretto) per la Società stessa.

Di conseguenza tali reati sono trattati all'interno del Modello, oltre ad essere puntualmente presi in considerazione all'interno delle misure di prevenzione della corruzione adottate ai sensi della L. 190/12.

Tra le attività sensibili relative a tale area emerse dall'analisi dei rischi si ricordano:

DIREZIONE/U.O. RESPONSABILI	PROCESSO 231	ATTIVITA' PER PROCESSO
Manu.ne Straordinaria All. di Risulta	Programmazione, Progettazione interventi, Direzione dei lavori, esecuzione	FO-2.1 Progettazione degli interventi di manutenzione straordinaria FO-2.2 Studio di fattibilita' dei lavori e progettazione preliminare FO-2.3 Progettaz. definitiva ed esecutiva commesse di costruzione e recupero FO-2.4 Verifica della progettazione FO-4.1 Gestire gli adempimenti per la Direzione lavori FO-4.2 Effettuare la Direzione dei lavori FO-4.3 Eseguire l'Ultimazione dei lavori e il Collaudo
Manu.ne Straordinaria All. di Risulta	Programmazione, Progettazione interventi, Direzione dei lavori, esecuzione	FO-2.1 Progettazione degli interventi di manutenzione straordinaria FO-2.2 Studio di fattibilita' dei lavori e progettazione preliminare FO-2.3 Progettaz. definitiva ed esecutiva commesse di costruzione e recupero FO-2.4 Verifica della progettazione FO-4.1 Gestire gli adempimenti per la Direzione lavori

		FO-4.2 Effettuare la Direzione dei lavori FO-4.3 Eseguire l'Ultimazione dei lavori e il Collaudo
Gare e appalti	Gestire gli approvvigionamenti	FS-5.1 Gestione Acquisti di Servizi
Gare e appalti	Gestire gli approvvigionamenti	FS-5.1 Gestione Acquisti di Servizi
Gare e appalti	Conferimento incarihi professionali	Conferimento incarihi professionali FS-3.1 Gestione Albi e valutazione professionisti
Gare e appalti	Conferimento incarihi professionali	Conferimento incarihi professionali FS-3.1 Gestione Albi e valutazione professionisti
Morosità	Gestire accertamenti, morosità e decadenze	FO-5.4 Gestire accertamenti, morosità e decadenze
Gare e appalti	Partecipazione a bandi di finanziamento e contributi. Richiesta di finanziamento e contributi	Partecipazione a bandi di finanziamento e contributi. Richiesta di finanziamento e contributi
Gare e appalti	Partecipazione a bandi di finanziamento e contributi. Richiesta di finanziamento e contributi	Partecipazione a bandi di finanziamento e contributi. Richiesta di finanziamento e contributi
Gare e appalti	Gestione delle gare di appalto.	Gestione delle gare di appalto.
S.I.A.	Gestione della bollettazione e della fatturazione attiva	FO-5.3 Gestire la bollettazione e la fatturazione
Utenza	Gestire i Provvedimenti Amministrativi (richieste, volture, subentri, assegnazioni, consegne...)	FO-5.1 Gestire l'assegnazione e il contratto di locazione FO-5.2 Gestire le variazioni anagrafiche e reddituali FO-5.5 Gestire Autogestioni e Condomini
Autogestioni e Condomini	Gestire i Provvedimenti Amministrativi (richieste, volture, subentri, assegnazioni, consegne...)	FO-5.5 Gestire Autogestioni e Condomini
Servizi generali	Gestire il protocollo	FS-2.1 Gestire il protocollo
Ragioneria	Gestione rapporti contrattuali (con enti di certificazione, istituti di credito ecc.)	Gestione rapporti contrattuali (con enti di certificazione, istituti di credito ecc.)
- Personale	Selezione del personale	FS-3.1 Selezionare e assumere il personale
Patrimoniale	Gestire il Patrimonio	FO-6.3 Gestione delle vendite di unita' immobiliari
Manutenzione Ordinaria Pronto Intervento	Gestire il Patrimonio	FO-6.2 Effettuare la Manutenzione del patrimonio
Ragioneria	Gestione risorse finanziarie	Gestione risorse finanziarie
TUTTE LE U.O.	Gestire i Rapporti con P.A. in occasione di accertamenti, verifiche	Gestire i Rapporti con P.A. in occasione di accertamenti, verifiche

1.4. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE

1.4.1. Principi

Si individuano qui di seguito i principi che informano le specifiche procedure interne dell'azienda previste in relazione a qualsiasi operazione/attività che coinvolga un ente della Pubblica Amministrazione, nonché le regole di condotta che sottendono alle specifiche previsioni di comportamento elaborate dalla società in relazione a tale ambito di applicazione.

Si stabilisce pertanto che tutte le regole, i processi e le prassi operative nei rapporti con la P.A. devono rispettare i principi e le regole di comportamento nel seguito delineate
Tutte le operazioni/attività che coinvolgono in qualsiasi modo un ente della Pubblica Amministrazione devono essere poste in essere nel pieno rispetto delle leggi vigenti, del Codice Etico e del Codice di Comportamento Interno, delle regole contenute nel presente Modello, delle policy e delle procedure/protocolli aziendali, dei valori e delle politiche della società.

La struttura aziendale è articolata in modo tale da soddisfare i requisiti fondamentali di formalizzazione, chiarezza, comunicazione e separazione dei ruoli richiesti in generale nel Decreto e di peculiare importanza nella gestione dei rapporti con la Pubblica Amministrazione, in particolare per ciò che concerne l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

La società si dota di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, mansionari etc.) improntati a principi generali di:

- Conoscibilità all'interno della società (ed eventualmente anche nei confronti delle altre società del Gruppo)
- Chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri
- Chiara descrizione delle linee di riporto

A tal fine, le procedure interne aziendali sono strutturate in modo da garantire in generale per ciascun processo ed in particolare nei rapporti con la Pubblica Amministrazione:

- Una distinzione, quanto più possibile netta, tra il soggetto che lo avvia a livello decisionale, il soggetto che lo esegue e lo porta a termine ed il soggetto che lo controlla
- La tracciabilità scritta di ciascuna fase rilevante
- Un adeguato livello di formalizzazione

Che i sistemi premianti e/o di incentivazione dei soggetti che hanno poteri di spesa e facoltà decisionali non siano commisurati al raggiungimento di risultati sostanzialmente irraggiungibili.

1.4.2. Norme generali di comportamento

I soggetti destinatari della presente Sezione coinvolti nelle attività elencate nei paragrafi precedenti devono rispettare principi e norme di comportamento di seguito dettate, nel rispetto degli obblighi normativi, delle procedure aziendali e del Codice Etico aziendale .

Coerentemente con i principi del Codice Etico, i rapporti tra la società e la Pubblica Amministrazione devono essere condotti in conformità alla legge e nel rispetto dei principi di lealtà, correttezza, trasparenza e verificabilità.

Si sottolinea che è assolutamente vietato:

- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, assunti individualmente o nel particolare contesto in cui si collocano, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (Artt. 24 e 25 del D.Lgs.n.231/2001)
- Promettere, offrire o acconsentire all'elargizione di denaro o altre utilità (beni materiali, servizi, etc.) a pubblici ufficiali o incaricati di pubblico servizio, o a loro familiari, che possano influenzare l'indipendenza del giudizio o indurre ad assicurare un vantaggio per la società
- Accordare vantaggi di qualsiasi natura (promessa di assunzione, etc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al punto precedente
- Distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale) ed in particolare, è vietata qualsiasi forma di regalo a funzionari pubblici o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere benefico o culturale, o il brand image della società. I regali offerti - salvo quelli di modico valore, devono essere documentati in modo adeguato a consentire le verifiche da parte dell'OdV
- Mettere in atto o favorire operazioni in conflitto di interesse dell'azienda, nonché attività in grado di interferire con la capacità di assumere decisioni imparziali nell'interesse dell'azienda nel rispetto del Codice Etico e delle normative applicabili
- Effettuare prestazioni in favore dei Consulenti e dei Partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi
- Riconoscere compensi in favore dei Consulenti e dei Partner che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale
- Effettuare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati, o comunque utilità a carico di bilanci pubblici, e/o per partecipare a gare o simili o risultarne vincitori
- Effettuare comunque dichiarazioni o attestazioni non veritiere ad organismi pubblici tali da indurre in errore tali soggetti, da creare un indebito profitto o vantaggio a favore della società e/o arrecare un danno all'ente pubblico

- Destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati
- Violare i principi e le procedure aziendali previste nella presente sezione della Sezione.

Al fine di scongiurare la commissione dei reati di cui alla presente sezione devono essere realizzati i seguenti presidi di controllo:

- Distribuzione delle responsabilità e previsione di adeguati livelli autorizzativi nelle attività di predisposizione, presentazione e ricezione di dati, informazioni e documenti verso/da rappresentanti della Pubblica Amministrazione, allo scopo di evitare sovrapposizioni funzionali o eccessive concentrazioni di potere
- Formale identificazione del soggetto deputato ad intrattenere rapporti con la PA. in relazione a ciascuna Potenziale Attività a Rischio
- Gestione in modo trasparente e univoco di qualsiasi rapporto professionale instaurato con membri della Pubblica Amministrazione o con soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio
- Attività di reporting all' OdV di eventuali situazioni di irregolarità

1.4.3. Presidi specifici relativi alla regolamentazione delle attività sensibili

Per il contenimento dei rischi di commissione di reati tra quelli indicati, connessi allo svolgimento dei processi di cui sopra, sono predisposti appositi presidi specifici, tra cui procedure (relative anche al sistema di gestione qualità aziendale) che dettagliano le attività e le responsabilità relative alla gestione delle richieste di contributo ed alla rendicontazione periodica.

Gli Organi Sociali, gli amministratori, i dipendenti e i procuratori aziendali nonché i collaboratori e tutte le altre controparti contrattuali, nell'ambito delle attività da essi svolte, devono rispettare le regole ed i divieti elencati al precedente paragrafo e ai fini dell'attuazione degli stessi devono rispettare le procedure specifiche qui di seguito descritte, oltre alle Regole e Principi Generali già contenuti nella Parte Generale del Modello 231.

In particolar modo nella gestione dei rapporti con la Pubblica Amministrazione devono essere osservate, tra le altre, le regole di comportamento di seguito indicate:

- Agli Organi Sociali, Dipendenti, Consulenti e Partner che materialmente intrattengono rapporti con la PA per conto dell'azienda deve essere formalmente conferito potere in tal senso dalla società (con apposita delega per i membri degli organi sociali e per i dipendenti - anche tramite il responsabile, individuato in base al sistema delle comunicazioni organizzative, ovvero nel relativo contratto di servizio o di consulenza o di partnership per gli altri soggetti destinatari del Modello 231). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta che rispetti tutti i criteri elencati nella Parte Generale

- Il responsabile individuato a rilasciare le procure deve predisporre una lista riepilogativa di tutti i Responsabili/addetti ad intrattenere rapporti con la Pubblica Amministrazione e renderla disponibile sull'Intranet aziendale
- I contratti tra l'azienda, i Consulenti e Partner che abbiano, anche solo potenzialmente, impatto sulle Potenziali Aree a Rischio devono essere definiti per scritto in tutte le loro condizioni e termini e devono contenere clausole standard al fine di garantire il rispetto del D.Lgs.n.231/2001
- Le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di contributi, finanziamenti, ed in genere di benefici a carico di bilanci pubblici, devono contenere solo elementi veritieri e, l'impegno della società, in caso di ottenimento degli stessi, all'effettiva utilizzazione dei fondi ottenuti secondo le finalità previste dalla specifica normativa di riferimento. In ogni caso, ciascuna delle dichiarazioni di cui al presente capo, ivi incluse le autocertificazioni ammesse dalla legge o dai bandi, devono essere corredate da documentazione idonea ad attestarne la veridicità, anche se eventualmente non richiesta dal destinatario di tali dichiarazioni
- Alle ispezioni giudiziarie, tributarie e amministrative (es. relative al D.Lgs.n.81/08 e successive modifiche, a verifiche tributarie, INPS, etc.) devono partecipare i soggetti a ciò espressamente delegati, dando avviso dell'avvio dell'ispezione/accertamento al Legale rappresentante ed all'OdV. Di tutto il procedimento relativo all'ispezione devono essere redatti e conservati appositi verbali. Nel caso il verbale conclusivo evidenziasse criticità, l'OdV ne deve essere informato con nota scritta da parte del responsabile coinvolto.
- La stipula di contratti/convenzioni con soggetti pubblici da parte della Società a seguito della partecipazione a procedure ad evidenza pubblica (asta pubblica, appalto-concorso, licitazione privata e trattative private) deve essere condotta in conformità ai principi, criteri e disposizioni dettate dal presente Modello
- Qualunque tipo di erogazione di fondi:
    - Deve essere deliberata previa adeguata istruttoria cui partecipino soggetti e funzioni diverse all'interno dell'azienda, in modo da minimizzare il rischio di una manipolazione illecita dei dati ed aumentare la condivisione delle conoscenze e delle decisioni aziendali
    - Presuppone una approfondita conoscenza della Clientela, così da consentire una valutazione della coerenza e della compatibilità dell'operazione con il profilo del Cliente, soprattutto laddove quest'ultimo non svolga attività di rilievo economico
- Ai Collaboratori esterni e Partner che materialmente intrattengono rapporti con la P.A. per conto dell'azienda, deve essere formalmente conferito potere in tal senso dall'azienda stessa, con apposita clausola contrattuale
- L'Organismo di Vigilanza deve essere informato con nota scritta di qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la P.A.

- I contratti tra la Società e i Collaboratori esterni e i Partner devono essere definiti per iscritto in tutte le loro condizioni e termini, e rispettare quanto indicato ai successivi punti
- I Collaboratori esterni devono essere scelti con metodi trasparenti e secondo specifica procedura aziendale, eventualmente differenziata tra fornitori di beni e servizi e professionisti
- Le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di concessioni, autorizzazioni o licenze devono contenere solo elementi assolutamente veritieri
- Alle ispezioni giudiziarie, tributarie e amministrative (es. relative al D.Lgs.n.81/08, verifiche tributarie, INPS, Autorità di vigilanza ecc.) devono partecipare i soggetti a ciò espressamente delegati. Di tutto il procedimento relativo all'ispezione devono essere redatti gli appositi verbali che verranno conservati dall'Organismo di Vigilanza.

In particolare, la Società ha predisposto e adotta:

- una procedura del sistema di gestione aziendale nel quale si definisce il processo di formazione delle decisioni e le responsabilità (MOG. 2.1 PROTOCOLLO FORMAZIONE DELLE DECISIONI). In tale procedura si attuano i tipici principi di controllo preventivo quali la separazione dei ruoli e delle responsabilità nelle varie fasi del processo e la documentazione e la tracciabilità dei controlli.
- Un protocollo sulle modalità per la gestione delle risorse finanziarie e della contabilità.

1.5. I CONTROLLI DELL'ORGANISMO DI VIGILANZA

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza, in stretto coordinamento con il RPCT al quale compete la vigilanza sul PTPCT, parte integrante del Modello 231 , effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui agli Artt. 24 e 25 del Decreto commessi nell'interesse o a vantaggio dell'azienda diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello.

I compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati di cui agli Artt. 24 e 25 del Decreto sono i seguenti:

- Verificare a titolo esemplificativo, l'idoneità dei presidi specifici e delle procedure interne di cui sopra, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.
- Proporre che vengano costantemente aggiornate le procedure aziendali per prevenire la commissione dei reati nei rapporti con la Pubblica Amministrazione, di cui alla presente Sezione; con riferimento a tale punto l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio di commissione dei suddetti reati, diretti a verificare la corretta

esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere; o proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Sezione

- Verificare l'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni.
- Sulla base dei flussi informativi ricevuti l'Organismo di Vigilanza condurrà verifiche mirate su determinate operazioni effettuate nell'ambito delle Aree Sensibili, volte ad accertare da un lato il rispetto di quanto stabilito nel Modello e nei protocolli, dall'altro l'effettiva adeguatezza delle prescrizioni in essi contenute a prevenire i reati potenzialmente commissibili.
- Esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

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

1.5.1. Flussi informativi verso l'organismo di vigilanza

Sussiste a carico di tutti i Destinatari del MOG (soggetti apicali, sottoposti, consulenti, etc.) l'**obbligo di segnalazione immediata all'OdV** in caso di notizie rilevanti sulla vita dell'Ente, violazioni del Modello, della presente Parte Speciale o situazioni di riscontrata inadeguatezza e/o non conformità di comportamenti ai principi contenuti nelle procedure/istruzioni aziendali e nel Codice Etico.
Le segnalazioni di illeciti, secondo le istruzioni impartite dall'OdV, dovranno avvenire con le modalità indicate nell'apposita **Procedura "*Flussi Informativi*",** nel rispetto della normativa in tema di *Whistleblowing*.
Con riferimento ai controlli periodici sui processi aziendali e allo svolgimento delle normali attività il D.Lgs. n. 231/01 prevede **flussi informativi con cadenze determinate** verso l'OdV da parte di specifici soggetti. Si rinvia alla **Procedura "*Flussi Informativi*",** allegata al Modello, per la descrizione delle specifiche modalità operative con cui dovranno essere inviati i suddetti flussi.

SEZIONE 2:

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

(ART. 24-BIS)

2. ART. 24-BIS – DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

2.1. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS.N.231/01

La presente Sezione si riferisce ai Delitti informatici e trattamento illecito di dati (di seguito, per brevità, i "Delitti Informatici")
Si descrivono qui di seguito le singole fattispecie di reato per le quali l'Art. 24-bis del D.Lgs.n.231/2001 prevede una responsabilità degli enti nei casi in cui tali reati siano stati compiuti nell'interesse o a vantaggio degli stessi.

- Falsità in un documento informatico pubblico o privato avente efficacia probatoria (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.).
- Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche (Introdotto dalla Legge n.90 del 28 giugno 2024) - Art. 617-bis c.p.
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.).
- Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (Introdotto dalla Legge n.90 del 28 giugno 2024) - Art. 617-sexsies c.p.
- Circostanze attenuanti (introdotto dalla Legge n.90 del 28 giugno 2024) - Art. 623-quater c.p.
- Estorsione (Introdotto dalla Legge n.90 del 28 giugno 2024) - Art. 629 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.).

- Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Introdotto dalla Legge n.90 del 28 giugno 2024) - Art. 635-quater.1 c.p.
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.).
- Frode informatica (Modificato da D.Lgs.n.184 dell'8 novembre 2021 e dal D.Lgs. n. 150 del 10 Ottobre 2022) - Art. 640-ter c.p.
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.).

2.2. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA

ERP LUCCA gestisce un sistema informativo di interesse pubblico e le proprie attività sono pressoché integralmente gestite da procedure informatiche. In linea generale quindi i reati in questione attraversano l'intera organizzazione aziendale. Tuttavia il focus dovrà indirizzarsi sui casi in cui si possa configurare un interesse o un vantaggio per la Società, riducendo per questa via i potenziali casi applicativi.
È da considerarsi, inoltre, che nell'espletamento delle proprie funzioni, una parte del personale dispone di credenziali per l'accesso a banche dati esterne di proprietà di soggetti pubblici, tra le quali si segnalano ad es.:

- ENTRATEL;
- SISTER-Agenzia delle Entrate;
- ANAC;
- INPS;
- SPORTELLO UNICO PREVIDENZIALE.

I reati che astrattamente possono con probabilità non irrilevante concretamente realizzarsi nel contesto aziendale sono i seguenti:

- Falsità in documenti informatici (Art. 491-bis c.p.)

Reato	Esempio di condotta
– Falsità in documenti informatici (Art. 491-bis c.p.)	A titolo esemplificativo, integrano il delitto di falsità in documenti informatici la condotta di inserimento fraudolento di dati falsi nelle banche dati pubbliche oppure la condotta dell'addetto alla gestione degli archivi informatici che proceda, deliberatamente, alla modifica di dati in modo da falsificarli Inoltre, il delitto potrebbe essere integrato tramite la cancellazione o l'alterazione di informazioni a valenza probatoria presenti sui sistemi dell'ente, allo scopo di eliminare le prove di un altro reato

- Accesso abusivo ad un sistema informatico o telematico (Art. 615-ter c.p.)	Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato Il delitto di accesso abusivo a sistema informatico si integra, ad esempio, nel caso in cui un soggetto accede abusivamente ad un sistema informatico e procede alla stampa di un documento contenuto nell'archivio del PC altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura) Il delitto potrebbe essere astrattamente commesso da parte di qualunque dipendente della società accedendo abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), ad esempio, per prendere cognizione di dati riservati di un'impresa concorrente, ovvero tramite la manipolazione di dati presenti sui propri sistemi come risultato dei processi di business allo scopo di produrre un bilancio falso o, infine, mediante l'accesso abusivo a sistemi aziendali protetti da misure di sicurezza, da parte di utenti dei sistemi stessi, per attivare servizi non richiesti dalla clientela
- Danneggiamento di informazioni, dati e programmi informatici (Art. 635-bis c.p.)	Il reato, ad esempio, si integra nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale Il danneggiamento potrebbe essere commesso a vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento delle obbligazioni da parte del fornitore
- 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.)	Questo delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà

	di privati ma destinati alla soddisfazione di un interesse di natura pubblica. Perché il reato si integri è sufficiente che si tenga una condotta finalizzata al deterioramento o alla soppressione del dato
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635-quinquies c.p.)	Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità (Art. 635-ter), quel che rileva è che il sistema sia utilizzato per il perseguimento di pubblica utilità indipendentemente dalla proprietà privata o pubblica del sistema stesso Il reato si può configurare nel caso in cui un dipendente cancelli file o dati, relativi ad un'area per cui sia stato abilitato ad operare, per conseguire vantaggi interni (ad esempio, far venire meno la prova del credito da parte di un ente o di un fornitore) ovvero che l'amministratore di sistema, abusando della sua qualità, ponga in essere i comportamenti illeciti in oggetto per le medesime finalità già descritte.
- Frode informatica (Art.640-ter c.p. modificato dal D.Lgs n. 36 del 10 aprile 2018, dal D.Lgs.n.184 dell'8 novembre 2021 e dal D.Lgs n. 150 del 10 Ottobre 2022)	Questo reato si configura quando chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.
- Abuso d'ufficio (Art. 323 c.p. inserito da D.Lgs.n.75 del 14 luglio 2020)	Condotte corruttive di pubblico ufficiale o incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto violando la legge nello svolgimento delle sue funzioni.
- Traffico di influenze illecite (Art.346-bis c.p. modificato da L.3 del 9 gennaio 2019)	Tale previsione è volta a punire condotte di accordi corruttivi: essa punisce chi si offre di mettere in contatto un soggetto con un pubblico ufficiale al fine di porre in essere un accordo illecito, in cambio di promessa o della dazione di denaro.

Tra le attività sensibili relative a tale area emerse dall'analisi dei rischi si ricordano:

DIREZIONE/U.O. RESPONSABILI	PROCESSO 231	ATTIVITA' PER PROCESSO

S.I.A.	Gestire le infrastrutture	FS-4.1 Gestire la rete informatica FS-4.2 Gestire le infrastrutture di sede

2.3. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE

2.3.1. Principi

La presente Sezione è inerente alle condotte poste in essere dai soggetti destinatari del Modello che operano, in particolare, nelle aree a Rischio reato informatico e nello svolgimento delle attività sensibili precedentemente citate

Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Sezione, in linea generale ed al fine di perseguire la prevenzione dei Reati Informatici è fatto espresso divieto a tutti i Soggetti coinvolti di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'Art. 24-bis del D.Lgs.n.231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Sezione

In generale, la prevenzione dei crimini informatici è svolta attraverso adeguate misure tecnologiche, organizzative e normative ed in particolare almeno attraverso l'applicazione dei seguenti controlli di carattere generale:

- Previsione nel Codice Etico di specifiche indicazioni volte a impedire la commissione dei reati informatici sia all'interno della società che tramite apparecchiature non soggette al controllo della stessa
- Previsione di un idoneo sistema di sanzioni disciplinari (o vincoli contrattuali nel caso di terze parti) a carico dei dipendenti (o altri destinatari del Modello) che violino in maniera intenzionale i sistemi di controllo o le indicazioni comportamentali fornite
- Predisposizione di adeguati strumenti tecnologici atti a prevenire e/o impedire la realizzazione di reati informatici da parte dei dipendenti e in particolare di quelli appartenenti alle strutture della società ritenute più esposte al rischio
- Predisposizione di programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali.

2.3.2. Norme generali di comportamento

- Esistenza di una normativa/procedura aziendale relativa a:
  1. Gestione degli accessi che tra l'altro individua le seguenti fasi:
     - Attribuzione accessi
     - Assegnazione dei codici identificativi personali (richieste di abilitazione/modifica delle utenze)

- Disattivazione dei codici utente associati al personale che ha perso il diritto di accesso a tutti i sistemi informatici o che non accede più ai vari sistemi
- Attività di controllo volta a verificare, prima della creazione di un'utenza, che la stessa non sia già stata precedentemente assegnata/disabilitata/rimossa e che uno stesso codice identificativo personale non venga assegnato, neppure in tempi diversi, a persone diverse

2. Modalità di utilizzo e di salvaguardia del PC intese come misure che l'utente deve adottare per garantire un'adeguata Protezione delle apparecchiature incustodite
3. Installazione di software sui sistemi operativi
4. Dismissione dei supporti di memorizzazione su cui sono registrate informazioni aziendali

- Attuazione di un sistema di accesso logico idoneo a controllare che le attività di utilizzo delle risorse da parte dei processi e degli utenti e di accesso alla rete si esplichino attraverso la verifica e la gestione dei diritti d'accesso
- Presenza di sistemi di protezione antivirus e antispam
- Esistenza di una serie di procedure, in materia di "privacy" e di "security", che disciplinano gli aspetti legati al corretto utilizzo delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni
- Attuazione del progetto di formazione, volta a sensibilizzare tutti gli utenti e/o particolari figure professionali, con l'obiettivo di diffondere all'interno della società le politiche, gli obiettivi e i piani previsti in materia di sicurezza informatica e al fine di soddisfare i requisiti previsti in materia di privacy
- Consegna a ciascun dipendente della Società, contestualmente all'assegnazione del pc e/o dell'indirizzo di posta Internet di norme per l'utilizzo dei Personal Computer aziendali e sull'utilizzo della posta Internet e in generale di documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico
- Individuazione tempestiva delle vulnerabilità dei sistemi
- Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che costituiscono il patrimonio dell'azienda oggetto di protezione (risorse tecnologiche e informazioni), attraverso, l'adozione di sistemi antincendio, antiallagamento, di condizionamento, gruppi di continuità UPS e di regolamentazione degli accessi
- Attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici (registrazione dei log on e log off)
- Protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di networking attraverso, tra l'altro, una serie di provvedimenti volti a garantire che:
- L'informazione inserita e elaborata dal sistema pubblico sia processata completamente ed in modo tempestivo
- Le informazioni sensibili siano protette durante i processi di raccolta e di conservazione
- L'accesso al sistema pubblico non consenta ingressi fortuiti alle reti con cui è connesso

2.3.3. Presidi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.), gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nello svolgimento delle attività a rischio sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all'Art.24-bis del D.Lgs.n.231/01, al rispetto delle regole e procedure aziendali emesse a regolamentazione di tale attività a rischio

Tali regole e procedure prevedono controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area. In particolare, si elencano qui di seguito le regole che devono essere rispettate dalla società e dai dipendenti e dagli altri soggetti eventualmente autorizzati nell'ambito delle Attività Sensibili

- I dati e le informazioni non pubbliche, relative anche a clienti e terze parti (commerciali, organizzative, tecniche), incluse le modalità di connessione da remoto, devono essere gestiti come riservati
- È vietato introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del soggetto responsabile individuato
- È vietato in qualunque modo modificare la configurazione di postazioni di lavoro fisse o mobili effettuata dal servizio infrastrutture
- È vietato acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.)
- È vietato ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla società
- È vietato divulgare, cedere o condividere con personale interno o esterno all'azienda le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti
- È vietato accedere ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti
- È vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi
- È vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi
- È vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi
- È vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi

- È vietato comunicare a persone non autorizzate, interne o esterne alla società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati
- È proibito distorcere, oscurare sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati
- È vietato lo spamming come pure ogni azione di risposta allo spam
- È obbligatorio segnalare all'organismo di vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Sezione sia stato commesso o possa essere commesso.

L'azienda si impegna a porre in essere i seguenti adempimenti:

- Informare adeguatamente i dipendenti e gli altri soggetti eventualmente autorizzati dell'importanza di mantenere i propri codici di accesso (username e password) confidenziali e di non divulgare gli stessi a soggetti terzi (cfr. Manuale utilizzo user id e password)
- Fare sottoscrivere ai dipendenti e agli altri soggetti eventualmente autorizzati uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo delle risorse informatiche aziendali
- Informare i dipendenti e agli altri soggetti eventualmente autorizzati della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccare l'accesso al pc "lock computer", qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso (cfr. Manuale utilizzo user id e password)
- Impostare i sistemi informatici in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente
- Fornire un accesso da e verso l'esterno (connessione alla rete internet) esclusivamente ai sistemi informatici dei dipendenti o di eventuali soggetti terzi che ne abbiano la necessità ai fini lavorativi o connessi all'amministrazione societaria
- Limitare gli accessi alla stanza server unicamente al personale autorizzato
- Proteggere, per quanto possibile, ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle
- Fornire ogni sistema informatico di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati
- Impedire l'installazione e l'utilizzo di software non approvati dalla società e non correlati con l'attività espletata per la stessa
- Limitare l'accesso alle aree ed ai siti internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "virus") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e file)
- Impedire l'installazione e l'utilizzo, sui sistemi informatici della società, di software (c.d. "p2p", di files sharing o di istant messaging) mediante i quali è possibile scambiare con altri soggetti

all'interno della rete internet ogni tipologia di file (quali filmati, documenti, canzoni, virus, ecc.) Senza alcuna possibilità di controllo da parte della società

- Qualora per la connessione alla rete internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna wi-fi), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni all'azienda, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti
- Prevedere un procedimento di autenticazione mediante username e password al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei dipendenti e degli altri soggetti eventualmente autorizzati (Cfr. Manuale utilizzo user Id e password)
- 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 dipendenti e degli altri soggetti eventualmente autorizzati (i.e. Connessione tramite VPN o RAS)
- Effettuare periodicamente, in presenza di accordi sindacali che autorizzino in tale senso e ove possibile, controlli ex ante ed ex post sulle attività effettuate dal personale sulle reti nonché, quando verrà completato il progetto di anomaly detection, rielaborare con regolare cadenza i log dei dati al fine di evidenziare eventuali comportamenti anomali.

La Società, inoltre, si è dotata di un *Regolamento per la gestione delle risorse informatiche* e di un assetto di procedure specifiche, conformi alle disposizioni normative in materia di privacy di cui al Reg. UE 679/2016 (GDPR) che costituisce, unitamente al Codice Etico, il presidio comportamentale di maggiore rilevanza in materia, disciplinando doveri e divieti in materia informatica a carico del personale e prevedendo specifiche sanzioni in caso di violazione.
Inoltre essa utilizza, quali presìdi fisici, una serie di misure tecniche sul sistema informativo per garantire la sicurezza e la protezione dei dati, prevenire possibili attacchi esterni e garantire un corretto utilizzo da parte del personale.
Si integrano infine nel MOG i presìdi previsti dalle misure di sicurezza in materia di protezione dei dati personali, previsti dalla vigente normativa.
Il fabbisogno formativo per il personale in materia di tutela e trattamento dei dati, di utilizzo dei sistemi informativi e relativi potenziali reati, è oggetto di analisi in sede di stesura del piano annuale della formazione ed alla conseguente attività di erogazione e di registrazione.
Tra le misure tecniche adottate dall'azienda si citano le seguenti:

- Sistemi di autenticazione informatica per l'accesso ai sistemi informatici (accesso al personal computer, accesso ai programmi, accesso alle banche dati esterne). Le chiavi di accesso (password) sono gestite secondo le indicazioni del Regolamento Informatico.
- Sistemi di autorizzazione attraverso la profilazione dei singoli utenti (o gruppi di utenti) nell'utilizzo delle risorse informatiche (compresi programmi gestionali e contabili), con la funzione di limitare l'accesso ai soli dati di propria competenza, in base alle regole organizzative della Società. Il Responsabile dei sistemi informatici predispone e cura l'aggiornamento di una matrice che evidenzia i profili di accesso ai sistemi, in base alle autorizzazioni fornite dai rispettivi responsabili.

- Altre misure tecniche previste dalla vigente normativa in materia di tutela e trattamento dei dati ed attività di audit previste a carico dell'amministratore di sistema.

Naturalmente si sottolinea come la rapida evoluzione dal lato tecnologico impone frequenti aggiornamenti ed adeguamenti dei protocolli vigenti, per accrescerne la loro efficacia complessiva. A questo fine ogni anno il responsabile dei sistemi informativi, nell'ambito della procedura di stesura del bilancio previsionale, esegue una valutazione dei fabbisogni di spesa per aggiornamenti tecnici o formativi.

2.4. I CONTROLLI DELL'ORGANISMO DI VIGILANZA

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui all'Art. 24-bis del Decreto, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'Art. 24-bis del Decreto sono i seguenti:

- Svolgere verifiche periodiche sul rispetto della presente Sezione e dei presidi sopra individuati e valutare regolarmente la sua efficacia a prevenire la commissione dei delitti di cui all'Art. 24-bis del Decreto; con riferimento a tale punto, l'OdV condurrà controlli a campione sulle attività potenzialmente a rischio di delitti informatici, diretti a verificare la corretta applicazione di regolamenti, procedure e protocolli in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere
- Verificare l'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni.
- Proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei delitti informatici di cui alla presente Sezione, anche in considerazione del progresso e dell'evoluzione delle tecnologie informatiche
- Consultarsi con il responsabile della Sicurezza Informatica e/o del Servizio Sistemi Informativi ed invitare periodicamente lo stesso a relazionare alle riunioni dell'OdV
- Esaminare la relazione annuale del DPO ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione evidenze ricevute chiedendo se necessario di incontrarlo.
- Esaminare i flussi informativi periodici ed eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute

2.4.1. Flussi informativi verso l'organismo di vigilanza

Sussiste a carico di tutti i Destinatari del MOG (soggetti apicali, sottoposti, consulenti, etc.) l'**obbligo di segnalazione immediata all'OdV** in caso di notizie rilevanti sulla vita dell'Ente, violazioni del Modello, della presente Parte Speciale o situazioni di riscontrata inadeguatezza e/o non conformità di comportamenti ai principi contenuti nelle procedure/istruzioni aziendali e nel Codice Etico.
Le segnalazioni di illeciti, secondo le istruzioni impartite dall'OdV, dovranno avvenire con le modalità indicate nell'apposita **Procedura "*Flussi Informativi*",** nel rispetto della normativa in tema di *Whistleblowing*.
Con riferimento ai controlli periodici sui processi aziendali e allo svolgimento delle normali attività il D.Lgs. n. 231/01 prevede **flussi informativi con cadenze determinate** verso l'OdV da parte di specifici soggetti. Si rinvia alla **Procedura "*Flussi Informativi*",** allegata al Modello, per la descrizione delle specifiche modalità operative con cui dovranno essere inviati i suddetti flussi.

SEZIONE 3:

REATI SOCIETARI

(ART. 25-TER)

3. ART. 25-TER – REATI SOCIETARI

3.1. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS.N.231/01

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex Art. 5 del D.Lgs.n.231/2001 è collegato il regime di responsabilità a carico della società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

La presente Sezione si riferisce ai reati societari.

Le fattispecie di reato di cui all'Art. 25-ter D.Lgs. 231/2001 sono le seguenti:

- False comunicazioni sociali (art. 2621 c.c.).
- False comunicazioni sociali – fatti di lieve entità (art. 2621-bis, c.c.).
- False comunicazioni sociali delle società quotate (art. 2622 c. c.).
- Falsità nelle relazioni o nelle comunicazioni delle società di revisione [1](art. 2624, co. 1 e 2, c.c.).
- Impedito controllo (art. 2625, co. 2, c.c.).
- Indebita restituzione di conferimenti (art. 2626 c.c.).
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.).
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.).
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.).
- Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.).
- Formazione fittizia del capitale (art. 2632 c.c.).
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.).
- Illecita influenza sull'assemblea (art. 2636 c.c.).
- Aggiotaggio (art. 2637 c.c.).

[1] L'articolo 2624 del codice civile, che disciplinava le falsità nelle relazioni o nelle comunicazioni della società di revisione, è stato abrogato dall'art. 37, co. 34, d. lgs.27 gennaio 2010, n. 39 (Testo unico della revisione legale dei conti). La corrispondente fattispecie di reato è stata trasferita nell'art. 27 del citato decreto, ma non è richiamata nel presente art. 25- ter, D.Lgs. 231/2001. Secondo autorevole dottrina ciò comporta la fuoriuscita di entrambi i reati dalla sfera dei fatti di reato rilevanti ai sensi del D.Lgs. 231/2001.

- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, co. 1 e 2, c.c.).
- Corruzione tra privati (art. 2635 co. 3 c.c.)[2].
- Istigazione alla corruzione tra privati (art. 2635-bis c.c.)[3].

3.2. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA

Di seguito si riporta una breve descrizione dei reati societari richiamati dall'Art. 25-ter (Reati societari) del D.Lgs.n.231/01 che si ritiene potrebbero trovare manifestazione nell'ambito delle attività svolte dall'azienda.

Reato	Esempio di condotta
• False comunicazioni sociali (Artt. 2621 c.c., 2621-bis c.c., 2621-ter c.c.)	Il Consiglio di Amministrazione ignora l'indicazione del responsabile amministrativo circa l'esigenza di un accantonamento (rettifica) al Fondo svalutazione crediti a fronte della situazione di crisi di un cliente, ed iscrive un ammontare di crediti superiore al dovuto; ciò al fine di non far emergere una perdita che comporterebbe l'assunzione di provvedimenti sul capitale sociale (artt. 2446 e 2447 del Codice civile).
• Impedito controllo (Art. 2625 c.c. modificato da D.Lgs.n.39 del 27 gennaio 2010)	Un funzionario della società rifiuta di fornire all'Organo di controllo i documenti richiesti per l'espletamento dell'incarico, quali, ad esempio, quelli concernenti le azioni legali intraprese dalla società per il recupero di crediti.
• Indebita restituzione dei conferimenti (Art. 2626 c.c.)	L'Assemblea dell'azienda, su proposta del Consiglio di Amministrazione, delibera la compensazione di un debito di un socio nei confronti della società con il credito da conferimento che quest'ultima vanta nei confronti del socio medesimo, attuando di fatto una restituzione indebita del conferimento.
• Illegale ripartizione degli utili o delle riserve (Art. 2627 c.c.)	L'Assemblea della Società, su proposta del Consiglio di Amministrazione, delibera la distribuzione di dividendi che costituiscono, non un utile di esercizio, ma fondi non distribuibili perché destinati dalla legge a riserva legale.
• Operazioni in pregiudizio dei creditori (Art. 2629 c.c.)	L'organo amministrativo delibera una riduzione del capitale sociale senza osservare i presupposti richiesti dalla legge, cagionando in tal modo un danno ai creditori sociali.
• Formazione fittizia del capitale (Art. 2632 c.c.)	L'Assemblea dell'azienda, su proposta del Consiglio di Amministrazione, delibera l'aumento del capitale sociale con un conferimento di beni sopravvalutati in modo rilevante.

[2] La fattispecie di reato ha subito modifiche con il decreto legislativo 15.3.2017 n. 38, di attuazione della decisione quadro 2003/568/GAI, relativa alla lotta contro la corruzione nel settore privato. Il provvedimento è entrato in vigore il 14.04.2017.
[3] Fattispecie di reato introdotta in seno all'art. 25 ter, lett. S-bis con il Decreto Legislativo n. 38 del 15/03/2017.

• Corruzione tra privati (Art. 2635 c.c. modificato dalla L. n.3 del 9 gennaio 2019)	Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altre utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni
• Istigazione alla corruzione tra privati (Art. 2635-bis c.c. modificato dalla L. n.3 del 9 gennaio 2019)	Offrire o promettere denaro o altre utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà.
• Illecita influenza sull'assemblea (Art. 2636 c.c.)	Il Consiglio di Amministrazione della società, al fine di ottenere una deliberazione favorevole dell'assemblea e il voto determinante anche del socio di maggioranza, predispone e produce nel corso dell'adunanza assembleare documenti alterati, diretti a far apparire migliore la situazione economica e finanziaria di un'azienda che lo stesso Consiglio di Amministrazione intende acquisire, in modo da ricavarne un indiretto profitto.

Con riferimento all'ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, co. 1 e 2, c.c.) va precisato che il termine "Autorità pubblica di Vigilanza" (letteralmente, "autorità di vigilanza") è chiaramente generico, completamente indeterminato e fa sorgere rilevanti dubbi interpretativi. In maniera precauzionale il termine è stato interpretato in maniera tale da includere tutte le autorità amministrative esistenti nel nostro sistema giuridico senza considerare il tipo di vigilanza concretamente svolto dalle stesse e l'indipendenza dal potere politico: pertanto, l'Autorità garante per la protezione dei dati personali, così come l'autorità garante della concorrenza e del mercato e l'autorità per la garanzia nelle comunicazioni oltre che l'ANAC possono essere considerate autorità di vigilanza.

Dato quanto sopra, il reato di cui all'articolo 2638 c.c. deve essere riferito a specifiche e determinate tipologie di informazione, che possono attenere alla posizione economica e finanziaria del soggetto sottoposto alla vigilanza dell'autorità in questione. Tale requisito richiesto dalla legge limita la sua applicazione e richiede di riflettere sulla tipologia di dati e informazioni che nel caso specifico verranno comunicati all'autorità di vigilanza, in quanto il reato si realizza solo quando l'informazione comunicata ha le caratteristiche previste dalla legge. Si ritiene per tali ragioni remota la probabilità di commissione di tali reati i ui soggetti attivi sono gli amministratori, i direttori generali, i sindaci e i liquidatori.

Anche gli altri reati previsti dall'art. 25-ter non sono stati, allo stato attuale, valutati rilevanti in quanto la probabilità di commissione di tali reati è ritenuta remota.

Tra le attività sensibili relative a tale area emerse dall'analisi dei rischi si ricordano:

DIREZIONE/U.O. RESPONSABILI	PROCESSO 231	ATTIVITA' PER PROCESSO
Manu.ne Straordinaria All. di Risulta	Programmazione, Progettazione interventi, Direzione dei lavori, esecuzione	FO-2.1 Progettazione degli interventi di manutenzione straordinaria FO-2.2 Studio di fattibilita' dei lavori e progettazione preliminare FO-2.3 Progettaz. definitiva ed esecutiva commesse di costruzione e recupero FO-2.4 Verifica della progettazione FO-4.1 Gestire gli adempimenti per la Direzione lavori FO-4.2 Effettuare la Direzione dei lavori FO-4.3 Eseguire l'Ultimazione dei lavori e il Collaudo
S.I.A.	Gestione della bollettazione e della fatturazione attiva	FO-5.3 Gestire la bollettazione e la fatturazione
Ragioneria	Gestire l'Amministrazione e la Contabilità	FS-1. Gestire l'Amministrazione e la Contabilità
Ragioneria / CdA	Elaborare il bilancio di esercizio	Elaborare il bilancio di esercizio
Segr. L.O.D.E. Lucchese – C.d.A.	Gestione adempimenti societari e rapporti con gli Organi	Gestione adempimenti societari e rapporti con gli Organi
Patrimoniale	Gestire il Patrimonio	FO-6.3 Gestione delle vendite di unita' immobiliari

3.3. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE

3.3.1. Principi

Con riferimento al processo "Programmazione, Progettazione interventi, Direzione dei lavori, esecuzione" astrattamente a rischio di commissione del **reato di corruzione tra privati** si rimanda ai presidi indicati nella Sezione sui reati contro e nei rapporti con la P.A..

Il personale dell'ERP LUCCA, a qualsiasi titolo coinvolto nel processo in oggetto, è tenuto ad osservare le modalità esposte nei regolamenti e procedure aziendali, le previsioni di legge esistenti in materia, le previsioni contenute nel Codice Etico e nel Modello di Organizzazione, Gestione e Controllo ex D.Lgs.231/2001 adottati.

Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Sezione, in linea generale ed al fine di perseguire la prevenzione dei Reati Societari è fatto espresso divieto a tutti i Soggetti destinatari del Modello 231 di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'art. 25-ter del D.Lgs.n.231/01, nonché di porre in

essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Sezione.

Con riferimento a quanto espresso sopra la società obbliga i suoi Amministratori, dipendenti e soggetti terzi che agiscono in rappresentanza della società al rispetto, in particolare, dei seguenti principi:

- nella gestione delle attività contabili devono essere osservate scrupolosamente le regole di corretta, completa e trasparente contabilizzazione, secondo i criteri indicati dalla legge e dai principi contabili nazionali o internazionali applicabili, in modo tale che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima, coerente e congrua;
- nello svolgimento delle attività di verifica e controllo da parte del Collegio dei revisori (o di eventuali altri organi interni o esterni) è necessario agire con trasparenza e prestare la massima collaborazione;
- le registrazioni contabili possono essere effettuate esclusivamente dai soggetti abilitati all'utilizzo del sistema informativo gestionale e contabile adottato dall'Azienda;
- ciascuna registrazione contabile deve riflettere esattamente le risultanze della documentazione di supporto. Pertanto, sarà compito del dipendente a ciò incaricato, fare in modo che la documentazione di supporto sia facilmente reperibile e ordinata secondo criteri logici;
- eventuali operazioni straordinarie devono essere poste in essere nel rispetto della disciplina prevista dal Codice Civile;

La Società condanna tramite l'applicazione del Codice Sanzionatorio i comportamenti difformi ai principi sopra menzionati.

Quanti venissero a conoscenza di omissioni, manomissioni, falsificazioni o trascuratezza della contabilità o della documentazione di supporto sulla quale le registrazioni contabili si fondano, sono tenuti a riferire i fatti al responsabile individuato nel Legale rappresentante e all'Organismo di Vigilanza.

Per ogni operazione contabile deve essere conservata agli atti sociali un'adeguata documentazione di supporto dell'attività svolta, in modo da consentire:

- L'agevole registrazione contabile
- L'individuazione dei diversi livelli di responsabilità
- La ricostruzione accurata dell'operazione, anche al fine di ridurre la probabilità di errori interpretativi

Le operazioni o i fatti gestionali sensibili e/o rilevanti deve essere documentati, coerenti e congrui, così che in ogni momento sia possibile identificare la responsabilità di chi ha operato (valutato,

deciso, autorizzato, effettuato, rilevato nei libri, controllato l'operazione). Le responsabilità di ciascuna operazione/processo aziendale devono essere chiaramente e formalmente definite.

3.3.2. Norme generali di comportamento

A titolo esemplificativo e non esaustivo, non è consentito:

- porre in essere operazioni simulate o diffondere notizie false sull'Ente e sulle sue attività;
- rappresentare o trasmettere per l'elaborazione e la rappresentazione in Bilancio, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria dell'Ente;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria dell'Ente;
- porre in essere 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 e di revisione affidata da legge alla Regione o al Collegio dei Revisori;
- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, le segnalazioni previste dalle leggi e dalla normativa applicabile nei confronti delle autorità di vigilanza cui è soggetta l'attività aziendale, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette autorità;
- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie dell'Ente.

3.3.3. Presidi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, dovranno tener conto, oltre a quanto precedentemente definito delle procedure e regole aziendali che prevedono:

- i dati e le informazioni devono essere trasmetti alla funzione responsabile attraverso un sistema che consente la tracciatura dei singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema
- Il rispetto del calendario di chiusura, finalizzato alla redazione del bilancio indicante:

  a) Data di chiusura dei periodi contabili
  b) Data di chiusura delle scritture contabili
  c) Data di predisposizione della Bozza del Bilancio e del Bilancio Definitivo

- Il supporto documentale a corredo delle informazioni e dei dati forniti dal Responsabile di cui al punto precedente

- Il controllo, da parte del consulente esterno incaricato nella predisposizione del bilancio delle voci aggregate di Bilancio confrontandole con quelle dell'anno precedente, mantenendo evidenza del riscontro effettuato e delle eventuali motivazioni relative a scostamenti anomali

- La tracciabilità informatica delle operazioni effettuate

- La tracciabilità dell'invio della bozza del Bilancio, alcuni giorni precedenti l'approvazione da parte dell'Amministratore Unico per permettere allo stesso la verifica delle connotazioni essenziali del bilancio prima che sia sottoposto all'Assemblea per l'approvazione

Si dispone l'attuazione dei seguenti presidi integrativi:

- Previsione di riunioni tra Organo di controllo e Organismo di Vigilanza per verificare l'osservanza della disciplina in tema di normativa societaria e di corporate governance
- Trasmissione al Collegio Sindacale, con congruo anticipo, di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del Consiglio di Amministrazione o sui quali esso debba esprimere un parere ai sensi di legge
- Partecipazione dell'organismo di Vigilanza alle riunioni assembleari mediante apposito invito predisposto dalla funzione Segreteria Generale. L'Organismo di Vigilanza valuterà l'utilità della propria partecipazione

3.4. I CONTROLLI DELL'ORGANISMO DI VIGILANZA

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di reati societari diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della società.

Inoltre, i compiti dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati societari sono i seguenti:

- Prevedere dei controlli sull'applicazione dei presidi specifici sopra individuati e laddove
- Proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Sezione
- Monitorare il rispetto delle procedure interne per la prevenzione dei reati societari.
- Incontrare l'Organo di controllo per verificare l'osservanza della disciplina in tema di normativa societaria e di corporate governance.
- Verificare l'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni.

- Esaminare le relazioni annuali dell'Organo di controllo e di quello di revisione (se non coincidenti) verificando la loro conformità agli standard professionali (Norme di comportamento e ISA) nonchè il superamento di eventuali rilievi e/o raccomandazioni.
- Esaminare eventuali segnalazioni specifiche e i flussi periodici provenienti dagli Organi Societari, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni/informazioni ricevute

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

3.4.1. Flussi informativi verso l'organismo di vigilanza

Sussiste a carico di tutti i Destinatari del MOG (soggetti apicali, sottoposti, consulenti, etc.) l'**obbligo di segnalazione immediata all'OdV** in caso di notizie rilevanti sulla vita dell'Ente, violazioni del Modello, della presente Parte Speciale o situazioni di riscontrata inadeguatezza e/o non conformità di comportamenti ai principi contenuti nelle procedure/istruzioni aziendali e nel Codice Etico.
Le segnalazioni di illeciti, secondo le istruzioni impartite dall'OdV, dovranno avvenire con le modalità indicate nell'apposita **Procedura "*Flussi Informativi*",** nel rispetto della normativa in tema di *Whistleblowing*.
Con riferimento ai controlli periodici sui processi aziendali e allo svolgimento delle normali attività il D.Lgs. n. 231/01 prevede **flussi informativi con cadenze determinate** verso l'OdV da parte di specifici soggetti. Si rinvia alla **Procedura "*Flussi Informativi*",** allegata al Modello, per la descrizione delle specifiche modalità operative con cui dovranno essere inviati i suddetti flussi.

SEZIONE 4:

REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME (ART. 25-SEPTIES)

4. ART. 25-SEPTIES – REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSI IN VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

4.1. INTRODUZIONE E FUNZIONE DEL REATO DI OMICIDIO COLPOSO E LESIONI COLPOSE COMMESSE CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE

Le fattispecie di reato di cui all'Art. 25-septies D.Lgs. 231/2001 sono le seguenti:

- Omicidio colposo (art. 589 c.p.).
- Lesioni personali colpose (art. 590, co. 3, c.p.).

Le norme in esame tutelano la vita e l'incolumità dei lavoratori. In particolare, viene sanzionata penalmente l'inosservanza di precetti cautelari contenuti nelle norme in materia di prevenzione di infortuni sul lavoro e malattie professionali, a seguito della quale si verifichino la morte o lesioni gravissime o gravi del lavoratore.

I reati contro la persona sono ipotesi aggravate dei delitti di omicidio colposo e lesioni personali colpose.

Tale aggravante consiste nella violazione delle norme per la prevenzione degli infortuni sul lavoro, sussiste non soltanto quando sia contestata la violazione di specifiche norme per la prevenzione degli infortuni sul lavoro, ma anche quando la contestazione ha per oggetto l'omissione dell'adozione di misure e/o accorgimenti per la più efficace tutela dell'integrità fisica dei lavoratori e, più in generale, la violazione di tutte le norme che, direttamente o indirettamente, tendono a garantire la sicurezza del lavoro in relazione all'ambiente in cui deve svolgersi.

- **Omicidio colposo (art. 589 c.p.).**

I soggetti che possono rispondere del reato sono tutti i soggetti tenuti ad osservare o far osservare le norme di prevenzione o protezione, vale a dire i datori di lavoro, i dirigenti, i preposti, i soggetti destinatari delle deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro nonché i medesimi lavoratori.

La colpa, nel caso che ci interessa, consiste nell'avere il soggetto agito in violazione delle norme sulla prevenzione degli infortuni sul lavoro o meglio nella mancata adozione delle misure di sicurezza e prevenzione tecnicamente possibili e concretamente attuabili alla luce dell'esperienza e delle più avanzate conoscenze tecnico scientifiche.

Se il reato in oggetto è commesso con violazione delle norme per la prevenzione degli infortuni sul lavoro, la pena è della reclusione da due a sette anni.

Le misure di sicurezza vanno intese sia in senso statico vale a dire quale obbligo di adottare le misure di protezione e sicurezza oggettiva, sia in senso dinamico da intendersi come obbligo di formare ed informare i lavoratori circa i rischi propri dell'attività lavorativa nonché sulle misure idonee per evitare i rischi o ridurli al minimo.

La colpa per violazione delle norme per la prevenzione degli infortuni sul lavoro, pertanto, può essere ravvisata non solo in caso di violazione delle specifiche norme per la prevenzione degli infortuni sul lavoro ma anche nel caso in cui l'evento (che in caso di omicidio consiste nella morte) dipenda dall'omessa adozione di quelle misure ed accorgimenti imposti all'imprenditore ai fini della tutela dell'integrità fisica e della personalità del lavoratore da differenziare a seconda della tipologia di lavoro e tenendo conto della tecnica e dell'esperienza (Art. 2087 del codice civile).

L'ente risponde, ai sensi del D.Lgs.n.231/2001, qualora abbia tratto un vantaggio dall'evento dannoso che può consistere, ad esempio, in un risparmio di costi o di tempi per non aver adottato le misure di prevenzione degli infortuni sul lavoro.

Il datore di lavoro risponde, ad esempio, di omicidio colposo nel caso in cui la morte sia derivata dall'inosservanza delle norme sulla prevenzione degli infortuni sul lavoro qualora l'evento della morte si sia verificato nei confronti di un dipendente oppure di un soggetto estraneo all'ambiente di lavoro purché la presenza sul luogo di lavoro non sia eccezionale o atipica.

- **Lesioni personali colpose gravi e gravissime (Art. 590, comma 3 c.p.)**

Tale ipotesi di reato si configura nei confronti di "Chiunque cagiona per colpa una lesione personale".

La colpa richiesta dall'Art. 25-septies del D.Lgs.n.231/2001, consiste nella violazione delle norme per la prevenzione degli infortuni sul lavoro e di igiene e sicurezza. L'ente risponde ai sensi del D.Lgs.n.231/2001 sia per le ipotesi di lesioni gravi che per i casi di lesioni gravissime qualora abbia tratto un vantaggio concreto da intendersi, ad esempio, come già si è detto, quale una riduzione dei costi per approntare le misure di sicurezza richieste dalla normativa vigente o, comunque, dovute in considerazione delle nuove acquisizioni tecnologiche.

Il delitto, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relativi all'igiene del lavoro o che abbiamo determinato una malattia professionale, è perseguibile d'ufficio.

Se il reato è commesso con violazione delle norme per la prevenzione degli infortuni sul lavoro, la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da 500 euro a 2.000 Euro e la pena per le lesioni gravissime è della reclusione da uno a tre anni.

Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo, ma la pena della reclusione non può superare gli anni cinque.

Ai sensi del comma 1 dell'Art. 583 cod. penale, la lesione è considerata **grave** nei seguenti casi:

1. Se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni
2. Se il fatto produce l'indebolimento permanente di un senso o di un organo

Ai sensi del comma 2 dell'Art. 583 cod. penale, la lesione è considerata invece **gravissima** se dal fatto deriva:

1. Una malattia certamente o probabilmente insanabile
2. La perdita di un senso
3. La perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella
4. La deformazione, ovvero lo sfregio permanente del viso

Esclusione della responsabilità amministrativa della società

Come già indicato nella Parte Generale del Modello, il D.Lgs.n.81/2008, all'Art. 30, ha indicato le caratteristiche e i requisiti che deve un modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al Decreto.

Pertanto, nella predisposizione del Modello e nella definizione degli standard di controllo la società ha tenuto conto:

- Delle previsioni del Decreto
- Della vigente disciplina legislativa della prevenzione dei rischi lavorativi
- Della ISO 45001:2018
- Delle Linee Guida Confindustria
- Dell'Art. 30 del D.Lgs.n.81/2008

4.2. TERMINI E FIGURE RELATIVE ALLE NORME PER LA SALVAGUARDIA DELLA SALUTE E SICUREZZA SUL LAVORO.

- **ASPP o Addetti al Servizio di Prevenzione e Protezione**

I soggetti in possesso delle capacità e dei requisiti professionali di cui all'art. 32 del Decreto Sicurezza designati per l'espletamento dei compiti rientranti nel Servizio di Prevenzione e Protezione.

- **Cantiere Temporaneo o Mobile o Cantiere**

Qualunque luogo in cui si effettuano lavori edili o di ingegneria civile così come individuati nell'allegato X del Decreto Sicurezza, ovvero, lavori di costruzione, manutenzione, riparazione, demolizione, conservazione, risanamento, ristrutturazione, equipaggiamento, trasformazione, rinnovamento o smantellamento di opere fisse, permanenti o temporanee, comprese le linee elettriche e le parti strutturali degli impianti elettrici. Sono, inoltre, lavori di costruzione edile o di ingegneria civile gli scavi ed il montaggio e lo smontaggio di elementi prefabbricati utilizzati per i lavori edili o di ingegneria civile.

- **Committente**

Il soggetto per conto del quale viene realizzata l'intera opera edile o di ingegneria civile, indipendentemente da eventuali frazionamenti della sua realizzazione secondo quanto disposto dagli artt. 88 e ss. del Decreto Sicurezza.

- **Coordinatore per l'Esecuzione dei Lavori**

Il soggetto incaricato dal committente o dal responsabile dei lavori tra l'altro, di verificare, con opportune azioni di coordinamento e controllo, l'applicazione, da parte delle imprese esecutrici e dei lavoratori, anche autonomi, delle disposizioni loro pertinenti contenute nel piano di sicurezza e coordinamento e di verificare altresì l'idoneità del piano operativo di sicurezza, assicurandone la coerenza con il primo.

- **Coordinatore per la Progettazione**

Il soggetto, incaricato dal committente o dal responsabile dei Lavori, di redigere il piano di sicurezza e di coordinamento e di predisporre un fascicolo contenente le informazioni utili ai fini della prevenzione e della protezione dai rischi cui sono esposti i lavoratori.

- **Datore di Lavoro**

Il soggetto titolare del rapporto di lavoro o, comunque, il soggetto che, secondo il tipo e l'organizzazione dell'impresa, ha la responsabilità dell'impresa stessa ovvero dell'unità produttiva in quanto titolare dei poteri decisionali e di spesa. È responsabile di provvedere all'attuazione di tutti gli obblighi fissati dal D.Lgs.n.81/08 e s.m.i. Gli obblighi non delegabili sono i seguenti:

- La valutazione di tutti i rischi e la conseguente elaborazione del documento (Art. 28 Del D.Lgs.n.81/08)
- La designazione del responsabile del servizio di prevenzione e protezione dei rischi.

- **Decreto Sicurezza**

Il Decreto Legislativo 9 aprile 2008, n. 81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e sicurezza nei luoghi di lavoro".

- **Dirigente**

Il soggetto che, in ragione delle competenze professionali e dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, attua le direttive del datore di lavoro organizzando l'attività lavorativa e vigilando sulla stessa.

- **DUVRI o Documento Unico di Valutazione dei Rischi per le Interferenze**

Il documento redatto dal datore di lavoro committente contenente una valutazione dei rischi che indichi le misure per eliminare o, ove ciò non risulti possibile, ridurre al minimo i rischi da interferenze nei contratti di appalto, d'opera o di somministrazione ai sensi dell'art. 26 del Decreto Sicurezza.

- **DVR o Documento di Valutazione dei Rischi**

Il documento redatto dal datore di lavoro contenente una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro ed i criteri per la suddetta valutazione, l'indicazione delle misure di prevenzione e protezione e dei dispositivi di protezione individuale conseguente a tale valutazione, 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 del nominativo del RSPP, del RLS e del medico competente che abbia partecipato alla valutazione del rischio, nonché l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione.

- **Fascicolo dell'Opera**

Il fascicolo predisposto a cura del coordinatore per la progettazione, eventualmente modificato nella fase esecutiva in funzione dell'evoluzione dei lavori ed aggiornato a cura del committente a seguito delle modifiche intervenute in un'opera nel corso della sua esistenza, contenente le informazioni utili ai fini della prevenzione e della protezione dei rischi cui sono esposti i lavoratori.

- **Lavoratori**

Soggetti che svolgono un'attività lavorativa nell'ambito della struttura organizzativa della società e contribuiscono, insieme al datore di lavoro, ai dirigenti ed ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro.

- **Medico Competente**

Il medico preposto all'attività di sorveglianza sanitaria. Il medico deve inoltre possedere uno dei titoli e dei requisiti formali e professionali indicati nel decreto sicurezza che collabora con il datore di lavoro, secondo quanto previsto all'Art.29 del D.Lgs.n.81/08 e s.m.i., ai fini della valutazione dei rischi

e al fine di effettuare la sorveglianza sanitaria (di cui all'Art. 41 del D.Lgs.n.81/08 e s.m.i.) ed adempiere tutti gli altri compiti di cui al decreto sicurezza.

- **Preposto**

Il soggetto che in ragione delle competenze professionali e nei limiti dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende all'attività lavorativa e garantisce l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa.

- **Reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro**

I reati di cui all'Art. 25-septies del D.Lgs.n.231/2001, ovvero l'omicidio colposo (Art. 589 c.p.) e le lesioni personali colpose gravi o gravissime (Art. 590 terzo comma c.p.) commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

- **RLS o Rappresentante dei Lavoratori per la Sicurezza**

Soggetto eletto o designato per rappresentare i lavoratori in relazione agli aspetti della salute e sicurezza sul lavoro.

- **RSPP o Responsabile del Servizio di Prevenzione e Protezione**

Il soggetto responsabile del servizio di prevenzione e protezione nominato dal datore di lavoro a cui risponde secondo quanto previsto dall'Art. 33 del D.Lgs.n.81/08 e s.m.i..

- **Responsabile dei Lavori**

Il soggetto che può essere incaricato dal committente ai fini della progettazione, dell'esecuzione o del controllo dell'esecuzione dell'opera o di una parte della procedura.

- **Sorveglianza Sanitaria**

L'insieme degli atti medici finalizzati alla tutela dello stato di salute e sicurezza dei lavoratori in relazione all'ambiente di lavoro, ai fattori di rischio professionali, ed alle modalità di svolgimento dell'attività lavorativa.

- **SPP o Servizio di Prevenzione e Protezione**

L'insieme delle persone, sistemi e mezzi esterni o interni alla società finalizzati all'attività di prevenzione e protezione dei rischi professionali.

- **SLL**

Salute e sicurezza dei lavoratori.

- **Addetto al Primo Soccorso e addetto alla prevenzione incendi**

Soggetti incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza.

- **Referente Tecnico**

Soggetto incaricato di assicurare la corretta realizzazione, in conformità alle norme e specifiche tecniche di progetto o del capitolato speciale, delle opere e dei servizi commissionati ad appaltatori/fornitori.

4.3. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA

I reati in oggetto risultano di fatto applicabili a qualsivoglia società e di conseguenza a tale logica non sfugge l'ERP LUCCA.
Le ipotesi di reato di cui all'art. 25-septies, infatti, nel contesto della Società, possono presentarsi in due diversi ambiti:

- Il primo relativo alle sedi aziendali: tale ipotesi si presenta configurabile, con una probabilità di accadimento abbastanza bassa, presso la sede principale tenendo conto delle specifiche attività di natura prettamente amministrativa svolta.
- Il secondo relativo ai cantieri esterni nei quali operano dipendenti dell'Ente in veste di stazione appaltante (es. Responsabile dei Lavori-RUP, Direttore Lavori, Direttore operativo ed ispettore di cantiere, coordinatore in fase di esecuzione).
  In questo ambito, che vede tra l'altro il sovrapporsi della normativa relativa agli appalti pubblici (D.Lgs. 50/2016), con il testo unico sulla sicurezza (D.Lgs. 81/2008), la probabilità di accadimento risulta in astratto maggiore.
  In questo ambito, tra l'altro, occorre considerare le responsabilità del Committente, del responsabile dei lavori (RUP) e delle altre figure professionali impegnate nel cantiere, a fronte di infortuni che possono interessare i dipendenti di tutte le imprese che operano in cantiere. A questo scopo, dunque, occorre ben focalizzare le attività di vigilanza e di controllo a carico del personale di ERP Lucca sul rispetto delle norme antinfortunistiche da parte delle imprese, al fine di prevenire eventuali responsabilità legate a carenze organizzative e/o omessa vigilanza.

I processi a rischio negli ambiti di cui sopra sono riconducibili a quelli definiti dall'art. 30 del D.lgs. n. 81/08 quali elementi essenziali ai fini di un sistema aziendale idoneo per l'adempimento di tutti gli obblighi giuridici relativi:

a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
d) alle attività di sorveglianza sanitaria;
e) alle attività di informazione e formazione dei lavoratori;
f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

4.4. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE

4.4.1. Principi

La presente Sezione è inerente alle condotte poste in essere dai soggetti destinatari del Modello che operano, in particolare, nelle aree a Rischio e nello svolgimento delle attività sensibili precedentemente citate.

Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Sezione, in linea generale ed al fine di perseguire la prevenzione dei Reati in materia di SSLL è fatto espresso divieto a tutti i Soggetti coinvolti di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'Art. 25-septies del D.Lgs.n.231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Sezione.

La Società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati a principi generali di:

- Conoscibilità all'interno della società
- Delimitazione dei ruoli, con una descrizione dei compiti di ciascuna funzione e dei relativi poteri
- Descrizione delle linee di riporto

Nello specifico, la società è dotata di una struttura organizzativa in conformità a quella prevista dalla normativa prevenzionistica vigente.

In coerenza con lo schema organizzativo e funzionale dell'azienda sono stati definiti i compiti e le responsabilità in materia di SSL a partire dal Datore di Lavoro fino al lavoratore.

Le misure relative alla SSL non devono in nessun caso comportare oneri finanziari per i lavoratori.

4.4.2. Norme generali di comportamento

La società, come previsto dal D.Lgs.n.81/08 e s.m.i., deve garantire il rispetto delle normative in tema di tutela della SSL, di tutela dell'ambiente nonché assicurare in generale un ambiente di lavoro sicuro, sano e idoneo allo svolgimento dell'attività, anche attraverso:

- Una continua analisi del rischio e della criticità dei processi e delle risorse da proteggere

- La programmazione della prevenzione, mirando ad un complesso che integri in modo coerente nella prevenzione e condizioni lavorative e organizzative dell'azienda nonché l'influenza dei fattori dell'ambiente di lavoro
- Il rispetto dei principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro
- L'eliminazione/riduzione al minimo dei rischi in relazione alle conoscenze acquisite in base al progresso tecnico, privilegiando gli interventi alla fonte
- La sostituzione di ciò che è pericoloso con ciò che non è pericoloso o che è meno pericoloso
- Il controllo e l'aggiornamento delle metodologie di lavoro
- Il controllo sanitario dei lavoratori, con particolare riguardo ai rischi specifici
- Attività di informazione, formazione, consultazione e partecipazione dei lavoratori ovvero dei loro rappresentanti, dei dirigenti e dei preposti sulle questioni riguardanti la sicurezza e la salute sul luogo di lavoro
- La partecipazione e consultazione dei lavoratori e dei loro rappresentanti
- La programmazione delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, anche attraverso l'adozione del Codice Etico e di buone prassi
- La formalizzazione di istruzioni adeguate ai lavoratori
- L'uso di segnali di avvertimento e sicurezza
- La regolare manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti
- La definizione di adeguate misure di emergenza da attuare in caso di pronto soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato
- Nella scelta dei fornitori di beni o servizi, ivi inclusi in materia di SSL, devono essere privilegiati l'affidabilità del fornitore e la sua capacità di assolvere correttamente alle obbligazioni assunte, oltre al rapporto qualità/prezzo del bene o della prestazione offerta.

È fatto espresso divieto di:

- Modificare o disattivare, senza autorizzazione i dispositivi di protezione individuali o collettivi
- Modificare o togliere, senza autorizzazione, i dispositivi di sicurezza o di segnalazione o di controllo
- Fabbricare, acquistare, noleggiare e utilizzare impianti, macchine, attrezzature o altri mezzi tecnici, inclusi dispositivi di protezione individuali e collettivi, non adeguati o non rispondenti alle disposizioni vigenti in materia di sicurezza
- Accedere ad aree di lavoro a cui non si è autorizzati
- Svolgere di propria iniziativa operazioni che non siano di competenza o che possano compromettere la sicurezza propria o di altri lavoratori

4.4.3. Presidi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Al fine di prevenire la commissione di reati quali quelli in oggetto, ERP LUCCA ha elaborato e aggiorna periodicamente la documentazione necessaria a comprovare la conformità ai principi di cui all'art. 30 del D.Lgs.81/08, l'esistenza di un sistema aziendale idoneo per l'adempimento di tutti gli obblighi giuridici relativi:

PROCESSI EX ART. 30 D.lgs. n. 81/08	STRUMENTI PER LA CONFORMITÀ'
a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici:	DvR
b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;	DvR
c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;	• organigramma SSLL • Protocollo gestione emergenze • Verbali riunioni periodiche • Fascicolo qualificazione imprese in appalto e attività svolta tramite la CONVENZIONE PER IL SERVIZIO DI CONTROLLO IN MATERIA DI SICUREZZASUL LAVORO DEI CANTIERI stipulata con l'Ente unico costituito da parte di ANCE, FeNEAL-UIL, FILCA CISL e FILLEA CGIL, che ai sensi dell'art.36 e seguenti del Codice civile per la formazione e la sicurezza per l'industria edilizia ed affini della provincia di Lucca e costituisce per l'edilizia l'Organismo paritetico di cui agli art.2 e 51 del D.Lgs. n.81/2008 smi
d) alle attività di sorveglianza sanitaria;	Protocollo sorveglianza sanitaria
e) alle attività di informazione e formazione dei lavoratori;	File con evidenza dello stato di aggiornamento del programma di formazione/addestramento obbligatoria e fascicoli dipendenti con attestati.
f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;	Report periodici RSPP
g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;	Documento con evidenza delle principali certificazioni e autorizzazioni e della loro scadenza/aggiornamento.

h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.	Riunione periodica SSLL, flussi informativi OdV – RSPP e audit OdV

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, etc.,) gli amministratori, gli organi sociali, i lavoratori, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, nello svolgimento delle attività sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all'Art. 25-septies, al rispetto della normativa vigente, delle regole e procedure aziendali emesse a regolamentazione delle attività a rischio.

Tali regole e procedure sono contenute nei Documenti del SGSL (Politica, Obiettivi e Programma di Miglioramento, Organigramma, etc.,).

Appalti (art. 26 D.lgs. n. 81/08)

La società predispone e mantiene aggiornato l'elenco delle aziende che operano all'interno dei propri siti con contratto d'appalto.

Le modalità di gestione e di coordinamento dei lavori in appalto, monitorate tramite la CONVENZIONE PER IL SERVIZIO DI CONTROLLO IN MATERIA DI SICUREZZASUL LAVORO DEI CANTIERI stipulata con l'Ente unico costituito da parte di ANCE, FeNEAL-UIL, FILCA CISL e FILLEA CGIL, che ai sensi dell'art.36 e seguenti del Codice civile per la formazione e la sicurezza per l'industria edilizia ed affini della provincia di Lucca e costituisce per l'edilizia l'Organismo paritetico di cui agli art.2 e 51 del D.Lgs. n.81/2008 smi, vengono formalizzate in contratti scritti nei quali siano presenti espressi riferimenti agli adempimenti in capo al Datore di Lavoro di cui all'art. 26 del Decreto Sicurezza, tra cui, in via esemplificativa:

- Verificare l'idoneità tecnico-professionale delle imprese appaltatrici in relazione ai lavori da affidare in appalto attraverso:
  - Acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato
  - Acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico professionale ai sensi dell'articolo 4 del Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445
- Fornire informazioni dettagliate agli appaltatori circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività
- Cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto
- Coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori
- Predisporre un unico DUVRI che indichi le misure adottate al fine di eliminare, o quanto meno ridurre al minimo, i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte

nell'esecuzione dell'opera complessiva; tale documento deve allegarsi al contratto di appalto o d'opera
- Verificare in fase di gestione del contratto ed esecuzione dei lavori il rispetto delle misure previste di prevenzione e protezione e il rispetto degli adempimenti di legge verso il personale di cui al punto precedente
- Assicurarsi che il personale dell'impresa appaltatrice o subappaltatrice esponga, in presenza dello specifico obbligo di legge, la tessera di riconoscimento con fotografia, dati anagrafici e indicazione del Datore di Lavoro

Nei contratti di somministrazione, di appalto e di subappalto, vengono specificamente indicati i costi relativi alla sicurezza del lavoro.
A tali dati possono accedere, su richiesta, gli RLS e le organizzazioni sindacali dei lavoratori.
Infine, nei contratti di appalto viene chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto

Conservazione documentale
La società, inoltre, garantisce che vengano adeguatamente conservati su supporto cartaceo ed informatico, e aggiornati i seguenti documenti:

- La cartella sanitaria, ove prevista, deve essere istituita e aggiornata dal medico competente e custodita dal Datore di Lavoro
- Il registro infortuni
- Verbalizzazione delle visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal medico competente
- Documenti che registrano gli adempimenti espletati in materia di sicurezza e salute sul lavoro
- Documento di Valutazione dei Rischi
- Documento di Valutazione dei Rischi integrato ("DUVRI") o POS.
- Nomina formale del Responsabile e degli Addetti al Servizio di Prevenzione e Protezione (RSPP e ASPP), del Medico Competente, degli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, nonché degli eventuali Dirigenti e Preposti

4.5. I CONTROLLI DELL'ORGANISMO DI VIGILANZA

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui all'Art. 25-septies del Decreto, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'Art. 25-septies del Decreto sono i seguenti:

- Svolgere verifiche periodiche sul rispetto della presente Sezione e dei presidi sopra individuati e valutare regolarmente la sua efficacia a prevenire la commissione dei reati di cui all'Art. 25-septies del Decreto; con riferimento a tale punto, l'OdV condurrà controlli a campione sulle attività potenzialmente a rischio, diretti a verificare la corretta applicazione di regolamenti, procedure e protocolli, completezza della documentazione indicata.
- Proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Sezione.
- Verificare l'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni.
- Proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Sezione
- L'Organismo di Vigilanza attiva una serie di scambio di informazioni con il RSPP (destinatario degli obblighi di invio dei flussi informativi periodici e delle segnalazioni ad accadimento) e le funzioni aziendali preposte alla gestione del sistema della sicurezza, al fine di attuare efficacemente le proprie attività di vigilanza.
- Esaminare i flussi informativi periodici ed eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute
- Conservare traccia dei flussi informativi periodici ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti

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

4.5.1. Flussi informativi verso l'organismo di vigilanza

Sussiste a carico di tutti i Destinatari del MOG (soggetti apicali, sottoposti, consulenti, etc.) l'**obbligo di segnalazione immediata all'OdV** in caso di notizie rilevanti sulla vita dell'Ente, violazioni del Modello, della presente Parte Speciale o situazioni di riscontrata inadeguatezza e/o non conformità di comportamenti ai principi contenuti nelle procedure/istruzioni aziendali e nel Codice Etico.
Le segnalazioni di illeciti, secondo le istruzioni impartite dall'OdV, dovranno avvenire con le modalità indicate nell'apposita **Procedura "*Flussi Informativi*",** nel rispetto della normativa in tema di *Whistleblowing*.
Con riferimento ai controlli periodici sui processi aziendali e allo svolgimento delle normali attività il D.Lgs. n. 231/01 prevede **flussi informativi con cadenze determinate** verso l'OdV da parte di specifici soggetti. Si rinvia alla **Procedura "*Flussi Informativi*",** allegata al Modello, per la descrizione delle specifiche modalità operative con cui dovranno essere inviati i suddetti flussi.

SEZIONE 5:

RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO

(ART. 25-OCTIES)

5. ART. 25-OCTIES – RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO.

5.1. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS.N.231/01

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex Art. 5 del D.Lgs.n.231/2001 è collegato il regime di responsabilità a carico della società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.
La presente Sezione si riferisce ai reati di riciclaggio, ricettazione e impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio.

Si descrivono qui di seguito le singole fattispecie di reato per le quali l'Art.25-*octies* del D.Lgs.n.231/01 prevede una responsabilità dell'ente nei casi in cui tali reati siano stati compiuti nell'interesse o a vantaggio dell'ente stesso.

Le fattispecie di reato di cui all'Art. 25-octies D.Lgs. 231/2001 sono le seguenti:

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648 bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.);
- Auto riciclaggio (art. 648-ter-1).

5.2. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA

L'art. 63 comma 3 del d.lgs. 21 novembre 2007, n. 231 ha introdotto l'art. 25-octies del D.lgs. 231/2001 che sancisce la responsabilità amministrativa dell'ente anche in relazione ai reati di ricettazione, riciclaggio e di impiego di denaro, beni o utilità di provenienza illecita commessi sul territorio nazionale dal dipendente/collaboratore nell'interesse o vantaggio dell'ente.

Successivamente la L. n. 186 del 15/12/2014, ha introdotto nel nostro ordinamento giuridico il reato di "autoriciclaggio", all'articolo 648 ter1 c.p. Il comma 5 dell'art. 3 della L. n. 186/2014 include il reato di autoriciclaggio tra i reati presupposto del D.Lgs. 231/2001 prevedendo, infatti, una modifica dell'art. 25 – octies al quale sono apportate le seguenti modificazioni: (i) al comma 1, le parole «e 648-ter» sono sostituite da «648-ter e 648-ter.1»; (ii) alla rubrica sono aggiunte le parole «nonché autoriciclaggio».

Per quanto riguarda il reato di autoriciclaggio, la particolare struttura del reato stesso rende del tutto peculiare il rapporto tra il medesimo reato ed il D.Lgs.231/2001, soprattutto alla luce delle modifiche occorse alla configurazione dei citati reati dal D. Lgs. 8 novembre 2021, n. 195.

L'art. 648-ter.1 c.p., modificato ulteriormente ad opera del citato D. Lgs. 8 novembre 2021, n. 195, sanziona, infatti, chiunque, dopo aver commesso o concorso a commettere un delitto impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Sono state così apportate varie modifiche alle fattispecie lato sensu riciclatorie (ovvero i reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio previsti rispettivamente agli artt. 648, 648-bis, 648-ter e 648-ter.1 c.p.), estendendo la platea dei reati presupposto anche alle contravvenzioni (purché punite con pena dell'arresto superiore nel massimo a un anno o nel minimo a sei mesi) e includendo i delitti colposi come presupposto anche dei reati di riciclaggio e autoriciclaggio.

Alla dilatazione del perimetro di rilevanza penale dei reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, e autoriciclaggio corrisponde una parallela dilatazione dell'area di rilevanza dei rispettivi illeciti amministrativi dipendenti da reato richiamati dall'art. 25-octies del Decreto 231/2001 e, di conseguenza, del perimetro di rischio punitivo che gli enti sono chiamati a governare.

Se, infatti, l'art. 648 ter-1 c.p., dal punto vista penale, trova applicazione nei confronti di chiunque investa il provento derivante dalla precedente commissione di un qualsiasi delitto o illeciti contravvenzionali, dalla prospettiva degli enti, l'inserimento del reato in oggetto nell'elenco dei reati presupposto di cui al d.lgs. 231/2001, apre la strada ad una serie di reati, formalmente esclusi dallo stesso decreto.

Partendo, infatti, dal presupposto che l'autoriciclaggio si configura se sussistono contemporaneamente le tre seguenti condizioni:

1. sia creata o si sia concorso a creare una provvista consistente in denaro, beni o altre utilità;
2. si impieghi la predetta provvista, attraverso un comportamento ulteriore e autonomo, in attività imprenditoriali, economiche e finanziarie;
3. si crei un concreto ostacolo alla identificazione della provenienza delittuosa della anzidetta provvista;

ne consegue che tutte le condotte illecite di cui sopra, capaci di generare profitto inteso anche come "risparmio", rappresentano un potenziale pericolo per l'ente, dal momento che la loro consumazione costituisce il primo passo per commissione del delitto di autoriciclaggio.

È quindi necessario che, anche in ambito aziendale, la prevenzione del reato di autoriciclaggio sia incentrata sulla prevenzione di delitti e illeciti contravvenzionali, in grado di generare un profitto investibile.

Tra gli illeciti in grado di costituire il presupposto per l'autoriciclaggio, ricomprendendovi solo quelli rilevanti per la società e da cui ai sensi del D.lgs. n. 231/01 può discendere la responsabilità sociale di impresa, si possono individuare i seguenti:

a) i reati societari di cui all'art. 25-ter del decreto;
b) i reati tributari di cui all'art. 25-quinquiesdecies del decreto.

Tali reati si devono tenere in considerazioni in quanto già previsti all'interno della mappatura dei rischi ed oggetto di protocolli/presidi per la riduzione dei rischi all'interno del Modello in vigore (reati di cui ai punti a), b), diversamente da quelli che, al contrario, sono stati già esclusi dalla mappatura in quanto ritenuti non applicabili nel contesto dell'attività svolta dalla Società.

Rispetto ad essi, conseguentemente, si ritiene che i presidi già individuati possano essere adeguati anche per la prevenzione dei reati in oggetto.

Per quanto riguarda la fattispecie di cui all'art. 25-octies del D.Lgs.231/01 riferita **all'Impiego di denaro, beni o utilità di provenienza illecita (Art. 648-ter c.p. modificato dal D.Lgs. n. 195 dell'8 novembre 2021)** trattasi di reati indirizzati ad enti soggetti alla disciplina antiriciclaggio (D.Lgs. 231/2007).

Tale disciplina, agli articoli dal 10 al 14, esplicita i destinatari della normativa antiriciclaggio, tra i quali sono compresi, tra l'altro, gli uffici della pubblica amministrazione ed altri operatori qualificati.

ERP LUCCA, pur non rilevando il rischio di ottenere e quindi di impiegare proventi di natura illecita (quindi di commettere i reati di riciclaggio e all'Impiego di denaro, beni o utilità di provenienza illecita), rientra nel perimetro di applicazione della disciplina del D.Lgs.231/07 e di conseguenza è destinataria degli obblighi di collaborazione attiva su cui la fattispecie sopra indicata si ancora ed in particolare dell'obbligo di segnalazione all'UIF, di tutte quelle operazioni, poste in essere da controparti contrattuali, ritenute "sospette" o quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento al terrorismo.

Il decreto, approvato dal Consiglio dei Ministri il 24 maggio 2017 (D.lgs. n. 90/17), oltre a introdurre a carico di soggetti determinati tra cui le P.A. e le società da esse partecipate una serie di obblighi di segnalazione di operazioni sospette all'Uif, riscrive integralmente, fra gli altri, il decreto legislativo n. 231/2007 in tema di contrasto al riciclaggio e al finanziamento del terrorismo, in attuazione della direttiva (UE) 2015/849 (c.d. IV Direttiva Antiriciclaggio).

La previsione di obblighi di segnalazione connessi ad operazioni da cui possono discendere violazioni di disposizioni contenute nella legislazione in materia di antiriciclaggio e conseguentemente configurarsi reati ricompresi in quelli di cui all'art. 25 octies del D.lgs. n. 231/01 impone, infatti, alle società a partecipazione pubblica di elaborare una serie di misure organizzative ad hoc astrattamente idonee a ridurre i relativi rischi.

L'articolo 10 del Decreto Legislativo n. 90 del 2017 dispone infatti che le pubbliche amministrazioni, di cui all'art. 11, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modifiche e di

cui all'art. 1, comma 2, lett. hh) nonchè i soggetti preposti alla riscossione dei tributi nell'ambito della fiscalità nazionale o locale, quale che ne sia la forma giuridica nonché le società partecipate dalle amministrazioni pubbliche e dalle loro controllate ex art. 2359 del codice civile comunichino all'Unita' d'Informazione Finanziaria (UIF) presso la Banca d'Italia i dati e le informazioni concernenti le operazioni sospette di cui vengono a conoscenza nell'esercizio della propria attività istituzionale, per consentire lo svolgimento di analisi finanziarie mirate a far emergere fenomeni di riciclaggio e di finanziamento del terrorismo.

Complessivamente le attività svolte nel settore dell'edilizia residenziale pubblica ed i relativi rapporti contrattuali instaurati dall'ERP LUCCA, specie nell'ambito delle procedure di appalto e delle commesse pubbliche, sono potenzialmente esposte al rischio di riciclaggio.

In sintesi, gli obblighi che ricadono sulle società a partecipazione pubblica in applicazione del quadro normativo sopra delineato sono i seguenti:

I. nominare con un provvedimento formalizzato un delegato (Gestore) a valutare e trasmettere le segnalazioni di operazioni da cui possono discendere violazioni di disposizioni contenute nella legislazione in materia di antiriciclaggio
II. registrare il "Gestore" sulla piattaforma UIF
III. individuare e segnalare alla UIF le operazioni da cui possono discendere violazioni di disposizioni contenute nella legislazione in materia di antiriciclaggio

Di fatto, ERP LUCCA potrebbe incorrere astrattamente nelle ipotesi di concorso nel reato di cui all'art. 648-ter c.p. nel momento in cui non assolvesse agli obblighi collaborativi sopra richiamati.

Per quanto attiene alle pubbliche amministrazioni e le società da esse partecipate, gli ambiti rispetto ai quali, ai sensi del suddetto art. 10, si applicano le disposizioni del decreto in narrativa riguardano:

- i procedimenti finalizzati all'adozione di provvedimenti di autorizzazione o concessione;
- le procedure di scelta del contraente per l'affidamento di lavori, forniture e servizi secondo le disposizioni di cui al codice dei contratti pubblici;
- i procedimenti di concessione ed erogazione di sovvenzioni, contributi, sussidi, ausili finanziari, nonché attribuzioni di vantaggi economici di qualunque genere a persone fisiche ed enti pubblici e privati.

Ulteriori rischi potenziali si possono rilevare in riferimento ad alcuni processi aziendali:

- gestione degli incassi in contanti e gestione della cassa, per quanto attiene al rispetto della normativa per il contrasto al riciclaggio ed all'uso del denaro contante, per la quali si ricordano le limitazioni all'uso del contante e dei titoli al portatore previste dal D.Lgs. 231/2007 all'art. 49 e s.m.i.;

Di seguito si riporta una breve descrizione dei reati richiamati dall'Art. 25-octies del D.Lgs.n.231/01 che si ritiene potrebbero trovare manifestazione nell'ambito delle attività svolte dall'azienda.

Reato	Esempio di condotta

• Ricettazione (Art. 648 c.p. modificato dal D.Lgs. n. 195 dell'8 novembre 2021)	Acquisto di un PC fuori dalla rete vendita tradizionale per conseguire un risparmio e tale bene risulta essere proveniente da un qualsiasi delitto come ad esempio da furto.
• Impiego di denaro, beni o utilità di provenienza illecita (Art. 648-ter c.p. modificato dal D.Lgs. n. 195 dell'8 novembre 2021)	Mancata segnalazione di operazioni sospette per conseguire un vantaggio nei rapporti con un appaltatore da cui ottiene un prezzo particolarmente favorevole pur avendo avuto contezza di segnali rilevanti (falsa dichiarazione nell'ambito delle verifiche dei requisiti previsti dal Codice degli Appalti).
• Auto riciclaggio (art. 648-ter-1 modificato dal D.Lgs. n. 195 dell'8 novembre 2021)	Falsa dichiarazione fiscale per conseguire risparmio di imposta e impiego di tale risparmio nell'attività aziendale.

Tra le attività sensibili relative a tale area emerse dall'analisi dei rischi si ricordano:

DIREZIONE/U.O. RESPONSABILI	PROCESSO 231	ATTIVITA' PER PROCESSO
Gare e appalti	Gestire gli approvvigionamenti	FS-5.1 Gestione Acquisti di Servizi
Gare e appalti	Conferimento incarichi professionali	Conferimento incarichi professionali FS-3.1 Gestione Albi e valutazione professionisti
Gare e appalti	Gestione delle gare di appalto.	Gestione delle gare di appalto.
S.I.A.	Gestione della bollettazione e della fatturazione attiva	FO-5.3 Gestire la bollettazione e la fatturazione
Ragioneria	Gestire l'Amministrazione e la Contabilità	FS-1. Gestire l'Amministrazione e la Contabilità
Ragioneria	Elaborare il bilancio di esercizio	Elaborare il bilancio di esercizio
Patrimoniale	Gestire il Patrimonio	FO-6.3 Gestione delle vendite di unita' immobiliari
Ragioneria	Gestione risorse finanziarie	Gestione risorse finanziarie

5.3. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE

5.3.1. Principi

La presente Sezione è inerente alle condotte poste in essere dai soggetti destinatari del Modello che operano, in particolare, nelle aree a Rischio e nello svolgimento delle attività sensibili precedentemente citate.

Il personale dell'ERP LUCCA, a qualsiasi titolo coinvolto nel processo in oggetto, è tenuto ad osservare le modalità esposte nei regolamenti e procedure aziendali, le previsioni di legge esistenti in materia, le previsioni contenute nel Codice Etico e nel Modello di Organizzazione, Gestione e Controllo ex D.Lgs.231/2001 adottati.

Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Sezione, in linea generale ed al fine di perseguire la prevenzione dei Reati Societari è fatto espresso divieto a tutti i

Soggetti destinatari del Modello 231 di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'art. 25-octies del D.Lgs.n.231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Sezione.

La Società condanna tramite l'applicazione del Codice Sanzionatorio i comportamenti difformi ai principi sopra menzionati.

In particolare, i destinatari hanno l'obbligo di segnalare all'Organismo di Vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Sezione sia stato commesso o possa essere commesso.

5.3.2. Norme generali di comportamento

Fermo restando quanto previsto nelle altre Sezioni e nei protocolli specifici previsti dal modello il presente paragrafo prevede l'espresso obbligo a carico degli Organi Sociali della Società e di tutti gli altri Destinatari del Modello di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate all'emissione delle fatture ed alla relativa registrazione, alla tenuta della contabilità, alla registrazione della relativa movimentazione ed alla predisposizione dei bilanci;
- assicurare che tutto il processo di gestione della contabilità aziendale sia condotto in maniera trasparente e documentabile.

Nello specifico i Destinatari sono tenuti a:

- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità (i.e. a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura);
- assicurare il rispetto, a cura della funzione competente, delle prescrizioni operative di raccolta documentale, definite dalla Società ai fini della corretta archiviazione, sia cartacea che elettronica, di tutta la documentazione relativa ai contratti/convenzioni stipulate (sia in forma attiva che passiva);
- assicurare lo scrupoloso adempimento, a cura delle funzioni aziendali competenti, delle prescrizioni normative e delle modalità operative definite dalla Società che disciplinano l'acquisizione e il controllo della documentazione rilevante ai fini del rilascio, a favore dei fornitori che ne avanzano richiesta nei termini di legge, dell'autorizzazione all'esecuzione dei lavori in subappalto;
- non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi di denaro di rilevante entità;
- effettuare un costante monitoraggio dei flussi finanziari aziendali.

- assicurare rigorosamente il rispetto della normativa in materia di tracciabilità dei flussi finanziari ai sensi della legge n. 136/2010 s.m.i. e quella sugli appalti pubblici;

Inoltre ai Destinatari è fatto divieto di:

- erogare prestazioni non necessarie, fatturare prestazioni non effettivamente erogate; duplicare la fatturazione per una medesima prestazione; omettere l'emissione di note di credito qualora siano state fatturate, anche per errore, prestazioni in tutto o in parte inesistenti o non finanziabili;
- omettere la registrazione documentale dei fondi della Società e della relativa movimentazione;
- richiedere o usare contributi, finanziamenti, mutui agevolati o altre erogazioni da parte dallo Stato, dalla PA in generale o da qualsiasi ente pubblico ovvero dall'UE o da altri organismi internazionali, mediante dichiarazioni mendaci, mediante documenti falsi ovvero mediante l'omissione di informazioni dovute;
- accordare qualsiasi incentivo commerciale che non sia in linea con i limiti di valore consentiti e non sia stato approvato e registrato in conformità a quanto stabilito dalle procedure interne;
- riconoscere qualsiasi commissione, sconto, credito e abbuono che non sia stato accordato in conformità con la normativa vigente e concesso ufficialmente ad entità societarie, dietro presentazione della documentazione di supporto.

Per garantire l'oggettività e la trasparenza delle operazioni contabili/amministrative ha, quindi, adottato un sistema che prevede:

- livelli autorizzativi definiti in base ai quali le decisioni in materia di investimenti, di acquisti e di vendite, possano essere assunte solo dagli organi e dai responsabili aziendali a ciò esplicitamente preposti, sulla base del sistema dei poteri e delle deleghe in essere, con firma congiunta per i poteri finanziari;
- segregazione nell'ambito del processo che prevede il coinvolgimento di una pluralità di attori, con responsabilità di gestione, verifica ovvero approvazione;
- tracciabilità del processo decisionale tramite documentazione e archiviazione (telematica e/o cartacea) di ogni attività del processo da parte della struttura coinvolta.

5.3.3. Presidi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Si ritiene necessario evidenziare come l'ERP LUCCA, per quanto riguarda il settore degli appalti, risponde alla normativa pubblicistica ex D.Lgs. 50/2016 e s.m.i., che contiene disposizioni cautelative come anche alle disposizioni in tema di tracciabilità dei flussi finanziari ex L. 136/2010, art. 3, s.m.i. le quali consentono un presidio importante anche dal punto di vista dell'assolvimento degli obblighi di collaborazione attiva descritti.

In particolare, il Codice degli appalti pubblici prevede una serie di verifiche svolte dalla Società, a carico delle imprese partecipanti alle procedure di gara, volte ad acquisire evidenza del possesso dei

requisiti (di ordine generale, di idoneità professionale, di capacità economico e finanziaria e tecnico-professionale).

La seconda (L. 136/2010 e s.m.i.) all'art. 3 stabilisce che "*per assicurare la tracciabilità dei flussi finanziari finalizzata a prevenire infiltrazioni criminali, gli appaltatori, i subappaltatori e i subcontraenti della filiera delle imprese nonché i concessionari di finanziamenti pubblici anche europei a qualsiasi titolo interessati ai lavori, ai servizi e alle forniture pubblici devono utilizzare uno o più conti correnti bancari o postali (..) dedicati".*

Nella gestione degli appalti di lavori pubblici, dunque, occorre sottolineare l'importanza delle attività di tracciabilità dei flussi finanziari, come disciplinate dalla normativa suddetta, le quali richiedono ulteriori presìdi di controllo da parte delle figure interne preposte.

In particolare, è previsto che nei contratti sottoscritti con gli appaltatori relativi ai lavori, ai servizi e alle forniture, il committente (ERP LUCCA):

- inserisca, a pena di nullità assoluta, un'apposita clausola con la quale essi assumono gli obblighi di tracciabilità dei flussi finanziari (art. 3 co. 8 primo capoverso della L. 136/2010);
- verifichi che nei contratti sottoscritti con i subappaltatori e i subcontraenti della filiera delle imprese a qualsiasi titolo interessate ai lavori, ai servizi e alle forniture sia inserita, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari (art. 3 co. 9 della L. 136/2010);
- inserisca nei contratti con i fornitori una specifica clausola con la quale gli stessi si dichiarano a conoscenza dei principi etici e comportamentali aziendali e dei principi contenuti nel Modello e si impegnino al rispetto degli stessi, con previsione di penali o, a seconda della gravità, della risoluzione del contratto in caso di mancato rispetto dei comportamenti etici o false dichiarazioni da parte del fornitore stesso.

Inoltre, in generale,

- come previsto dagli articoli 11 e 12 delle istruzioni Uif la società individua con un provvedimento formalizzato un delegato (Gestore) a valutare e trasmettere le comunicazioni all'Uif.
- Il "Gestore" provvede alla segnalazione di operazioni sospette previa loro individuazione sulla base dei parametri (segnali di anomalia) forniti dalla UIF, applicando apposita check list su operazioni di acquisto estratte con tecniche di campionamento casuale.
- In conformità all'articolo 10 delle istruzioni Uif, la società, nel quadro dei programmi di formazione continua del personale, adotta misure idonee ad assicurare il riconoscimento, da parte dei propri dipendenti, delle fattispecie meritevoli di comunicazione alla stessa UIF secondo quanto previsto nel punto precedente.
- Applicazione del Codice dei Contratti pubblici e di criteri trasparenti di scelta dei professionisti le cui prestazioni non ricadono nel predetto Codice basati sulle competenze/esperienze.

5.4. I CONTROLLI DELL'ORGANISMO DI VIGILANZA

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui all'Art. 25-octies del Decreto, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'Art. 25-octies del Decreto sono i seguenti:

- Svolgere verifiche periodiche sul rispetto della presente Sezione e dei presidi sopra individuati e valutare regolarmente la sua efficacia a prevenire la commissione dei reati di cui all'Art. 25-septies del Decreto; con riferimento a tale punto, l'OdV condurrà controlli a campione sulle attività potenzialmente a rischio, diretti a verificare la corretta applicazione dei presidi specifici sopra individuati.
- Verificare l'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni.
- Proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Sezione.
- Proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Sezione
- L'Organismo di Vigilanza attiva una serie di scambio di informazioni con il "Gestore" (destinatario degli obblighi di invio delle segnalazioni ad accadimento) e con il RPCT, al fine di attuare efficacemente le proprie attività di vigilanza.
- Esaminare i flussi informativi periodici ed eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute
- Conservare traccia dei flussi informativi periodici ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti

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

5.4.1. Flussi informativi verso l'organismo di vigilanza

Sussiste a carico di tutti i Destinatari del MOG (soggetti apicali, sottoposti, consulenti, etc.) l'**obbligo di segnalazione immediata all'OdV** in caso di notizie rilevanti sulla vita dell'Ente, violazioni del

Modello, della presente Parte Speciale o situazioni di riscontrata inadeguatezza e/o non conformità di comportamenti ai principi contenuti nelle procedure/istruzioni aziendali e nel Codice Etico.
Le segnalazioni di illeciti, secondo le istruzioni impartite dall'OdV, dovranno avvenire con le modalità indicate nell'apposita **Procedura "*Flussi Informativi*",** nel rispetto della normativa in tema di *Whistleblowing*.
Con riferimento ai controlli periodici sui processi aziendali e allo svolgimento delle normali attività il D.Lgs. n. 231/01 prevede **flussi informativi con cadenze determinate** verso l'OdV da parte di specifici soggetti. Si rinvia alla **Procedura "*Flussi Informativi*",** allegata al Modello, per la descrizione delle specifiche modalità operative con cui dovranno essere inviati i suddetti flussi.

SEZIONE 6:

REATI AMBIENTALI

(ART. 25-UNDECIES)

6. ART. 25-UNDECIES – REATI AMBIENTALI

6.1. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS.N.231/01

La presente Sezione 6 disciplina i rischi connessi alla commissione, nell'interesse o a vantaggio di ERP Lucca S.r.l., dei reati ambientali previsti dall'**art. 25-undecies del D.Lgs. 8 giugno 2001, n. 231,** come modificato dal **D.L. 14 luglio 2025, n. 116,** convertito con modificazioni dalla **L. 11 settembre 2025, n. 147** (c.d. "Decreto Terra dei Fuochi"), e dal **D.Lgs. 81/2026** di attuazione della Direttiva (UE) 2024/1203 sulla tutela penale dell'ambiente.
Le modifiche normative del biennio 2025-2026 hanno:

- introdotto nuove fattispecie di reato nel codice penale (Titolo VI-bis c.p.) e nel D.Lgs. 152/2006;
- novellato le fattispecie esistenti, con particolare riguardo alla nozione di "abusivamente" e all'introduzione di nuove aggravanti;
- aggravato il quadro sanzionatorio 231, con incremento delle quote e previsione di sanzioni interdittive anche permanenti nei casi più gravi;
- abrogato l'art. 733-bis c.p., le cui condotte rilevanti sono state assorbite nelle nuove fattispecie codicistiche.

Il catalogo dei reati presupposto aggiornato è il seguente:

TABELLA 1 – Catalogo reati presupposto ex art. 25-undecies D.Lgs. 231/2001

Norma	Denominazione/Condotta tipica	Sanzione pecuniaria 231 (quote)	Sanzioni interdittive	Attività ERP Lucca esposte
Art. 452-bis c.p. (come novellato)	Inquinamento ambientale	Da 250 a 600	Sì – casi qualificati	Cantieri, rifiuti, scarichi, bonifiche
Art. 452-bis.1 c.p. (nuovo)	Commercio di prodotti inquinanti	Da 250 a 600	Sì – casi qualificati	Acquisto/impiego materiali, forniture
Art. 452-ter c.p. (nuovo)	Morte o lesioni quale conseguenza di inquinamento ambientale o commercio prodotti inquinanti	Da 400 a 800	Sì	Cantieri, siti contaminati

Norma	Denominazione/Condotta tipica	Sanzione pecuniaria 231 (quote)	Sanzioni interdittive	Attività ERP Lucca esposte
Art. 452-quater c.p. (come novellato)	Disastro ambientale	Da 400 a 800	Sì	Cantieri maggiori, gestione rifiuti pericolosi
Art. 452-quinquies c.p.	Delitti ambientali colposi	Da 200 a 500	Sì – solo forme aggravate	Tutte le attività tecniche e di cantiere
Art. 452-sexies c.p.	Traffico e abbandono di materiale ad alta radioattività	Da 300 a 700	Sì	Astratta
Art. 452-septies c.p.	Impedimento del controllo	Da 150 a 400	No	Gestione documentale, ispezioni
Art. 452-octies c.p.	Aggravanti per associazione a delinquere	Aumento fino a 2/3	Sì	Filiera appaltatori
Art. 452-quinquiesdecies c.p. (nuovo)	Definizione di "abusivamente" – norma interpretativa	(incide su tutte le fattispecie)	—	Tutte le attività con titoli autorizzativi
Art. 452-sexiesdecies c.p. (nuovo)	Aggravante per profitto rilevante o uso di documenti falsi	Aumento di 1/3 delle sanzioni pecuniarie	Sì – nei casi più gravi	Gestione documentale, appalti
Art. 452-quaterdecies c.p.	Attività organizzate per il traffico illecito di rifiuti	Da 300 a 800	Sì	Gestione rifiuti, filiera appaltatori
Art. 137 D.Lgs. 152/2006	Scarichi non autorizzati di acque reflue	Da 150 a 250	No	Cantieri, impianti
Art. 256 D.Lgs. 152/2006 (come novellato)	Attività di gestione rifiuti non autorizzata	Da 150 a 250	Sì – forme aggravate	Cantieri, depositi temporanei
Art. 255-bis D.Lgs. 152/2006 (nuovo)	[Condotta specifica introdotta dalla riforma – verificare testo definitivo]	Da 150 a 250	No	Cantieri, gestione rifiuti
Art. 255-ter D.Lgs. 152/2006 (nuovo)	[Condotta specifica introdotta dalla riforma – verificare testo definitivo]	Da 150 a 250	No	Cantieri, gestione rifiuti

Norma	Denominazione/Condotta tipica	Sanzione pecuniaria 231 (quote)	Sanzioni interdittive	Attività ERP Lucca esposte
Art. 256-bis D.Lgs. 152/2006	Combustione illecita di rifiuti	Da 150 a 300	No	Cantieri, aree di deposito
Art. 257 D.Lgs. 152/2006	Omessa bonifica di siti contaminati	Da 150 a 250	No	Direzione Lavori, patrimonio
Art. 258 D.Lgs. 152/2006 (come novellato)	Violazione degli obblighi di comunicazione, tenuta dei registri obbligatori e formulari	Da 150 a 250	No	Ufficio tecnico, DL, uff. contratti
Art. 259 D.Lgs. 152/2006 (come novellato)	Traffico illecito di rifiuti (forme base)	Da 150 a 250	No	Gestione rifiuti, appalti
Art. 260-bis D.Lgs. 152/2006 (come novellato)	Violazioni del sistema di tracciabilità rifiuti (RENTRI)	Da 150 a 250	No	Gestione documentale, ufficio tecnico
Art. 279 D.Lgs. 152/2006	Violazione delle prescrizioni in materia di emissioni in atmosfera	Da 150 a 250	No	Impianti, cantieri

6.1.1. Aggravanti e incrementi sanzionatori 231

Per i delitti aggravati ai sensi degli artt. **452-bis commi 2-4 c.p., 452-bis.1 commi 2-4 c.p., 452-quater terzo comma c.p.**e per le condotte che integrano l'aggravante di cui all'**art. 452-sexiesdecies primo comma n. 1 c.p.** (profitto rilevante o uso di documenti falsi), le sanzioni pecuniarie applicabili all'ente sono **aumentate di un terzo** rispetto ai valori base.
Nei casi più gravi, e segnatamente qualora l'ente o una sua unità organizzativa siano stabilmente utilizzati allo scopo di consentire o agevolare la commissione dei reati di cui agli artt. 452-bis, 452-quater, 452-quinquies (nelle forme aggravate) e 452-quaterdecies c.p., può essere disposta l'**interdizione definitiva dall'esercizio dell'attività**.

6.2. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA

ERP Lucca S.r.l. è una società in house del Comune di Lucca che opera principalmente nei settori dell'**edilizia residenziale pubblica**, della **gestione, manutenzione e recupero del patrimonio immobiliare pubblico** e della **realizzazione di nuovi alloggi di edilizia sociale**. La sua attività si svolge prevalentemente tramite **appalti a imprese terze**, attraverso le funzioni di committenza, direzione lavori e controllo.
In ragione di tale operatività, i seguenti reati presupposto sono valutati come **concretamente configurabili** nel contesto aziendale:

Livello di rischio ALTO:

- Omessa bonifica o comunicazione ritardata in presenza di contaminazione (art. 257 D.Lgs. 152/2006): rilevabile in occasione di demolizioni, scavi, manutenzioni straordinarie.
- Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.): rischio da filiera appalto, con più soggetti coinvolti nella gestione illecita sistematica.

Livello di rischio MEDIO-ALTO:

- Inquinamento ambientale (art. 452-bis c.p.): mediante scarichi, dispersioni, gestione non conforme di rifiuti pericolosi nei cantieri affidati ad appaltatori.
- Combustione illecita di rifiuti (art. 256-bis D.Lgs. 152/2006): rischio derivante da pratiche illecite di smaltimento adottate da appaltatori/subappaltatori nei cantieri di ERP Lucca.

Livello di rischio MEDIO:

- Violazioni in materia di emissioni in atmosfera (art. 279 D.Lgs. 152/2006): rilevante in cantieri con attività di demolizione, taglio, verniciatura, o uso di mezzi non conformi nei cantieri affidati ad appaltatori.
- Scarichi non autorizzati (art. 137 D.Lgs. 152/2006): in cantieri con scarichi su suolo o acque.
- Impedimento del controllo (art. 452-septies c.p.): mediante ostacolo all'accesso ispettivo o alla trasmissione di dati ambientali.

Livello di rischio BASSO / RESIDUALE (astrattamente rilevante):

- Delitti ambientali colposi (art. 452-quinquies c.p.): configurabile qualora le condotte sopra descritte siano realizzate per negligenza, imperizia o inosservanza di regole procedurali interne.
- Traffico illecito di rifiuti transfrontaliero (art. 259 D.Lgs. 152/2006): rischio residuale.

Anche le fattispecie classificate a rischio basso o residuale non sono escluse dall'ambito di applicazione della presente Parte Speciale. Ciò in quanto la **colpa di organizzazione** — che costituisce il fondamento della responsabilità dell'ente ai sensi del D.Lgs. 231/2001 — può derivare non solo dall'esecuzione materiale della condotta illecita da parte di soggetti apicali o sottoposti, ma anche da omissioni nei controlli, nelle qualifiche di terzi, nelle verifiche documentali e nell'attivazione dei flussi informativi. Pertanto, i presìdi della presente Parte Speciale si applicano a tutte le fattispecie catalogate.

Nel contesto della Società è chiaro che, difficilmente, possa manifestarsi una diretta responsabilità nel cagionare l'inquinamento (il responsabile dell'inquinamento, piuttosto, potrebbe essere individuato nell'impresa appaltatrice), mentre sembra meno remota l'ipotesi di responsabilità derivante da una mancata comunicazione da parte del Direttore Lavori, in caso di eventi che possano contaminare il sito o eventi che evidenziano un inquinamento pregresso dello stesso.

Ciò anche se, da una prima analisi, sembra esclusa (ai fini 231) la responsabilità di omessa comunicazione da parte del proprietario o gestore dell'area che invece è prevista dall'art. 245 comma II D.Lgs. 152/2006.

In ogni caso in queste fattispecie si ritiene di non poter escludere *tout-court* un coinvolgimento della Società in un procedimento penale a carico della persona fisica, con un rischio generico derivante da una colpa in organizzazione.
Le decisioni più recenti, tuttavia, segnalano che, per affermare la responsabilità 231, non basta invocare astrattamente un "risparmio di spesa": occorre spiegare **perché l'attività illecita del terzo sia riferibile anche all'ente** e quale utilità ne abbia tratto. Sul piano del Modello, questo impone di considerare come condotte a rischio:

- la **scelta consapevole o colposamente superficiale** di operatori meno costosi ma non affidabili;
- la **mancata predisposizione di controlli preventivi e successivi** idonei a impedire il vantaggio economico derivante dall'illecito;
- la **tolleranza organizzativa** verso prassi irregolari di cantiere che consentano tempi più rapidi o costi minori.

6.3. Attività sensibili, funzioni coinvolte e condotte a rischio reato

TABELLA – Mappa delle attività sensibili

Area sensibile	Processo/attività specifica	Funzioni aziendali coinvolte	Fattispecie rilevanti	Condotte in concreto
A – Gestione adempimenti ambientali e bonifiche	Rilevazione eventi contaminanti in corso d'opera; comunicazioni ex art. 242 e 257 D.Lgs. 152/2006; ripristino	DL, RUP, Responsabile Tecnico, Ufficio Legale/Compliance	Art. 257 D.Lgs. 152/2006; artt. 452-bis, 452-quater c.p.	• non rilevare o non far emergere l'evento contaminante; • ritardare o omettere la comunicazione ex art. 242; • non attivare misure di prevenzione o messa in sicurezza; • proseguire i lavori nonostante il rischio; • non eseguire o eseguire in modo difforme la bonifica

Area sensibile	Processo/attività specifica	Funzioni aziendali coinvolte	Fattispecie rilevanti	Condotte in concreto
B – Gestione rapporti autorizzativi e documentale	Verifica validità autorizzazioni ambientali di appaltatori/trasportatori/impianti; conservazione documenti; verifica genuinità certificati di analisi; gestione audit trail	DL, Ufficio Contratti, Ufficio Tecnico, Ufficio Amministrativo	Art. 452-quinquiesdecies c.p. (nozione di abusività); art. 452-sexiesdecies c.p. (documenti falsi); artt. 258, D.Lgs. 152/2006	• usare operatori con autorizzazioni scadute, incoerenti o assenti; • acquisire o utilizzare certificati di analisi falsi o dubbi; • liquidare prestazioni senza verifica documentale
C – Gestione appalti e filiera	Selezione, qualificazione e monitoraggio di appaltatori/subappaltatori; clausole ambientali contrattuali; verifiche in corso di esecuzione; liquidazione prestazioni	Ufficio Contratti, DL, RUP, Direzione	Tutte le fattispecie di cui alla presente Sezione, per effetto del rischio da "colpa di organizzazione" nella selezione e supervisione dei terzi	• qualificare in modo inadeguato appaltatori e subappaltatori; • non inserire clausole ambientali efficaci; • non monitorare l'esecuzione in cantiere; • non reagire a non conformità note; • pagare comunque il fornitore malgrado anomalie ambientali o documentali

Condotte a rischio reato

Condotte che possono integrare l'art. 257 D.Lgs. 152/2006

L'art. 242 impone, al verificarsi di un evento potenzialmente contaminante, l'adozione entro ventiquattro ore delle misure di prevenzione e l'immediata comunicazione ai sensi dell'art. 304, comma 2; se l'indagine preliminare accerta il superamento delle CSC anche per un solo parametro, occorre darne immediata notizia agli enti competenti e avviare la successiva procedura.
L'art. 257 sanziona chi cagiona l'inquinamento e **non provvede alla bonifica** in conformità al progetto approvato, nonché la **mancata comunicazione** di cui all'art. 242.
In concreto, per ERP Lucca, le condotte a rischio possono essere:

- **omessa segnalazione interna ed esterna** del rinvenimento, durante scavi, demolizioni o manutenzioni, di terreni, acque, materiali o sostanze che facciano presumere una contaminazione del sito;
- **ritardo nella comunicazione** agli enti competenti, pur in presenza di indizi tecnici di potenziale contaminazione o di superamento delle soglie rilevanti;
- **mancata attivazione delle misure di prevenzione o messa in sicurezza d'emergenza** subito dopo l'evento contaminante o il suo rilevamento;
- **prosecuzione delle lavorazioni** nonostante l'emersione di un possibile inquinamento, senza sospensione dell'attività nell'area interessata e senza attivazione della procedura tecnica di verifica;
- **omessa o incompleta indagine preliminare** sui parametri interessati dall'evento contaminante;
- **omessa presentazione del piano di caratterizzazione** o mancata collaborazione all'avvio della procedura amministrativa successiva al superamento delle CSC;
- **mancata esecuzione, esecuzione tardiva o difforme** degli interventi di bonifica o ripristino ambientale rispetto al progetto approvato;
- **sottovalutazione o occultamento documentale** di risultati analitici, rilievi tecnici o evidenze di cantiere idonei a far emergere l'obbligo di comunicazione.

Sul piano interpretativo, la giurisprudenza richiamata nelle fonti segnala che il reato di omessa bonifica ha natura permanente e che anche l'omessa comunicazione, quando permane la minaccia di danno e l'omissione, non si esaurisce in un fatto istantaneo. Inoltre, le Sezioni Unite civili hanno chiarito che il proprietario non responsabile della contaminazione non è gravato dall'obbligo generale di bonifica, ma resta tenuto agli obblighi di comunicazione e alle misure di prevenzione nei limiti previsti dal sistema speciale del Codice dell'ambiente.

Condotte che possono integrare l'inquinamento ambientale ex art. 452-bis c.p.

La Cassazione ha chiarito che il delitto di inquinamento ambientale richiede una **compromissione o un deterioramento significativi e misurabili** della matrice ambientale o dell'ecosistema e che non è necessaria la prova della contaminazione del sito nel senso tecnico di cui all'art. 240 TUA.

- **sversamenti o dispersioni** di sostanze inquinanti nel suolo, sottosuolo o acque durante l'esecuzione di lavori;

- **movimentazione non controllata di materiali contaminati** che determini diffusione dell'inquinamento;
- **gestione impropria di rifiuti o reflui di cantiere** con conseguente deterioramento della matrice ambientale;
- **mancata adozione di misure di contenimento** dopo un evento noto, con aggravamento del danno;
- **prosecuzione di attività "abusive"** in violazione di prescrizioni amministrative o di legge, nozione che la giurisprudenza intende in senso ampio, non limitato all'assenza assoluta di autorizzazione.

Condotte che possono sfociare nel disastro ambientale ex art. 452-quater c.p.

Le fonti disponibili non riportano il testo dell'art. 452-quater, ma l'art. 25-undecies contempla i delitti più gravi del Titolo VI-bis con aggravamenti sanzionatori. In ottica di processo a rischio, il salto dal 452-bis al 452-quater può derivare da condotte omissive o commissive che producano una compromissione di eccezionale gravità.

In concreto, le condotte da presidiare sono soprattutto:

- **inerzia protratta** a fronte di contaminazioni rilevate o ragionevolmente percepibili;
- **mancato contenimento** di una diffusione significativa di contaminanti;
- **pluralità di omissioni tecniche e gestionali** che consentano il peggioramento progressivo e massivo della situazione ambientale.

Condotte che esprimono "abusività" ex artt. 258 e 260-bis D.Lgs. 152/2006

La giurisprudenza indica che la condotta "abusiva" non è solo quella svolta in totale assenza di autorizzazione, ma anche quella posta in essere con autorizzazioni scadute, illegittime, non pertinenti o in violazione di leggi e prescrizioni amministrative. Il Modello tipo ambientale richiama, coerentemente, come condotta di rischio l'**esercizio di attività in assenza di autorizzazione valida o in violazione delle prescrizioni contenute nei titoli abilitativi**.

In concreto, il processo può generare rischio se vi sono:

- **mancata verifica della validità temporale** delle autorizzazioni di trasportatori, impianti o appaltatori;
- **mancata verifica della coerenza oggettiva** tra autorizzazione posseduta e attività concretamente svolta (es. tipologia di rifiuti, categoria, classe, impianto di destinazione);
- **accettazione di titoli abilitativi incompleti, non aggiornati o non genuini**;
- **utilizzo di impianti o trasportatori non autorizzati o autorizzati per attività diverse**;
- **mancato blocco operativo o amministrativo** pur dopo la rilevazione di irregolarità autorizzative.

Profili aggravati: profitto/risparmio di spesa e documenti falsi

Il documento modello ambientale segnala come specifico rischio l'uso di documenti falsi e il collegamento con aggravanti legate al profitto. Sul piano giurisprudenziale, è stato chiarito che il **profitto** può consistere anche nel **risparmio di spesa**, ad esempio nell'evitato costo di corretto smaltimento. Di conseguenza, sono particolarmente sensibili le condotte consistenti in:

- **accettare documentazione falsa per abbattere i costi di gestione rifiuti**;
- **chiudere volontariamente gli occhi su incongruenze documentali** in presenza di offerte economicamente anomale;
- **omettere verifiche su autorizzazioni e analisi** pur a fronte di evidenti indicatori di rischio, ottenendo così un vantaggio economico per l'ente o per il contraente.

Tutte le fattispecie di reato della sezione, per possibile colpa di organizzazione e per responsabilità da fatto del soggetto inserito nella filiera aziendale.

La Cassazione ha ribadito che, per la responsabilità dell'ente, non basta la commissione del reato-presupposto da parte della persona fisica: occorre anche la dimostrazione della **colpa di organizzazione**, cioè del deficit di cautele organizzative e gestionali idonee a prevenire il reato. La stessa giurisprudenza ha chiarito che la motivazione sulla responsabilità 231 è insufficiente se non spiega in concreto **interesse o vantaggio** dell'ente e non collega la condotta del soggetto agente alla sfera dell'ente.
Nel processo di Selezione, qualificazione e monitoraggio di appaltatori/subappaltatori; clausole ambientali contrattuali; verifiche in corso di esecuzione; liquidazione prestazioni, quindi, le condotte a rischio, riportate di seguito, non coincidono solo con il fatto illecito "materiale", ma con tutte le scelte od omissioni organizzative che lo rendono possibile o più probabile.

- Condotte concrete in fase di selezione e qualificazione
- Condotte concrete nella strutturazione del contratto
- Condotte concrete nel monitoraggio in corso di esecuzione
- Condotte concrete nella fase di contabilizzazione e liquidazione

6.4. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE

6.4.1. Principi

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, la politica e le procedure aziendali nonché le regole contenute nel Modello e nella presente Sezione operando, in questo modo, in coerenza con i valori e i principi che sono alla base dell'attività d'impresa in azienda
In generale, il sistema di organizzazione, gestione e controllo della società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti

Nello svolgimento delle attività sopra descritte e, in generale, delle proprie funzioni, gli amministratori, gli organi sociali, i dipendenti, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, devono conoscere e rispettare:

- **La normativa italiana e straniera applicabile alle attività svolte**
- **Le direttive UE in materia di reati ambientali**
- **Il Codice Etico Aziendale**
- **Le disposizioni contenute nel presente Modello**
- **Le procedure e le linee guida aziendali nonché tutta la documentazione attinente al sistema di organizzazione, gestione e controllo della Società**

La presente Sezione è inerente alle condotte poste in essere dai soggetti destinatari del Modello che operano, in particolare, nelle aree a rischio reato e nello svolgimento delle attività sensibili.

6.4.2. Norme generali di comportamento

Nell'ambito delle attività sensibili individuate al paragrafo 6.3, tutti i Destinatari del Modello – Organi Societari, dirigenti, dipendenti, collaboratori e, per quanto applicabile, appaltatori e fornitori – sono tenuti al rispetto dei seguenti principi e delle seguenti norme di comportamento. Le presenti norme si aggiungono a quelle di carattere generale contenute nella Parte Generale del Modello e nel Codice Etico di ERP Lucca S.r.l.
Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Sezione, in linea generale e al fine di perseguire la prevenzione dei reati ambientali è fatto espresso divieto a tutti i soggetti destinatari del Modello di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'Art. 25-undecies del D.Lgs.n.231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Sezione

È da considerarsi vietato qualsiasi comportamento che possa integrare una condotta rilevante di una qualsivoglia fattispecie di reato contemplata dall'Art.25-undecies del D.Lgs.n.231/01

6.4.3. Divieti espressi

È **assolutamente vietato**, anche qualora la condotta potesse risultare vantaggiosa per ERP Lucca S.r.l.:
Relativamente alla gestione dei rifiuti:

- gestire, far gestire o tollerare la gestione di rifiuti in assenza dei prescritti titoli abilitativi (autorizzazioni, iscrizioni all'Albo Nazionale Gestori Ambientali, comunicazioni);
- consentire, disporre o tollerare l'abbandono, il deposito incontrollato o la combustione illecita di rifiuti di qualsiasi tipologia, sia da parte di personale interno sia da parte di appaltatori/subappaltatori operanti nei cantieri di ERP Lucca S.r.l.;

- classificare deliberatamente i rifiuti in modo non corrispondente alla loro effettiva natura al fine di ridurre i costi di smaltimento o eludere controlli;
- affidare trasporto o smaltimento di rifiuti a soggetti privi della necessaria abilitazione o i cui titoli siano scaduti, sospesi o revocati.

Relativamente alla documentazione e alla tracciabilità:

- utilizzare, predisporre, accettare o fare affidamento su **formulari di identificazione rifiuti, registri di carico e scarico, certificati di analisi, rapporti di prova, attestazioni di idoneità o qualsiasi altra documentazione ambientale** che sia non veritiera, incompleta, alterata o contraffatta;
- omettere, ritardare o rendere in modo incompleto le segnalazioni obbligatorie verso le autorità competenti in materia ambientale;
- ostacolare, ritardare o impedire ispezioni, verifiche o accessi di autorità di controllo ambientale o dell'OdV;
- omettere la trasmissione all'OdV delle informazioni e segnalazioni previste dalla presente Parte Speciale.

Relativamente alle autorizzazioni:

- avviare o proseguire attività soggette ad autorizzazione ambientale in assenza di un valido titolo abilitativo, ovvero oltre i limiti o le prescrizioni dello stesso;
- ottenere o fare ottenere autorizzazioni ambientali mediante dichiarazioni false, documentazione non veritiera o rappresentazioni inesatte della situazione di fatto;
- proseguire attività in regime di autorizzazione scaduta, sospesa o revocata, senza aver tempestivamente presentato domanda di rinnovo.

Relativamente ai prodotti e materiali:

- acquistare, impiegare o fare utilizzare, nell'ambito dei lavori affidati, **prodotti, materiali o sostanze** di cui sia nota o ragionevolmente prevedibile l'idoneità a cagionare un deterioramento significativo della qualità del suolo, delle acque, dell'aria o di ecosistemi, in assenza di previa verifica tecnica e documentale di conformità;
- fare ricorso a fornitori, produttori o intermediari di materiali che non abbiano fornito adeguata documentazione tecnica circa le caratteristiche ambientali dei prodotti.

Relativamente a bonifiche e contaminazioni:

- omettere la segnalazione interna immediata di eventi che possano aver determinato o determinare una contaminazione del suolo, del sottosuolo o delle acque in occasione di lavori, demolizioni, scavi o manutenzioni;
- ritardare la comunicazione all'autorità competente al di là dei termini prescritti dall'art. 242 D.Lgs. 152/2006;
- proseguire le lavorazioni in un sito dove sia stato rilevato o fondatamente sospettato un inquinamento pregresso, senza aver attivato la procedura interna di incident reporting ambientale.

6.4.4. Obblighi positivi

È **obbligatorio**:

Per tutte le funzioni operative:

- verificare, prima dell'affidamento di lavori, la validità e la pertinenza delle autorizzazioni ambientali di appaltatori, subappaltatori, trasportatori di rifiuti e impianti destinatari;
- garantire la **tracciabilità documentale completa** di ogni flusso di rifiuti prodotti nei cantieri di ERP Lucca S.r.l., dal deposito temporaneo fino alla destinazione finale;
- conservare tutta la documentazione ambientale (formulari, registri, certificati, schede tecniche, autorizzazioni di terzi) secondo le modalità e i tempi indicati nella procedura di gestione documentale ambientale;
- segnalare immediatamente al proprio superiore gerarchico, alla funzione Legale/Compliance e all'OdV qualsiasi evento di contaminazione ambientale, sversamento, abbandono di rifiuti o irregolarità documentale rilevata.

Per il Direttore Lavori:

- effettuare verifiche periodiche sui rifiuti prodotti in cantiere, sul loro deposito temporaneo, sulla correttezza dei formulari e sulla qualificazione degli operatori;
- segnalare tempestivamente alla funzione Legale/Compliance e all'OdV qualsiasi contestazione o prescrizione ambientale ricevuta o notificata in relazione al cantiere diretto;
- attivare immediatamente la procedura di incident reporting ambientale al primo rinvenimento di situazioni di possibile contaminazione pregressa o in atto.

Per l'Ufficio Contratti/Acquisti:

- verificare, in fase di qualificazione, la documentazione ambientale degli operatori da inserire nell'albo fornitori;
- aggiornare periodicamente la documentazione ambientale acquisita dagli appaltatori attivi;
- sospendere la liquidazione delle prestazioni in presenza di documentazione ambientale mancante, incoerente o dubbia, dandone immediata comunicazione al DL e all'OdV.

Per il Responsabile Unico del Procedimento (RUP):

- verificare che i capitolati speciali di appalto contengano le clausole ambientali previste al paragrafo 6.6 della presente Parte Speciale;
- monitorare il rispetto delle prescrizioni ambientali durante l'esecuzione contrattuale;
- trasmettere all'OdV, con cadenza semestrale, un report sullo stato degli adempimenti ambientali nei contratti attivi.

6.4.5. Presidi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Nel caso di rifiuti prodotti presso la sede occorre sottolineare, in genere, le modeste quantità e la non pericolosità dei rifiuti prodotti dalle attività che sono di tipo puramente amministrativo (nella sede sociale). Eventuali interventi manutentivi su coperture in amianto o altri interventi che possano generare rifiuti pericolosi, sono affidate a imprese esterne qualificate ed in possesso delle necessarie autorizzazioni, verificate dal RUP all'atto dell'affidamento e successivamente al momento della

liquidazione della fattura prevedendo la verifica dell'avvenuto corretto smaltimento tramite la consegna della copia del formulario.

Nel secondo caso (rifiuti prodotti nei cantieri mobili), per quanto tali reati siano direttamente commessi da personale dell'impresa aggiudicataria dell'appalto, può emergere una colpa in organizzazione a carico dell'Ente, in particolare in relazione alle attività di inquinamento dei suoli e di smaltimento dei rifiuti prodotti in cantiere.
A questo scopo l'ERP LUCCA inserisce, all'interno del Capitolato d'appalto, specifiche prescrizioni a carico delle ditte appaltatrici in materia di smaltimento dei rifiuti, comprese le precise responsabilità nella predisposizione dei formulari dei rifiuti.

In relazione ai reati di cui all'art. 257 D.Lgs. 152/2006 (*Siti contaminati)* il Direttore Lavori è destinatario di specifici obblighi di comunicazione tempestiva all'autorità competente di eventi che possano contaminare il sito o che evidenzino un inquinamento pregresso.

6.4.5.1. Presìdi contrattuali sugli appaltatori

I contratti di appalto, subappalto, fornitura e servizi con contenuto ambientale significativo devono contenere, a pena di inammissibilità dell'offerta in fase di selezione, le seguenti clausole:

- dichiarazione di possesso e mantenimento di tutte le autorizzazioni, iscrizioni e certificazioni ambientali necessarie per l'esecuzione del contratto, con obbligo di comunicazione immediata di qualsiasi variazione, sospensione o revoca;
- obbligo di rispetto di tutte le norme ambientali applicabili e delle disposizioni della presente Parte Speciale, nella misura in cui applicabili alle attività appaltate;
- obbligo di utilizzo, per il trasporto dei rifiuti prodotti in cantiere, esclusivamente di soggetti iscritti all'Albo Nazionale Gestori Ambientali per la categoria e la classe adeguate;
- obbligo di tracciabilità completa dei rifiuti tramite formulari (FIR) regolarmente compilati e sistema RENTRI, con trasmissione delle copie a ERP Lucca S.r.l. entro i termini di legge;
- obbligo di segnalazione immediata a ERP Lucca S.r.l. di qualsiasi evento che possa avere determinato o determinare una contaminazione del sito;
- obbligo di utilizzo di prodotti, materiali e sostanze conformi alla normativa ambientale vigente e di trasmissione delle relative schede tecniche e dichiarazioni di conformità;
- facoltà di ERP Lucca S.r.l. e dell'OdV di effettuare, in qualsiasi momento, audit e ispezioni documentali sull'esecuzione degli adempimenti ambientali;
- clausola risolutiva espressa in caso di violazioni della normativa ambientale di rilievo penale o di gravi irregolarità documentali;
- penale contrattuale per ogni violazione accertata delle prescrizioni ambientali;
- obbligo di sospensione immediata dei lavori in caso di rinvenimento di situazioni di possibile contaminazione, fino al nulla osta di ERP Lucca S.r.l.

6.4.5.2. Presìdi su bonifiche e contaminazioni – Procedura di incident reporting ambientale

È adottata la seguente procedura ("Incident reporting ambientale") che prevede:
Fase 1 – **Rilevazione e segnalazione immediata** (entro 2 ore dall'evento):
Il DL o il soggetto che rileva l'evento informa immediatamente il RUP, la funzione Legale/Compliance e l'OdV tramite il canale di segnalazione dedicato.
Fase 2 – **Valutazione tecnica** (entro 24 ore):
Attivazione del Responsabile Tecnico per la valutazione preliminare dell'entità dell'evento e delle misure di contenimento immediate. Verbalizzazione tecnica dell'accaduto con documentazione fotografica.
Fase 3 – **Decisione sull'obbligo di comunicazione all'autorità** (entro 24 ore):
La funzione Legale/Compliance, sentito il Responsabile Tecnico, valuta la sussistenza dell'obbligo di comunicazione ai sensi dell'art. 242 D.Lgs. 152/2006 e ne informa la Direzione e l'OdV.
Fase 4 – **Comunicazione all'autorità competente** (nei termini di legge):
Trasmissione della comunicazione prescritta, con copia all'OdV.
Fase 5 – **Follow-up e chiusura** (continuativa):
Monitoraggio dell'evoluzione, aggiornamento dell'OdV, conservazione della documentazione.
Matrice delle responsabilità:

Fase	DL/Personale cantiere	RUP	Resp. Tecnico	Legale/Compliance	OdV	Direzione
1 – Segnalazione immediata	✓	✓ (riceve)	—	✓ (riceve)	✓ (riceve)	—
2 – Valutazione tecnica	✓ (supporto)	✓	✓ (responsabile)	✓	✓ (informa)	—
3 – Decisione su comunicazione	—	—	✓ (consulta)	✓ (decide)	✓ (informa)	✓ (approva)
4 – Comunicazione autorità	—	—	✓ (supporto)	✓ (redige/trasmette)	✓ (riceve copia)	✓
5 – Follow-up	✓	✓	✓	✓	✓ (monitora)	✓

6.5. I CONTROLLI E I FLUSSI INFORMATIVI DELL'ORGANISMO DI VIGILANZA

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui all'Art. 25-undecies del Decreto, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'Art. 25-undecies del Decreto sono i seguenti:

- Svolgere verifiche periodiche sul rispetto della presente Sezione e dei presidi sopra individuati e valutare regolarmente la sua efficacia a prevenire la commissione dei delitti di cui all'Art. 25-undecies del Decreto; con riferimento a tale punto, l'OdV condurrà controlli a campione sulle attività potenzialmente a rischio, diretti a verificare la corretta applicazione dei presidi specifici sopra individuati.
- Verificare l'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni.
- Proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Sezione.
- Proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Sezione.
- L'Organismo di Vigilanza attiva una serie di scambi di informazioni con i responsabili delle aree a rischio sopra individuate, al fine di attuare efficacemente le proprie attività di vigilanza.
- Esaminare i flussi informativi periodici ed eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute
- Conservare traccia dei flussi informativi periodici ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti

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

6.5.1. Controlli periodici dell'OdV

L'OdV svolge le seguenti attività di verifica, con la cadenza indicata:

Controllo	Oggetto	Cadenza	Output
Audit su incident reporting	Verifica che gli eventi contaminanti siano stati segnalati nei tempi previsti e che la procedura Incident reporting ambientale sia stata correttamente applicata	Ad evento + verifica annuale di sistema	Nota di verifica
Monitoraggio indicatori di rischio (KRI)	Numero di sospensioni di liquidazione per documentazione ambientale; numero di contestazioni a fornitori; numero di contestazioni da autorità;; ritardi nella trasmissione all'OdV dei flussi informativi	Trimestrale	Report nel Verbale di verifica
Verifica clausole contrattuali ambientali	Controllo a campione che i contratti stipulati contengano le clausole di cui al paragrafo 6.6 della presente Parte Speciale	Annuale	Verbale di verifica

6.5.2. Flussi informativi verso l'organismo di vigilanza

Sussiste a carico di tutti i Destinatari del MOG (soggetti apicali, sottoposti, consulenti, etc.) l'**obbligo di segnalazione immediata all'OdV** in caso di notizie rilevanti sulla vita dell'Ente, violazioni del Modello, della presente Parte Speciale o situazioni di riscontrata inadeguatezza e/o non conformità di comportamenti ai principi contenuti nelle procedure/istruzioni aziendali e nel Codice Etico.
Le segnalazioni di illeciti, secondo le istruzioni impartite dall'OdV, dovranno avvenire con le modalità indicate nell'apposita **Procedura "*Flussi Informativi*",** nel rispetto della normativa in tema di *Whistleblowing*.
Con riferimento ai controlli periodici sui processi aziendali e allo svolgimento delle normali attività il D.Lgs. n. 231/01 prevede **flussi informativi con cadenze determinate** verso l'OdV da parte di specifici soggetti. Si rinvia alla **Procedura "*Flussi Informativi*"** per la descrizione delle specifiche modalità operative con cui dovranno essere inviati i suddetti flussi.

Flussi periodici obbligatori
Le seguenti funzioni trasmettono all'OdV, con la cadenza indicata, le informazioni di seguito specificate:

Funzione	Informazione	Cadenza	Formato
RUP/Ufficio Contratti	Elenco appaltatori attivi con documentazione ambientale aggiornata (autorizzazioni, iscrizioni Albo, certificazioni); segnalazione di scadenze imminenti	Semestrale	Report strutturato
RUP/Ufficio Contratti	Segnalazione di sospensioni di liquidazione per documentazione ambientale irregolare	Immediata (entro 48 ore)	Comunicazione scritta
DL / Resp. Tecnico	Segnalazione di eventi contaminanti, sversamenti, abbandoni di rifiuti; esiti della procedura di incident reporting	Immediata (fase 1 e 4 di PROC-AMB-02)	Comunicazione scritta
Ufficio Contratti	Elenco dei casi in cui sono state applicate penali contrattuali per violazioni ambientali; casi di attivazione della clausola risolutiva	Semestrale	Report strutturato
Legale/Compliance	Comunicazione di qualsiasi provvedimento, verbale, ispezione, prescrizione, contestazione amministrativa o penale di natura ambientale ricevuta da ERP Lucca S.r.l.	Immediata (entro 24 ore dal ricevimento)	Comunicazione scritta con copia del provvedimento

Flussi straordinari
Indipendentemente dalla cadenza periodica, è obbligatoria la segnalazione immediata all'OdV di:

- qualsiasi notizia di indagine penale o amministrativa avente ad oggetto reati ambientali riconducibili alle attività di ERP Lucca S.r.l. o di suoi appaltatori/fornitori;
- qualsiasi richiesta di informazioni da parte delle autorità di controllo ambientale (ARPA, Polizia Provinciale, Carabinieri Forestali, ecc.);
- qualsiasi situazione in cui si rilevi o si sospetti fondatamente che un appaltatore stia gestendo i rifiuti di cantiere in modo illecito;
- casi in cui il costo dichiarato per il trasporto e lo smaltimento dei rifiuti risulti significativamente inferiore ai valori di mercato correnti, potenzialmente indicativo di irregolarità nella filiera di smaltimento.

SEZIONE 7:

REATI TRIBUTARI

(ART. 25-QUINQUIESDECIES)

7. ART. 25-QUINQUIESDECIES – REATI TRIBUTATI

7.1. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS.N.231/01

7.1.1. Definizioni

Per una appropriata lettura e comprensione delle disposizioni di legge di cui appresso va premesso che, ai fini della normativa tributaria di cui al citato D.lgs. n.74/2000, si applicano le seguenti definizioni di carattere generale applicabili a tutti i Reati Presupposto tributari:

a) per "fatture o altri documenti per operazioni inesistenti" si intendono le fatture o gli altri documenti aventi rilievo probatorio analogo in base alle norme tributarie, *(i)* emessi a fronte di operazioni non realmente effettuate in tutto o in parte o *(ii)* che indicano i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, ovvero *(iii)* che riferiscono l'operazione a soggetti diversi da quelli effettivi;
b) per "elementi attivi o passivi" si intendono *(i)* le componenti, espresse in cifra, che concorrono, in senso positivo o negativo, alla determinazione del reddito o delle basi imponibili rilevanti ai fini dell'applicazione delle imposte sui redditi o sul valore aggiunto e *(ii)* le componenti che incidono sulla determinazione dell'imposta dovuta;
c) per "dichiarazioni" si intendono anche le dichiarazioni presentate in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche o di sostituto d'imposta, nei casi previsti dalla legge;
d) il "fine di evadere le imposte" e il "fine di consentire a terzi l'evasione" si intendono comprensivi, rispettivamente, anche *(i)* del fine di conseguire un indebito rimborso o il riconoscimento di un inesistente credito d'imposta, e *(ii)* del fine di consentirli a terzi;
e) riguardo ai fatti commessi da chi agisce in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche, il "fine di evadere le imposte" ed il "fine di sottrarsi al pagamento" si intendono riferiti alla società, all'ente o alla persona fisica per conto della quale si agisce;
f) per "imposta evasa" si intende la differenza tra l'imposta effettivamente dovuta e quella indicata nella dichiarazione, ovvero l'intera imposta dovuta nel caso di omessa dichiarazione, al netto delle somme versate dal contribuente o da terzi a titolo di acconto, di ritenuta o comunque in pagamento di detta imposta prima della presentazione della dichiarazione o della scadenza del relativo termine; non si considera imposta evasa quella teorica e non effettivamente dovuta collegata a una rettifica in diminuzione di perdite dell'esercizio o di perdite pregresse spettanti e utilizzabili;

g) le soglie di punibilità riferite all'imposta evasa si intendono estese anche all'ammontare dell'indebito rimborso richiesto o dell'inesistente credito di imposta esposto nella dichiarazione;
h) per "operazioni simulate oggettivamente o soggettivamente" si intendono (i) le operazioni apparenti, diverse da quelle disciplinate dall'articolo 10-bis della legge 27 luglio 2000, n. 212, poste in essere con la volontà di non realizzarle in tutto o in parte ovvero (ii) le operazioni riferite a soggetti fittiziamente interposti;
i) per "mezzi fraudolenti" si intendono condotte artificiose attive nonché quelle omissive realizzate in violazione di uno specifico obbligo giuridico, che determinano una falsa rappresentazione della realtà.

7.1.2. Le fattispecie di reato

Il D.L. n. 124/2019, convertito in **L. n. 157/2019** pubblicata in Gazzetta Ufficiale n. 301 del 24/12/2019, ha esteso la responsabilità amministrativa delle società, degli enti e delle associazioni anche prive di personalità giuridica alla commissione di determinati reati tributari.
In particolare, l'art. 39, co. 2, del citato Decreto ha ampliato, con efficacia dalla data di pubblicazione in Gazzetta Ufficiale della Legge di conversione dello stesso, la portata dell'art. **25 *quinquiesdecies* del D.lgs. n. 231/2001**, rubricato "Reati tributari", introducendo nel catalogo dei reati presupposto le fattispecie più gravi di reati **tributari disciplinati dal D.lgs. n. 74/2000:**

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art 2);
- Dichiarazione fraudolenta mediante altri mezzi fraudolenti (art. 3);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8);
- Occultamento o distruzione dei documenti contabili al fine di evadere le imposte (art. 10);
- Sottrazione fraudolenta al pagamento delle imposte (art. 11).

Inoltre, con l'entrata in vigore del **Decreto legislativo 14 luglio 2020, n. 75,** solo se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, sono entrati a far parte dei reati presupposto tributari i seguenti delitti previsti dal decreto legislativo 10 marzo 2000, n. 74:

- dichiarazione infedele previsto dall'articolo 4;
- omessa dichiarazione previsto dall'articolo 5;
- indebita compensazione previsto dall'articolo 10-quater.

Con il Decreto Legislativo 14 giugno 2024, n. 87 sono stati introdotte rilevanti modifiche alla disciplina dei **reati tributari** (art.25-quinquiesdecies D.lgs.231/01): introduzione di nuovi elementi/definizioni (es. su indebita compensazione, omessi versamenti).

L'art 25 *quinquiesdecies* così recita:
"*... 1. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, si applicano all'ente le seguenti sanzioni pecuniarie:*

a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 1, la sanzione pecuniaria fino a cinquecento quote;
b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 2, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
c) per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote;
d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, la sanzione pecuniaria fino a cinquecento quote;
e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
f) per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote;
g) per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote.
1-bis. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, si applicano all'ente le seguenti sanzioni pecuniarie:
a) per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote;
b) per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote;
c) per il delitto di indebita compensazione previsto dall'articolo 10-quater, la sanzione pecuniaria fino a quattrocento quote.
2. Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.
3. Nei casi previsti dai commi 1 e 2, si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e)... ».

Le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e) sono di seguito riportate:

- divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio (il divieto di contrattare con la pubblica amministrazione può anche essere limitato a determinati tipi di contratto o a determinate amministrazioni; può essere definitivo quando l'ente è già stato condannato alla stessa sanzione almeno tre volte negli ultimi sette anni);
- esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- divieto di pubblicizzare beni o servizi.

Quando nei confronti dell'ente viene applicata una sanzione interdittiva può essere disposta la pubblicazione della sentenza di condanna, che viene eseguita "a spese dell'ente" (art. 18).
Con la sentenza di condanna è sempre disposta la confisca del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato (sono comunque fatti salvi i diritti acquisiti

dai terzi in buona fede). Quando non è possibile eseguire la confisca a norma del comma 1, la stessa può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato.
Tra le novità previste dalla legge di conversione (L. 157/2019) c'è l'applicabilità a determinati reati tributari (segnatamente, a quelli previsti e puniti dagli artt. 2, 3, 8 e 11 d.lgs. n. 74/2000) della c.d. "confisca allargata", cioè della " confisca del denaro, dei beni o delle altre utilità di cui il condannato non può giustificare la provenienza e di cui, anche per interposta persona fisica o giuridica, risulta essere titolare o avere la disponibilità a qualsiasi titolo in valore sproporzionato al proprio reddito, dichiarato ai fini delle imposte sul reddito, o alla propria attività economica " (artt. 12 *ter* d.lgs. n. 74/2000 e 240 bis c.p.).

Di seguito si descrivono le singole fattispecie di reati tributari rilevanti per la società.

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

"... 1. E' punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.
2. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.
2-bis. Se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni ...".

SOGGETTO ATTIVO: Coloro (firmatari) che sono obbligati dalla legge tributaria a presentare le dichiarazioni ai fini dei redditi o ai fini IVA (si tratta, quindi, di un reato proprio).
La dichiarazione dei soggetti diversi dalle persone fisiche è sottoscritta, a pena di nullità, dal rappresentante legale, e in mancanza da chi ne ha l'amministrazione anche di fatto, o da un rappresentante negoziale (artt. 1, co. 4 e 8, co. 6, d.p.r. 322/98).
Nei casi di fallimento o di liquidazione coatta amministrativa, le dichiarazioni sono presentate dal curatore o dal commissario liquidatore (artt. 5, co. 4, e 8, co. 4, d.p.r. 322/98).
CONDOTTA BIFASICA:
1) Detenzione (ai fini di prova nei confronti dell'Amministrazione finanziaria) o contabilizzazione di fatture o altri documenti per operazioni inesistenti:

- Fatture
- Altri documenti aventi valore probatorio, a fini fiscali, dell'avvenuta realizzazione di operazioni economiche (scontrini, ricevute fiscali, schede carburante, bolle di accompagnamento, parcelle, prospetti paga, documenti di trasporto, note di addebito, note di credito)
- Operazioni inesistenti penalmente rilevanti:

a) Inesistenza oggettiva, in quanto l'operazione non è mai avvenuta in tutto o in parte.

Tale ipotesi, più diffusa, consiste nell'emissione di fatture (lato senso intese) a fronte di prestazioni mai effettuate ovvero realmente effettuate ma per quantitativi inferiori rispetto a quelli documentalmente indicati.

b) Inesistenza soggettiva - rilevante solo ai fini IVA - in quanto uno dei soggetti indicati in fattura è rimasto del tutto estraneo all'operazione documentata (con esclusione dunque delle ipotesi di fatture solo parzialmente soggettivamente inesistenti, in cui beneficiario della prestazione sia anche un terzo - es. ristrutturazione di un immobile adibito non solo a uso aziendale ma anche abitativo, il cui costo venga portato in detrazione dall'azienda).

Tale ipotesi sussiste, quindi, quando a fronte di un'operazione commerciale effettivamente avvenuta, le fatture o gli altri documenti aventi rilievo probatorio in base alle norme tributarie, riferiscono l'operazione a soggetti diversi da quelli effettivi.

Rientra nell'ambito dell'inesistenza soggettiva sia il caso dell'"*interposizione fittizia*" che il caso dell'"*interposizione reale*":

- *Interposizione fittizia:* L'operazione è in realtà avvenuta ma tra soggetti diversi da quelli dichiarati (tutti i soggetti di essa vogliono che gli effetti del negozio si producano nei confronti di una persona diversa da quella che appare nell'atto (c.d. "simulazione relativa soggettiva");
- *Interposizione reale:* Gli effetti della vendita si producono realmente in capo all'acquirente e, quindi, manca un accordo simulatorio. Pertanto, affinchè possano aversi effetti tributari penalmente rilevanti, occorre che una terza persona ponga in essere un successivo negozio di trasferimento in favore di un altro soggetto.

- Falsità ideologica o materiale (anche autoprodotta): Indicazione in una delle dichiarazioni relative alle imposte sul reddito o sul valore aggiunto di elementi passivi fittizi.

2) Indicazione in una delle dichiarazioni relative alle imposte sul reddito o sul valore aggiunto di elementi passivi fittizi:

- Si allude a tutte le dichiarazioni finalizzate a determinare reddito, basi imponibili e imposta:

- Dichiarazioni annuali;
- Dichiarazioni straordinarie in caso di liquidazione, liquidazione coatta amministrativa, fallimento, trasformazione, fusione, scissione;
- Dichiarazione consolidata di gruppo.

- Elementi passivi fittizi

Tale ipotesi delittuosa ricorre, quindi, tutte le volte in cui la dichiarazione, oltre ad essere non veritiera, risulti "insidiosa", ossia sorretta da un impianto contabile o documentale di comodo in grado di sviare o intralciare la successiva attività di accertamento da parte dell'Amministrazione finanziaria.

La condotta consiste nell'indicazione in una delle dichiarazioni relative all'IVA o ai redditi di elementi passivi fittizi, giustificati da fatture o altri documenti per operazioni inesistenti, con cui vengono artificiosamente "gonfiate" le componenti negative del reddito al fine di diminuire l'imponibile e, conseguentemente, l'imposta dovuta all'erario.

DOLO SPECIFICO

Finalità di evadere le imposte sui redditi o sul valore aggiunto. Il dolo specifico deve essere diretto a realizzare un'evasione propria, non assumendo rilevanza l'evasione altrui.

CONSUMAZIONE E TENTATIVO

Il momento in cui si consuma il reato in questione coincide con la presentazione della dichiarazione annuale ai fini dei redditi o del valore aggiunto.

Il delitto ha quindi natura istantanea, consumandosi con la presentazione della dichiarazione annuale.

Ai sensi dell'art del D.lgs. 74/2000, nell'ipotesi di dichiarazione fraudolenta mediante uso di fatture per operazioni inesistenti non è configurabile il tentativo.

Anche la Suprema Corte ha confermato che i comportamenti tenuti dall'agente prima della presentazione della dichiarazione (comprese le condotte di acquisizione e registrazione nelle scritture contabili di fatture o documenti fittizi), sono irrilevanti ai fini penali del presente articolo, in quanto per la configurabilità del reato in esame è indispensabile la presentazione della dichiarazione e l'effettivo inserimento nella stessa di elementi passivi fittizi (*Cass. Pen., sez. III, 20/05/2014 n. 52752).*

TRATTAMENTO SANZIONATORIO

Il DL 124/2019 ha introdotto un'ipotesi particolare di confisca, disciplinata dal nuovo articolo 12-*ter* D.lgs. 74/2000, secondo il quale, nei casi di condanna o di applicazione della pena per il delitto di cui all'articolo 2, quando l'ammontare degli elementi passivi fittizi è superiore ad euro centomila, si applica l'art 240 bis c.p. (c.d. "*confisca allargata*"). Tale confisca allargata ha ad oggetto il denaro, i beni o le altre utilità di cui il condannato non può giustificare la provenienza e di cui, anche per interposta persona fisica o giuridica, risulta essere titolare o avere la disponibilità a qualsiasi titolo in valore sproporzionato al proprio reddito, dichiarato ai fini selle imposte sul reddito o alla propria attività economica.

N.B. Con l'inclusione dei reati tributari nel catalogo dei reati presupposto, ad opera dell'art 39 del D.L. 124/2019, sarà possibile procedere direttamente alla "*confisca diretta*" o alla "*confisca per equivalente*" del patrimonio dell'ente ai sensi dell'art 19 del D.lgs. 231/01, nonché al sequestro preventivo di cui all'art 53 dello stesso Decreto.

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

"*... 1. Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:*

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

b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero

qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.
2. Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.
3. Ai fini dell'applicazione della disposizione del comma 1, non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali…".

SOGGETTO ATTIVO: Il delitto in questione ha natura di "reato comune", potendo essere commesso da chiunque abbia presentato una dichiarazione tributaria ai fini delle imposte dirette o dell'IVA attraverso le modalità fraudolente descritte dalla norma.
L'unica categoria esclusa dal novero dei soggetti attivi di tale fattispecie è quella dei sostituti d'imposta (ricompresi unicamente tra gli autori del delitto di cui all'art 5 D.lgs. 74/2000).
CONDOTTA
La norma in questione prevede una pluralità di condotte che, comunque incentrandosi nel complesso sulla presentazione della dichiarazione, integrano alternativamente ed autonomamente il delitto di frode fiscale.
Realizzazione di artifici (alternativamente) con:

1) Compimento di operazioni simulate

- Oggettivamente (non avvenute)
- Soggettivamente (avvenute ma tra soggetti diversi)

2) Utilizzo di documenti falsi

- contabilizzati
- detenuti ai fini di prova

N.B. Si fa riferimento ai documenti registrati nelle *scritture contabili obbligatorie* (cioè nelle scritture indicate dall'art 2214 c.c. e dagli artt. 14 e ss. Del D.P.R. 600/73), *o detenuti ai fini di prova nei confronti dell'amministrazione finanziaria.*
In particolare, rientrano nella categoria delle scritture contabili obbligatorie:
- Registri IVA delle fatture, dei corrispettivi e degli acquisti;
- le Scritture ausiliarie;
- il Registro dei beni ammortizzabili;
- il Registro riepilogativo di magazzino;
- i Libri sociali obbligatori.

A ben vedere, l'utilizzo di tali documenti falsi presenta molte affinità con la c.d. "*falsa rappresentazione nelle scritture contabili obbligatorie*" dell'abrogato articolo 3 (appare quindi ragionevole ritenere che tale soppressione risulti solo apparente con la conseguente indiretta permanenza della rilevanza penale della falsità in scritture contabili obbligatorie anche nella nuova ipotesi di frode fiscale).

La detenzione di tali documenti, essendo finalizzata alla prova per l'amministrazione finanziaria, non si esaurisce nella loro semplice conservazione ma presuppone che gli stessi possano essere esibiti all'Amministrazione o addirittura trasmessi su richiesta di quest'ultima.

3) Utilizzo di "altri mezzi fraudolenti" idonei a ostacolare l'accertamento e a indurre in errore il fisco (escluse le mere ipotesi di omessa fatturazione, sotto-fatturazione, indicazione di elementi attivi inferiori a quelli reali).

N.B. Per "*mezzo fraudolento*" (ai sensi dell'art 1, co. 1, lett g-ter del D.lgs. 74/2000) si intende la condotta artificiosa attiva nonché quella omissiva realizzate in violazione di uno specifico obbligo giuridico che determina una falsa rappresentazione della realtà.
Secondo dottrina maggioria la "*contabilità in nero*" - essendo priva di concreta capacità decettiva e non essendo destinata all'Amministrazione Finanziaria - non appare idonea ad integrare un mezzo fraudolento.
Indicazione in una delle dichiarazioni relative alle imposte sul reddito o sul valore aggiunto di:

- Componenti attivi inferiori: «elementi attivi per un ammontare inferiore a quello effettivo»
- Componenti passivi fittizi: «elementi passivi fittizi o crediti e ritenute fittizi»

Superamento delle soglie di punibilità (congiuntamente)

- Imposta evasa , con riferimento a taluna delle singole imposte, sia superiore a 30.000 €;
- Ammontare complessivo degli elementi attivi sottratti all'imposizione sia superiore al 5% dell'ammontare complessivo degli elementi attivi indicati nella dichiarazione o comunque superiore ad 1,5 milioni di €;
- ovvero ammontare complessivo di crediti e ritenute fittizie in diminuzione dell'imposta sia superiore al 5% dell'imposta medesima ovvero sia superiore a 30.000 €.

Imposta evasa
Sussiste questo requisito allorquando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte (imposte sui redditi o sul valore aggiunto), a euro trentamila. Ai sensi dell'art. 1 lett. f) D.lgs. 74/2000 per "imposta evasa" si intende la differenza tra l'imposta effettivamente dovuta e quella indicata nella dichiarazione, ovvero l'intera imposta dovuta nel caso di omessa dichiarazione, al netto delle somme versate dal contribuente o da terzi a titolo di acconto, di ritenuta o comunque in pagamento di detta imposta prima della presentazione della dichiarazione o della scadenza del relativo termine.
La successiva lett. g) dello stesso articolo stabilisce che le soglie di punibilità riferite all'imposta evasa si intendono estese anche all'ammontare dell'indebito rimborso richiesto o dell'inesistente credito d'imposta esposto nella dichiarazione. In forza di quest'ultima precisazione estensiva, dunque, ai fini della valutazione del superamento delle soglie di punibilità, vengono ad essere accomunate:
a. L'ipotesi classica dell'imposta evasa
b. L'indebita richiesta di rimborso
c. L'inesistente esposizione di credito d'imposta
DOLO SPECIFICO
Finalità di evadere le imposte sui redditi o sul valore aggiunto.

La giurisprudenza prevalente ritiene che le soglie di punibilità abbiano natura di elementi costitutivi del reato. Di conseguenza il dolo va inteso come coscienza e volontà anche del superamento delle soglie di punibilità.

CONSUMAZIONE E TENTATIVO

Il delitto di dichiarazione fraudolenta mediante altri artifici è un reato istantaneo e si perfeziona nel momento in cui viene presentata la dichiarazione mendace che, in qualità di atto recettizio, esplica i suoi effetti giuridici nel momento in cui perviene all'ufficio finanziario competente.

Quanto alla forma tentata, l'articolo 6 D.lgs. 74/2000 esclude che il reato in questione possa essere punito a titolo di tentativo.

- **EMISSIONE DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 8 D.LGS. 74/2000, comma 1 e comma 2 *bis*):**

"*... 1. E' punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.*

2. Ai fini dell'applicazione della disposizione prevista dal comma 1, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

2-bis. Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni...".

SOGGETTO ATTIVO: Reato comune, che può essere commesso da "*chiunque*".

CONDOTTA

Si tratta di un reato di mera condotta (di tipo commissivo), di pericolo, consistente nell'emissione o rilascio di fatture o altri documenti per operazioni inesistenti.

- Emissione di fatture o rilascio di altri documenti fiscalmente rilevanti:
  - Emissione di Fatture
  - Rilascio di altri documenti fiscalmente rilevanti (es: ricevuta o scontrino fiscale)

Le due condotte sopra esposte, alternativamente previste dalla norma incriminatrice, hanno un "nucleo concettuale comune" rappresentato dalla fuoriuscita del documento fiscale mendace dalla disponibilità dell'emittente (cioè di colui che lo ha formato mediante consegna a mano o spedizione o trasmissione telematica al destinatario).

- Sufficiente anche un solo documento falso.
- Unico reato anche in caso di pluralità di documenti falsi emessi o rilasciati nel medesimo periodo di imposta.

N.B. In relazione alle persone giuridiche, ai sensi dell'art 76, comma 2, DPR 12 dicembre 1986 n. 917, "*... il periodo di imposta è costituito dall'esercizio o periodo di gestione della società o dell'ente determinato dalla legge o dall'atto costitutivo. Se la durata dell'esercizio o periodo di gestione non è determinato da legge o atto costitutivo, o è determinata in due o più anni, il periodo di imposta è costituito dall'anno solare...".*

- Attestazione di operazioni nella realtà inesistenti (falsità ideologica):

- Rilevanza delle fatture per operazioni soggettivamente inesistenti (rilevante ai soli fini IVA)
- Inesistenza oggettiva:
  - Comprese le ipotesi di sovrafatturazione quantitativa (con indicazione del corrispettivo o iva in misura superiore a quella reale);

- Sono escluse le ipotesi di operazioni nulle, annullabili, incongrue dal punto di vista economico e di sovrafatturazione qualitativa (realizzate attraverso una maggiorazione del prezzo rispetto al reale valore di beni o servizi forniti).

N.B. Non possono considerarsi penalmente rilevanti ex art. 8 D.lgs. 74/2000 nemmeno le "*schede carburanti*" in quanto sono emesse dallo stesso soggetto che acquista il carburante e non già dal cedente.

DOLO SPECIFICO.

Finalità di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto.

Irrilevanza penale delle condotte aventi fini esclusivamente extratributari (es: consentire l'esercizio di un'attività professionale ad un soggetto non abilitato; consentire un differimento infrannuale del versamento IVA stornando successivamente le fatture emesse).

Secondo dottrina e giurisprudenza maggioritaria laddove la finalità perseguita dall'emittente sia esclusiva rispetto a quella dell'evasione fiscale altrui, l'emittente non può rispondere per il delitto in questione proprio per difetto del dolo specifico richiesto dall'art 8 (es: nei casi in cui i documenti falsi siano emessi per ottenere indebite sovvenzioni, per consentire all'utilizzatore di ottenere un finanziamento, per realizzare una truffa, etc.).

CONSUMAZIONE E TENTATIVO

Il delitto si consuma con l'emissione o il rilascio dei documenti fiscali mendaci, ovvero nel momento in cui questi ultimi esorbitano dalla disponibilità dell'emittente e pervengono al destinatario tramite consegna *brevi manu* o spedizione (anche telematica).

Nell'ipotesi in cui i documenti falsi, emessi o rilasciati nel corso del medesimo periodo d'imposta, siano plurimi, il delitto si consuma al momento dell'emissione o rilascio dell'ultimo di essi.

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

"… Salvo che il fatto costituisca più grave reato, è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari …".

Si tratta di reato di pericolo concreto, non essendo necessario il verificarsi di un danno per l'Erario.

SOGGETTO ATTIVO: Tale fattispecie non si rivolge solo ed esclusivamente ai soggetti obbligati alla tenuta delle scritture contabili; infatti la fattispecie contempla anche "documenti" per i quali non è previsto un particolare regime contabile, di guisa che siamo in presenza di un reato comune. Per i soggetti diversi dal contribuente si pensi, ad esempio, al consulente tenuti alla conservazione di documenti fiscali.

In particolare, la giurisprudenza ha affermato che l'imprenditore non può essere individuato come autore diretto del reato se ha affidato le scritture contabili al commercialista di fiducia, che poi non le ha esibite alla Guardia di Finanza (*Cfr. Cass. Pen., sez. III, 19 marzo 2015, n. 11479*).

CONDOTTA

La condotta sanzionata dall'art. 10 è solo quella di occultamento o distruzione (anche solo parziale) delle scritture contabili obbligatorie e *non anche quella della loro mancata tenuta*, espressamente sanzionata in via meramente amministrativa dall'art. 9 del d.lgs. n. 471 del 1997 (*Sez. 3, n. 38224 del 07/10/2010*). In altre parole, la fattispecie criminosa dell'art. 10 presuppone l'istituzione della documentazione contabile.

In primis, si precisa che per *scritture contabili o documenti di cui è obbligatoria la conservazione* si intende, ai sensi dell'art. 2214 c.c.:

- Libro giornale,
- Libro degli inventari
- Altre scritture contabili che siano richieste dalla natura e dalle dimensioni dell'impresa (es. contratto preliminare di compravendita di immobili stipulato da un'impresa di costruzioni)

Condotta commissiva:

- Occultamento: temporanea o definitiva indisponibilità della documentazione da parte degli organismi verificatori (documenti materialmente nascosti, posti in un luogo diverso da quello preposto a conservarli o semplice rifiuto della loro esibizione);
- Distruzione: soppressione del documento, cancellazione o abrasioni parziali di certe sue parti rilevanti per accertare il volume d'affari;
- Omessa tenuta delle scritture contabili (rilevanza penale controversa).

- Idoneità della condotta ad impedire la ricostruzione del volume d'affari.

N.B. L'occultamento e la distruzione della contabilità in sé non integrano il reato *de quo* se non hanno determinato l'impossibilità di procedere alla ricostruzione dei redditi o del volume d'affari.

Irrilevanza penale della condotta qualora ci sia la possibilità di ricostruire comunque il volume di affare, inteso quale «ammontare complessivo delle cessioni di beni e delle prestazioni di servizi [..] effettuate, registrate o soggette a registrazione nel corso di un anno solare» (art. 20 d.p.r. 633/72).

Secondo la dottrina prevalente, l'occultamento o la distruzione di più documenti determina la realizzazione di un unico reato laddove questi si riferiscano ad un medesimo periodo di imposta.

DOLO SPECIFICO

Coscienza e volontà di distruggere le scritture contabili o i documenti di cui è obbligatoria la conservazione e di determinare così l'impossibilità di procedere alla ricostruzione dei redditi o del volume d'affari.

Il delitto richiede che la volontà dolosa abbia una determinata direzione, cioè finalità di evadere o di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto.

CONSUMAZIONE E TENTATIVO

In ordine al momento consumativo, esso è diverso a seconda che si tratti di occultamento o distruzione.

a) L'occultamento costituisce un reato permanente che si consuma nel momento dell'ispezione e cioè nel momento in cui gli agenti chiedono di esaminare detta documentazione;

b) La distruzione realizza un'ipotesi di reato istantaneo e si consuma nel momento della soppressione della documentazione.

- **SOTTRAZIONE FRAUDOLENTA AL PAGAMENTO DI IMPOSTE (ART. 11 D.LGS. 74/2000):**

"... 1. E' punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.
2. E' punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni...".
Il bene giuridico protetto è il corretto funzionamento della procedura di riscossione coattiva in relazione al diritto di credito dell'Erario (si tratta solo di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte).

SOGGETTO ATTIVO: il richiamo in ambedue i commi della parola "chiunque" non deve trarre in inganno:
si tratta, infatti, di un reato proprio in quanto i potenziali soggetti attivi del reato possono essere esclusivamente i contribuenti tenuti al pagamento delle imposte sui redditi o sul valore aggiunto.
La fattispecie di cui al secondo comma è stata definita reato proprio a soggettività allargata perché attuabile anche da persona diversa dal debitore, difatti la norma espressamente dice: "*al fine di ottenere per sé o per altri un pagamento parziale dei tributi".* La dottrina ritiene quindi che soggetto attivo, in tal caso, sia l'imprenditore e l'amministratore dell'ente in crisi ovvero il soggetto che presenta e sottoscrive la transazione fiscale (es: il professionista che predispone ed attesta, con apposita relazione, la veridicità di quanto contenuto nel piano di ristrutturazione aziendali, quando vi siano elementi attivi o passivi sottostimati o sopravvalutati).
Il fatto che i beni oggetto della condotta possano anche essere "altrui" conferma che si possa riferire la condotta tipica anche a chi agisca come rappresentante della persona giuridica contribuente (quale amministratore, liquidatore, etc.).
CONDOTTA
La condotta del reato in questione ha natura esclusivamente commissiva e può consistere:

- COMMA 1 → nell'alienare simulatamente o nel compiere altri atti fraudolenti sui propri o su altrui beni (sia beni mobili che immobili); si tratta, quindi, di un'attività di materiale sottrazione di disponibilità.

- L'alienazione può definirsi "*simulata*", quando sia finalizzata a creare una situazione giuridica apparente diversa da quella reale; l'atto oggetto di contestazione deve quindi essere idoneo a

rappresentare una realtà non corrispondente al vero, mettendo a repentaglio (o comunque ostacolando) l'azione di recupero del bene da parte dell'erario. Serve una valutazione *ex ante* circa la suddetta idoneità dell'atto simulato a rendere inefficace l'attività recuperatoria dell'Amministrazione finanziaria.

Sono penalmente rilevanti, a titolo esemplificativo, le seguenti condotte:

- Condotta di colui che aveva realizzato la vendita di una particella immobiliare ad una società svizzera con soci non identificabili al solo fine di sottrarre il bene alla procedura esecutiva dell'Agenzia delle Entrate (*Cass. Pen, sez. III, sent. n. 13233 del 24/02/2016);*
- Condotta di un commercialista che in prossimità degli esiti di una verifica fiscale, aveva ceduto immobili e quote sociali alla convivente (*Cass. Pen, sez. III, Sent. n. 39079 del 09.04.2013*).

La casistica trattata dalla giurisprudenza ha consentito di ritenere integrato il reato allorquando:

1) È stato costituito un fondo patrimoniale;
2) Si è verificata anche solo una simulazione soggettiva mediante una interposizione fittizia di persona;
3) Gli amministratori di una società hanno realizzato più operazioni di cessioni di aziende e scissioni societarie simulate finalizzate a conferire ai nuovi soggetti societari beni immobili;
4) Si è realizzata una pluralità di trasferimenti immobiliari, costituenti un'operazione unitaria;
5) Si è alienato simulatamente l'avviamento commerciale di un'impresa.

- Per "atti fraudolenti" devono intendersi quei comportamenti che, quand'anche formalmente leciti, siano tuttavia connotati da elementi di inganno o di artificio, dovendosi ravvisare l'esistenza di uno stratagemma tendente a sottrarre garanzie patrimoniale all'esecuzione.

Esempi di atti fraudolenti penalmente rilevanti:

1) Smobilitazione di un'ingente somma di denaro giacente presso un deposito fiduciario con trasformazione in numerosi assegni circolari di importo inferiore al limite di tracciabilità;
2) Costituzione di un trust/fondo patrimoniale in un periodo precedente all'attività accertativa e di riscossione dell'Amministrazione Finanziaria → laddove sia idoneo a rappresentare ai terzi una realtà (riduzione di patrimonio) non corrispondente al vero.

- COMMA 2 → nell'indicare, nella documentazione presentata ai fini della procedura di transazione fiscale, elementi attivi o passivi diversi da quelli reali (quindi un'attività di falsificazione della consistenza patrimoniale).

E' considerato reato di pericolo concreto in quanto la condotta deve essere idonea alla lesione dell'oggetto di tutela ed il fine della medesima deve specificamente essere quello della sottrazione al pagamento di imposte, che costituisce il "concreto" danno erariale.

DOLO SPECIFICO

COMMA 1 → Il dolo è costituto dalla consapevolezza della preesistenza di un debito nei confronti del fisco complessivamente superiore a 50.000 euro e dalla coscienza e volontà di realizzare le condotte tipiche sopra analizzate. L'azione deve essere ulteriormente sorretta dal dolo specifico, consistente nella finalità di sottrarre beni all'esecuzione forzata (tale finalità può concorrere con altre, non

essendo necessario che l'atto posto in esser sia totalmente privo di ogni altra ragione economico-giuridica).

COMMA 2 → volontà di ottenere un pagamento parziale dei tributi o dei relativi accessori; l'autore deve rappresentarsi e volere la presentazione di documenti falsi nel contesto della procedura di transazione fiscale, mediante il carattere fittizio degli elementi indicati per una somma che superi la soglia di punibilità ivi prevista.

L'unico presupposto per la configurabilità del reato è l'esistenza di uno specifico debito tributario, comprensivo di interessi e sanzioni, di ammontare superiora ad euro 50.000. Tale soglia rappresenta un elemento costitutivo del fatto tipico.

CONSUMAZIONE E TENTATIVO

COMMA 1 → Il delitto si consuma con la conclusione dell'atto fraudolento idoneo a mettere in pericolo il bene giuridico tutelato.

Nel caso in cui la condotta si articoli in una pluralità di azioni (es: trasferimenti immobiliari), finalizzate a rendere in tutto o in parte inefficace la procedura di riscossione coattiva, il delitto si perfeziona con il compimento del primo atto e si consuma nel momento in cui viene realizzato l'ultimo atto dispositivo.

Trattandosi di un delitto di pericolo, è controversa la configurabilità del tentativo, anche se recentemente la giurisprudenza della Suprema Corte si è espressa in senso positivo (cit. *Cass. Pen., Sez. III, 12.03.2019 n. 42936*).

COMMA 2 → Il delitto si consuma nel momento della presentazione della proposta di transazione fiscale ai competenti uffici dell'amministrazione finanziaria.

La dottrina, trattandosi di reato di pericolo, è divisa sulla possibilità di prevedere la forma tentata di tale fattispecie.

7.2. CONFIGURABILITÀ DEI REATI NEL CONTESTO DI ERP LUCCA

Tutti i reati di cui al paragrafo precedente possono, astrattamente, trovare spazio nel contesto in cui opera la società. Vi sono però alcune tipologie di reato, ricomprese nel novero di quelli "tributari", aggiunte nel catalogo di quelli presupposto ai sensi del D.lgs. n. 231/01 nel corso del 2020, che non risultano rilevanti nel caso di specie.

Ai soli fini di chiarezza si precisa che non sono ritenuti infatti rilevanti altri reati seppur compresi nel novero dei Reati Presupposto tributari (anch'essi previsti dal D.lgs. 10 marzo 2000, n. 74), in quanto la probabilità che le condotte da cui essi possono scaturire è risultata remota.

Ci riferiamo in particolare ai reati introdotti nell'alveo di quelli "231" con il Decreto Legislativo n. 75 del 14 luglio 2020 che ha recepito in via definitiva la Direttiva (UE) 2017/1371 (cd. Direttiva PIF) del Parlamento europeo e del Consiglio del 5 luglio 2017, recante norme per la "*lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale*".

Le modificazioni più rilevanti riguardano proprio l'art. 25-*quinquiesdecies*, disposizione recentemente introdotta nel decreto 231 per effetto del D.L. n. 124/2019, al quale viene aggiunto il nuovo comma 1-*bis*, che prevede, in relazione alla commissione dei reati tributari di cui agli artt. 4

(dichiarazione infedele), 5 (omessa dichiarazione) e 10-*quater* (indebita compensazione) d.lgs. n. 74/2000 e a condizione che gli stessi siano «*commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro*», l'irrogazione della sanzione pecuniaria fino a trecento quote per il delitto di dichiarazione infedele e fino a quattrocento quote per i delitti di omessa dichiarazione e indebita compensazione. Si tratta di ipotesi rispetto alle quali la probabilità di accadimento è stata ritenuta remota per come si sviluppano i processi e per i volumi di affari delle attività, storicamente al di sotto delle soglie di punibilità da cui possono originarsi imponibili Iva non inferiori ai dieci milioni di euro.

Tra le attività sensibili relative a tale area emerse dall'analisi dei rischi si ricordano:

DIREZIONE/U.O. RESPONSABILI	PROCESSO 231	ATTIVITA' PER PROCESSO
Manu.ne Straordinaria All. di Risulta	Programmazione, Progettazione interventi, Direzione dei lavori, esecuzione	FO-2.1 Progettazione degli interventi di manutenzione straordinaria FO-2.2 Studio di fattibilita' dei lavori e progettazione preliminare FO-2.3 Progettaz. definitiva ed esecutiva commesse di costruzione e recupero FO-2.4 Verifica della progettazione FO-4.1 Gestire gli adempimenti per la Direzione lavori FO-4.2 Effettuare la Direzione dei lavori FO-4.3 Eseguire l'Ultimazione dei lavori e il Collaudo
Gare e appalti	Gestire gli approvvigionamenti	FS-5.1 Gestione Acquisti di Servizi
S.I.A.	Gestione della bollettazione e della fatturazione attiva	FO-5.3 Gestire la bollettazione e la fatturazione
Ragioneria	Gestire l'Amministrazione e la Contabilità	FS-1. Gestire l'Amministrazione e la Contabilità
Ragioneria	Elaborare il bilancio di esercizio	Elaborare il bilancio di esercizio
Ragioneria	Gestione adempimenti tributari	Gestione adempimenti tributari
Patrimoniale	Gestire il Patrimonio	FO-6.3 Gestione delle vendite di unita' immobiliari
Ragioneria	Gestione risorse finanziarie	Gestione risorse finanziarie

7.3. PRESÌDI PREVISTI DAL MODELLO DI ORGANIZZAZIONE E GESTIONE

7.3.1. Principi

Organizzazione e poteri

Ciascuno dei responsabili delle funzioni aziendali o dei professionisti esterni coinvolti nello svolgimento della specifica operazione nell'ambito delle Aree a rischio o a supporto reato è formalmente investita della funzione di responsabile della singola operazione (d'ora innanzi, per brevità, il/i "**Responsabile/i**").

Tali Responsabili:

- divengono i soggetti referenti dell'operazione "a rischio o a supporto reato";

- devono rispettare i principi di comportamento contenuti nel Codice etico;
- I singoli Responsabili interni devono, altresì, fare in modo che i loro sottoposti, delegati a svolgere attività che comportano la gestione dei flussi, rispettino le prescrizioni e le Procedure in uso. Sulle operazioni in questione l'OdV potrà predisporre ulteriori controlli dei quali verrà data evidenza scritta.

In linea generale, il sistema di organizzazione per la gestione della materia in oggetto deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, e di segregazione delle funzioni e dei ruoli, in modo che nessun soggetto possa gestire da solo un intero processo, in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.
Ai componenti degli organi sociali e ai dipendenti che per conto della Società intrattengono rapporti con la Agenzia delle Entrate e le autorità/uffici fiscali in genere deve essere attribuito formale potere in tal senso. I soggetti muniti di poteri verso l'esterno devono agire nei limiti dei poteri ad essi conferiti. I soggetti privi di poteri verso l'esterno devono richiedere l'intervento dei soggetti muniti di idonei poteri.
Qualunque criticità o conflitto di interesse che dovessero sorgere nell'ambito del rapporto con le autorità fiscali devono essere comunicati, per iscritto, anche all'ODV.

7.3.2. Norme generali di comportamento

Obblighi e divieti di carattere generale

In ogni caso, il processo decisionale afferente le aree di attività a rischio di commissione di reati è uniformato ai seguenti obblighi:

a) Implementazione di un adeguato assetto amministrativo-contabile volto a rilevare tempestivamente eventuali crisi di impresa e relativa verifica da parte dell'Organo di Revisione contabile e di quello di controllo laddove nominato ai fini dell'applicazione della normativa sulla Crisi.
b) ogni operazione a rischio (ad es. acquisti), è preceduta da idonea identificazione, qualificazione e valutazione dell'altra parte contraente;
c) ogni operazione a rischio (es esecuzione contratti di servizio) è supportata da debita evidenza scritta (e-mail, rapporti scritti o corrispondenza), dal momento del suo instaurarsi, sino al suo perfezionamento; la documentazione deve essere ordinata in modo tale da consentire la tracciabilità di tutte le fasi di ogni singola operazione, idonea a descrivere i profili salienti delle attività specificamente intraprese;
d) i soggetti responsabili delle predette attività, quale che ne sia il livello o le mansioni specifiche, sono tenuti a conservarne tutta la relativa documentazione e a fornirla all'OdV in sede di controlli specifici;
e) l'impiego di risorse economiche e finanziarie è sempre puntualmente autorizzato e contabilizzato, dai soggetti legittimati o preposti, in modo da averne debita evidenza scritta.

f) I Destinatari non devono perseguire finalità di evasione di imposte sui redditi o sul valore aggiunto, o di altre imposte in generale, né nell'interesse o vantaggio della Società né nell'interesse o vantaggio di terzi.
g) I Destinatari, nelle dichiarazioni relative a dette imposte, e nella loro predisposizione, non devono introdurre elementi passivi fittizi avvalendosi di fatture o altri documenti per operazioni inesistenti. A tale riguardo:
h) Gli uffici aziendali devono controllare che le fatture e i documenti contabili si riferiscano a prestazioni effettivamente svolte da parte dell'emittente delle fatture/documenti ed effettivamente ricevute dalla Società;
i) Gli uffici aziendali non devono registrare nelle scritture contabili obbligatorie, né detenere a fini di prova nei confronti dell'amministrazione finanziaria, fatture o altri documenti per operazioni inesistenti;
j) Gli uffici aziendali devono verificare la regolare applicazione dell'imposta sul valore aggiunto.
k) I Destinatari devono astenersi *(i)* dal compiere operazioni simulate oggettivamente o soggettivamente nonché *(ii)* dall'avvalersi di documenti falsi o di altri mezzi fraudolenti idonei a ostacolare l'accertamento e a indurre in errore l'amministrazione finanziaria.
l) I Destinatari devono astenersi dall'indicare in dichiarazioni relative alle imposte sui redditi o sul valore aggiunto: *(i)* elementi attivi per un ammontare inferiore a quello effettivo o *(ii)* elementi passivi fittizi o *(iii)* crediti e ritenute fittizi.
m) I Destinatari devono astenersi dall'emettere o rilasciare fatture o altri documenti per operazioni inesistenti al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto.
n) I Destinatari devono astenersi dall'occultare o distruggere in tutto o in parte le scritture contabili, o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari, con il fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi.
o) I Destinatari devono astenersi dall'alienare simulatamente o dal compiere altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva da parte dell'amministrazione finanziaria, con il fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte.
p) I Destinatari devono altresì astenersi dall'indicare nella documentazione presentata ai fini della procedura di transazione fiscale *(i)* elementi attivi per un ammontare inferiore a quello effettivo o *(ii)* elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila, con il fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori.

In generale, è assolutamente vietato ai Destinatari del presente Modello:

- porre in essere, concorrere in o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente, integrino, direttamente o indirettamente, anche solo in astratto o in via potenziale, i reati previsti dalla presente Parte Speciale;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi di reato, possano esserne il presupposto (ad esempio, mancato controllo) o possano potenzialmente diventare fattispecie di reato;
- porre in essere comportamenti non conformi alle Procedure per il presidio del rischio fiscale o, comunque, non in linea con i principi e le disposizioni contenute nel Modello e nel Codice Etico.

Ricorso a servizi consulenziali di terzi

La predisposizione e l'invio delle dichiarazioni dei redditi e Iva sono affidate a terzi esterni alla Società. I terzi stessi dovranno essere vincolati contrattualmente a rispettare gli obblighi e i divieti di cui al paragrafo che precede.

In particolare, all'interno di detti contratti deve essere contenuta apposita dichiarazione delle controparti:

a) di essere a conoscenza della normativa di cui al D.lgs. 231/2001 e delle sue implicazioni per la Società;
b) di impegnarsi a rispettare detta normativa e farla rispettare dai propri dipendenti e collaboratori;
c) di non essere mai stati condannati (o avere richiesto il patteggiamento) e di non essere al momento imputati o indagati in procedimenti penali relativi ai Reati Presupposto; nel caso di esistenza di condanna o di procedimento in corso, e sempre che l'accordo sia ritenuto indispensabile e da preferirsi a un contratto con altri soggetti, dovranno essere adottate particolari cautele;
d) di impegno a rispettare il Modello (ed in particolare le prescrizioni della presente Parte Speciale) e il Codice Etico della Società, ovvero, nel caso di enti, di avere adottato un proprio analogo Modello e un Codice Etico che regolamentano la prevenzione dei reati contemplati nel Modello e nel Codice Etico della Società;
e) di impegnarsi in ogni caso ad astenersi dal compiere attività che possano configurare alcuno dei Reati Presupposto o che comunque si pongano in contrasto con la normativa e/o con il Modello;
f) di adeguare il servizio a eventuali richieste della Società fondate sulla necessità di ottemperare alla prevenzione dei Reati Presupposto di cui trattasi.
g) Inoltre, nei contratti con i consulenti e con i prestatori di servizi deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte dei prestatori delle norme di cui al D.lgs. 231/2001 (quali ad es. clausole risolutive espresse, penali).

7.3.3. Presidi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Prevenire la commissione di un reato tributario tra quelli sopra illustrati e di conseguenza redigere uno specifico protocollo ai fini 231 non è un compito semplice in quanto, diversamente da molti altri, i reati tributari sono pervasivi nell'ambito dell'attività di impresa ed è quindi difficile relegarli in ambiti di attività specifici o circoscritti.
Abbiamo tuttavia proceduto ad un preventivo "*risk assesment*", cioè una valutazione preliminare delle attività aziendali, individuando le fasi in cui si sviluppano i processi sopra indicati, ritenuti a maggiore "rischio fiscale".
Tali fasi, per cui sono stati poi concepiti i presidi specifici per il contenimento del rischio oggetto di trattazione sotto, sono riepilogate nella tabella che segue.

FASI AZIENDALI A RISCHIO REATI TRIBUTARI
La gestione delle risorse finanziarie (riferita al ciclo attivo, a quello passivo, a quello dei pagamenti e degli incassi e relativi processi autorizzatori nonchè alla tenuta della contabilità).
Definizione dell'assetto amministrativo-contabile volto a rilevare tempestivamente eventuali crisi di impresa.
Il processo per la gestione degli acquisti (la scelta, la qualificazione dei fornitori e l'esecuzione dei contratti).
La scelta e la qualificazione professionale dei consulenti fiscali e dei ruoli chiave interni, in ambito fiscale.
Il complesso dei processi riconducibili ad attività tributaria: i. Calcolo delle imposte in sede di elaborazione del bilancio di esercizio ii. predisposizione di dichiarazioni e comunicazioni concernenti la materia tributaria; iii. presentazione di dichiarazioni e comunicazioni concernenti la materia tributaria; iv. pagamento di imposte dirette e Iva.
Sponsorizzazioni, spese di rappresentanza.
operazione di riconducibili alla gestione straordinaria

7.3.3.1. IL SISTEMA DI PREVENZIONE DEI REATI TRIBUTARI

Se fino ad oggi aree di attività come quelle menzionate sono state analizzate in quanto fonti di rischio indiretto o "strumentale", in grado di ospitare condotte volte ad occultare o preparare la commissione di reati quali – a titolo esemplificativo – il riciclaggio, la corruzione tra privati o le illecite operazioni sul capitale sociale, con l'entrata in vigore della modifica legislativa le stesse devono invece essere studiate ed affrontate, con riferimento ai reati tributari, come aree a rischio "diretto".

In altre parole, l'intero sistema di procedure e protocolli già delineato nell'ambito di queste attività è stato sottoposto a revisione, al fine di verificarne l'idoneità preventiva con specifico riferimento agli illeciti richiamati dal nuovo art. 25-quinquiesdecies, D.lgs. 231/2001.
La presente Parte Speciale è inerente alle condotte poste in essere da amministratori, dirigenti e Dipendenti (d'ora innanzi, per brevità "**Esponenti Aziendali**") o terzi, tra cui i consulenti fiscali con cui l'Ente intrattiene rapporti di natura contrattuale (d'ora innanzi, per brevità, i "**Collaboratori**") operanti nelle Aree a rischio e a supporto reato (d'ora innanzi per brevità, gli Esponenti Aziendali ed i Collaboratori verranno cumulativamente indicati come i "**Destinatari**").
I Destinatari sono consapevoli che ogni condotta che possa astrattamente configurare gli estremi dei reati di cui alla presente parte speciale è fermamente respinta con ogni mezzo dall'Ente, il cui Codice Etico è fortemente orientato al fine di garantire la massima trasparenza e la tracciabilità delle operazioni e dei flussi finanziari in entrata ed in uscita, relativamente ad operazioni di ogni natura.
Il sistema di prevenzione dei rischi di reati tributari è stato imperniato su norme e principi di comportamento e su misure specifiche.
Rispetto a queste ultima la prima linea di difesa per prevenire questa tipologia di reati è sicuramente l'adozione di un sistema amministrativo – contabile adeguato, che dovrebbe essere affiancato da un sistema gestionale altrettanto efficace. Le "distrazioni" contabili e gestionali, cioè la scarsa attenzione dell'impresa a questi aspetti sono infatti terreno fertile per la commissione dei reati in argomento.

Con riferimento ai reati in esame preme infatti osservare che si tratta di ipotesi astrattamente riconducibili a condotte a rischio di rilevanza trasversale.
Nell'ottica di favorire una più efficace prevenzione, si prevede pertanto l'applicazione **di protocolli operativi di rilevanza trasversale.**
Ad esito dell'analisi dei rischi è emersa la necessità di introdurre tali presidi con particolare riguardo alle fasi (in cui si sviluppano i processi aziendali) maggiormente esposte al rischio di commissione di reati tributari e precisamente:

i. **protocollo per la gestione delle risorse finanziarie** (riferita al ciclo attivo, a quello passivo, a quello dei pagamenti e degli incassi e relativi processi autorizzatori nonchè alla tenuta della contabilità).
ii. **Protocollo per il contenimento del rischio di ricettazione, riciclaggio e autoriciclaggio**.

Al fine di prevenire il rischio "specifico" di commettere reati tributari e quindi il fenomeno della sotto fatturazione o della mancata fatturazione o peggio della emissione o di utilizzo di fatture per operazioni inesistenti, fenomeni che possono costituire il rischio di violazioni fiscali penalmente rilevanti anche sotto il profilo "231", è stato inoltre elaborato un **protocollo specifico per la gestione di attività fiscali.**

È fatto pertanto espresso obbligo ai Destinatari del presente Modello di rispettare misure specifiche per il contenimento del rischio indicate nel "***Protocollo per la gestione dei processi di natura fiscale***" che disciplina specificamente le modalità con cui i processi a rischio devono essere gestiti per evitare

la commissione delle fattispecie criminose e recepisce a tal fine, al proprio interno, i presidi posti del sistema di controllo interno rilevati attraverso la *gap analisys*.

7.4. I CONTROLLI DELL'ORGANISMO DI VIGILANZA

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui all'Art. 25-quinquiesdecies del Decreto, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'Art. 25-quinquiesdecies del Decreto sono i seguenti:

- Svolgere verifiche periodiche sul rispetto della presente Sezione e dei presidi sopra individuati e valutare regolarmente la sua efficacia a prevenire la commissione dei reati di cui all'Art. 25-quinquiesdecies del Decreto; con riferimento a tale punto, l'OdV condurrà controlli a campione sulle attività potenzialmente a rischio, diretti a verificare la corretta applicazione dei presidi specifici sopra individuati.
- Verificare l'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni.
- Proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Sezione.
- Proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Sezione.
- L'Organismo di Vigilanza attiva una serie di scambi di informazioni con i responsabili delle aree a rischio sopra individuate, al fine di attuare efficacemente le proprie attività di vigilanza.
- Esaminare i flussi informativi periodici ed eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute
- Conservare traccia dei flussi informativi periodici ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti

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

7.4.1. Flussi informativi verso l'organismo di vigilanza

Sussiste a carico di tutti i Destinatari del MOG (soggetti apicali, sottoposti, consulenti, etc.) l'**obbligo di segnalazione immediata all'OdV** in caso di notizie rilevanti sulla vita dell'Ente, violazioni del Modello, della presente Parte Speciale o situazioni di riscontrata inadeguatezza e/o non conformità di comportamenti ai principi contenuti nelle procedure/istruzioni aziendali e nel Codice Etico.
Le segnalazioni di illeciti, secondo le istruzioni impartite dall'OdV, dovranno avvenire con le modalità indicate nell'apposita **Procedura "*Flussi Informativi*",** nel rispetto della normativa in tema di *Whistleblowing*.
Con riferimento ai controlli periodici sui processi aziendali e allo svolgimento delle normali attività il D.Lgs. n. 231/01 prevede **flussi informativi con cadenze determinate** verso l'OdV da parte di specifici soggetti. Si rinvia alla **Procedura "*Flussi Informativi*",** allegata al Modello, per la descrizione delle specifiche modalità operative con cui dovranno essere inviati i suddetti flussi.

SEZIONE 8:

REATI TRIBUTARI

(ART. 25-QUINQUIESDECIES)

8. ART. 25-vicies – REATI COMMESSI CON L'USO DI SISTEMI DI INTELLIGENZA ARTIFICIALE

8.1. INTRODUZIONE E FUNZIONE DELLA PARTE SPECIALE IN MATERIA DI REATI COMMESSI CON L'USO DI SISTEMI DI INTELLIGENZA ARTIFICIALE

La presente Parte Speciale si riferisce ai reati commessi con l'uso di sistemi di intelligenza artificiale di cui all'**Art. 25-vicies del D.Lgs. n. 231/2001** e ha come obiettivo che tutti i destinatari del Modello, ossia amministratori, dirigenti e dipendenti aziendali, nonché consulenti, collaboratori e partner, adottino regole di condotta conformi a quanto prescritto dal D.Lgs. n. 231/2001, al fine di prevenire il verificarsi dei reati sopra richiamati.

In particolare, la presente Parte Speciale ha lo scopo di:

- fornire le regole di comportamento e le procedure che gli amministratori, i dirigenti e i dipendenti, nonché i consulenti, i liberi professionisti e i partner aziendali sono tenuti ad osservare ai fini della corretta applicazione del Modello.
- fornire all'Organismo di Vigilanza e ai responsabili delle altre funzioni aziendali che cooperano con il medesimo gli strumenti operativi necessari per l'esercizio delle attività di controllo, monitoraggio e verifica in relazione all'utilizzo dei sistemi di intelligenza artificiale e alla prevenzione dei reati presupposto connessi.

L'inserimento nel D.Lgs. 231/2001 dell'**Art. 25-vicies**, dedicato ai reati commessi con l'uso di sistemi di intelligenza artificiale, è stato disposto dall'**Art. 15 del D.Lgs. 9 settembre 2026, n. 160**, nell'ambito dell'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2024/1689 (**AI Act**). La nuova disposizione individua, quali reati-presupposto della responsabilità amministrativa degli enti, i delitti di cui agli **artt. 437-bis e 612-quater c.p.**.

Il nuovo quadro normativo rafforza il rilievo delle misure tecniche di sicurezza, della sorveglianza umana e della corretta gestione dei sistemi di intelligenza artificiale, con particolare riferimento ai sistemi qualificati come ad alto rischio.

La rilevanza ai fini del D.Lgs. 231/2001 non deriva, pertanto, dall'utilizzo dell'intelligenza artificiale in quanto tale, ma dalla concreta ricorrenza delle condotte e dei presupposti previsti dalle fattispecie penali richiamate dall'Art. 25-vicies.

Ne deriva la necessità di assicurare che l'impiego dei sistemi di intelligenza artificiale nell'ambito dei processi aziendali sia accompagnato da adeguati presidi organizzativi, tecnici e procedurali, in particolare con riferimento alla sicurezza dei sistemi, alla supervisione umana, alla gestione degli accessi e delle modifiche e alla verifica dei contenuti generati o alterati mediante sistemi di intelligenza artificiale.

8.2. CRITERI PER LA DEFINIZIONE DI REATI COMMESSI CON L'USO DI SISTEMI DI INTELLIGENZA ARTIFICIALE

Con il **D.Lgs. n. 160 del 9 settembre 2026**, il legislatore ha introdotto nel D.Lgs. 231/2001 il nuovo **Art. 25-vicies**, ampliando il catalogo dei reati-presupposto mediante il richiamo ai delitti di cui agli **artt. 437-bis e 612-quater c.p.**.

Ai fini della presente Parte Speciale, assumono rilievo le condotte riconducibili all'impiego, alla gestione e alla diffusione di contenuti mediante sistemi di intelligenza artificiale, nei limiti e alle condizioni previste dalle specifiche fattispecie penali richiamate.

In particolare, assumono rilievo:

- l'omessa adozione delle misure tecniche di sicurezza previste per la progettazione, l'addestramento, la produzione e l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, quando ne derivi un pericolo per la vita o l'incolumità pubblica o individuale ovvero per la sicurezza dello Stato.
- l'omessa adozione di misure di sorveglianza umana nei casi previsti dall'**Art. 437-bis c.p.**, compresa la specifica fattispecie relativa all'utilizzatore professionale di sistemi di intelligenza artificiale ad alto rischio.
- l'alterazione di sistemi di intelligenza artificiale ad alto rischio, quando ne derivi un pericolo per la vita o l'incolumità pubblica o individuale ovvero per la sicurezza dello Stato.
- la cessione, pubblicazione o altra diffusione, senza il consenso della persona interessata, di immagini, video o voci falsificati o alterati mediante sistemi di intelligenza artificiale, nei casi e alle condizioni previste dall'**Art. 612-quater c.p.**.

La rilevanza nel Modello ex art. D.Lgs. 231/01 delle suddette condotte discende, pertanto, non dall'utilizzo in sé della tecnologia, ma dalla concreta integrazione delle fattispecie penali richiamate dall'Art. 25-vicies e dalla sussistenza dei relativi presupposti.

8.3. LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS.N.231/2001

Il nuovo **Art. 25-vicies del D.Lgs. 231/2001**, introdotto dall'Art. 15 del D.Lgs n.160 del 9 settembre 2026, ha ampliato il catalogo dei reati presupposto includendo le seguenti fattispecie:

- **Art. 437-bis c.p.** *Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi.*
- **Art. 612-quater c.p.** *Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale.*

8.3.1. Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi (Art. 437-bis c.p. introdotto da D.Lgs n.160 del 9 settembre 2026)

L'**Art. 437-bis c.p.** punisce chi omette di adottare le misure tecniche di sicurezza previste per la progettazione, l'addestramento, la produzione e l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi, ovvero omette di adottare misure di sorveglianza umana, quando da tali omissioni derivi pericolo per la vita o l'incolumità pubblica o individuale.

Qualora dal fatto derivi un pericolo per la sicurezza dello Stato, è prevista la reclusione da due a otto anni.

La norma punisce inoltre, salvo che il fatto costituisca più grave reato, chiunque, al di fuori dei casi indicati dal primo comma, altera sistemi di intelligenza artificiale ad alto rischio, qualora dall'alterazione derivi pericolo per la vita o l'incolumità pubblica o individuale.

Qualora dall'alterazione derivi un pericolo per la sicurezza dello Stato, è prevista la reclusione da tre a dieci anni.

Se taluno dei fatti previsti dal primo comma è commesso per colpa grave, la pena è ridotta da un terzo a un sesto.

È inoltre prevista una specifica fattispecie relativa all'**utilizzatore professionale di sistemi di intelligenza artificiale ad alto rischio** che ometta intenzionalmente di adottare misure di sorveglianza umana, qualora da tale omissione derivi pericolo per la vita o l'incolumità pubblica o individuale ovvero per la sicurezza dello Stato.

Ai fini della presente Parte Speciale assumono pertanto particolare rilievo i presidi relativi alla sicurezza dei sistemi di IA ad alto rischio, alla prevenzione di malfunzionamenti o alterazioni del loro funzionamento, alla gestione delle modifiche e degli accessi e alla predisposizione di adeguate misure di sorveglianza umana.

8.3.2. Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale (Art. 612-quater c.p.)

L'**Art. 612-quater c.p.**, introdotto dall'**Art. 26 della Legge 23 settembre 2025, n. 132**, punisce chi cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità.

La fattispecie è punita con la reclusione da uno a cinque anni.

Il delitto è punibile a querela della persona offesa. Si procede tuttavia d'ufficio se il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate.

Ai fini della presente Parte Speciale assumono pertanto rilievo le attività aziendali che comportino la produzione, gestione, pubblicazione o diffusione di immagini, video o voci generati o alterati mediante sistemi di intelligenza artificiale, con particolare attenzione alle verifiche preventive, alle autorizzazioni alla diffusione e alla tutela dei dati e dell'identità delle persone coinvolte.

8.4. LE ATTIVITÀ SENSIBILI RELATIVE AI REATI COMMESSI CON L'USO DI SISTEMI DI INTELLIGENZA ARTIFICIALE

I reati contemplati dagli **artt. 437-bis e 612-quater c.p.**, richiamati dall'**Art. 25-vicies del D.Lgs. 231/2001**, riguardano rispettivamente l'omessa adozione di misure tecniche di sicurezza e di sorveglianza umana in relazione a sistemi di intelligenza artificiale ad alto rischio, l'alterazione illecita dei medesimi sistemi e la diffusione illecita di immagini, video o voci falsificati o alterati mediante sistemi di intelligenza artificiale.

Le attività sensibili riguardano quindi quei processi aziendali nei quali l'utilizzo o la gestione di sistemi di intelligenza artificiale possa assumere rilevanza ai fini delle fattispecie sopra indicate.

In particolare:

- **Produzione, gestione e diffusione di contenuti audiovisivi mediante sistemi di IA**: attività che comportino la generazione, alterazione, pubblicazione o diffusione di immagini, video o voci mediante sistemi di intelligenza artificiale, con particolare riferimento ai controlli preventivi sull'autorizzazione alla diffusione, sulla provenienza e sulla genuinità dei contenuti.
- **Occupazione: selezione dei candidati (filtro CV), valutazione delle performance e gestione dei dipendenti**. Questi sistemi intervengono nelle fasi iniziali e centrali della ricerca del personale per automatizzare o supportare le decisioni di assunzione, monitorano e analizzano l'operato dei lavoratori già assunti per misurarne la produttività, supportano le decisioni operative quotidiane e le scelte finali sulla carriera del lavoratore.
- **Gestione dei sistemi e degli strumenti di intelligenza artificiale utilizzati dal personale**: attività di selezione, autorizzazione, configurazione e utilizzo degli strumenti di IA messi a disposizione di dipendenti, consulenti e collaboratori nell'ambito dei processi aziendali.
- **Formazione e sensibilizzazione del personale**: attività finalizzate ad assicurare che gli utilizzatori dei sistemi di IA conoscano le regole aziendali, i limiti di utilizzo, gli obblighi di supervisione e le procedure di segnalazione di anomalie, malfunzionamenti o utilizzi non autorizzati.

La corretta gestione di tali attività richiede l'adozione di presidi organizzativi e tecnici idonei a garantire, in relazione ai sistemi e ai processi effettivamente presenti nell'organizzazione, la sicurezza dei sistemi di IA ad alto rischio, la supervisione umana, la tracciabilità degli accessi e delle modifiche, nonché il controllo sulla produzione e diffusione dei contenuti generati o alterati mediante sistemi di intelligenza artificiale.

8.5. ORGANI E FUNZIONI AZIENDALI COINVOLTE

Tutte le funzioni aziendali sono potenzialmente coinvolte nei processi sensibili relativi all'utilizzo e alla gestione dei sistemi di intelligenza artificiale in quanto, direttamente o indirettamente, utilizzano, gestiscono, controllano o supervisionano sistemi di IA nell'ambito dei processi aziendali.

8.6. PRINCIPI E NORME GENERALI DI COMPORTAMENTO

Tutti i Processi Sensibili relativi all'utilizzo e alla gestione dei sistemi di intelligenza artificiale devono essere svolti conformandosi alle leggi vigenti, al Codice Etico aziendale, alle procedure interne applicabili e alle disposizioni contenute nel presente Modello.

In linea generale, l'impiego dei sistemi di intelligenza artificiale da parte dell'ente deve essere improntato ai principi di correttezza, trasparenza, tracciabilità, sicurezza e, nei casi previsti dalla normativa e dalle procedure aziendali, supervisione umana, assicurando che l'utilizzo delle tecnologie avvenga nell'ambito delle responsabilità attribuite alle competenti funzioni aziendali.

Il sistema organizzativo della Società deve assicurare il rispetto dei requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli, con particolare riferimento all'attribuzione delle responsabilità, alla definizione delle linee gerarchiche e delle attività operative, nonché alla gestione dei sistemi di intelligenza artificiale utilizzati nei processi aziendali.

In tale contesto, l'utilizzo dei sistemi di intelligenza artificiale deve avvenire secondo i livelli autorizzativi e le procedure aziendali applicabili, con adeguati presidi di monitoraggio e verifica da parte delle funzioni competenti, al fine di prevenire utilizzi impropri, alterazioni non autorizzate dei sistemi e diffusione illecita di contenuti generati o alterati mediante sistemi di intelligenza artificiale.

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali aziendali e dei Destinatari del Modello (dipendenti, consulenti e partner, nei limiti delle rispettive funzioni) di:

• porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, individualmente o collettivamente, possano integrare le fattispecie di reato previste dall'**Art. 25-vicies del D.Lgs. 231/2001** in materia di sistemi di intelligenza artificiale.

• violare i principi, le regole di comportamento e le procedure aziendali adottate dalla Società, nonché le disposizioni contenute nella presente Parte Speciale.
• utilizzare sistemi di intelligenza artificiale in assenza delle autorizzazioni previste dalle procedure aziendali, ovvero in modo non conforme alle finalità aziendali o alle istruzioni impartite dalle funzioni competenti.

• cedere, pubblicare o altrimenti diffondere, senza il consenso della persona interessata, immagini, video o voci falsificati o alterati mediante sistemi di intelligenza artificiale, nei casi e alle condizioni previste dall'**Art. 612-quater c.p.**.

• utilizzare o diffondere contenuti generati o alterati mediante sistemi di intelligenza artificiale in violazione delle procedure aziendali e dei livelli autorizzativi applicabili.

• utilizzare sistemi di intelligenza artificiale nelle fasi iniziali e centrali della ricerca del personale per automatizzare o supportare le decisioni di assunzione, monitorano e analizzano l'operato dei lavoratori già assunti per misurarne la produttività, supportano le decisioni operative quotidiane e le scelte finali sulla carriera del lavoratore.

La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

• tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge, del Codice Etico e delle procedure aziendali, in tutte le attività che comportino l'utilizzo o la gestione di sistemi di intelligenza artificiale.

• garantire che l'impiego dei sistemi di intelligenza artificiale avvenga nel rispetto dei presidi di sicurezza, dei livelli autorizzativi e, nei casi previsti, dei principi di supervisione e controllo umano.

• assicurare che l'utilizzo dei sistemi di intelligenza artificiale sia coerente con le finalità aziendali e avvenga nel rispetto dei presidi organizzativi definiti dalla Società.

• contribuire al corretto funzionamento del sistema organizzativo, assicurando la tempestiva segnalazione di anomalie, malfunzionamenti, alterazioni non autorizzate o utilizzi impropri dei sistemi di intelligenza artificiale.

• assicurare, nei processi aziendali interessati, la corretta gestione e conservazione delle informazioni e della documentazione relative all'utilizzo dei sistemi di intelligenza artificiale.

8.7. PRESIDI DI PREVENZIONE PER AREE SENSIBILI

Per il dettaglio degli strumenti operativi di contenimento del rischio si rinvia al documento "Elenco protocolli per il contenimento dei rischi 231", approvato dall'organo amministrativo e periodicamente aggiornato, che include le "linee guida per l'utilizzo di sistemi di intelligenza artificiale".

8.8. I CONTROLLI DELL'ORGANISMO DI VIGILANZA

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a

seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui all'Art. 25-vicies del Decreto, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'Art. 25-vicies del Decreto sono i seguenti:

- Svolgere verifiche periodiche sul rispetto della presente Sezione e dei presidi sopra individuati e valutare regolarmente la sua efficacia a prevenire la commissione dei reati di cui all'Art. 25-vicies del Decreto; con riferimento a tale punto, l'OdV condurrà controlli a campione sulle attività potenzialmente a rischio, diretti a verificare la corretta applicazione dei presidi specifici sopra individuati.
- Verificare l'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni.
- Proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Sezione.
- Proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Sezione.
- L'Organismo di Vigilanza attiva una serie di scambi di informazioni con i responsabili delle aree a rischio sopra individuate, al fine di attuare efficacemente le proprie attività di vigilanza.
- Esaminare i flussi informativi periodici ed eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute
- Conservare traccia dei flussi informativi periodici ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti

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

8.8.1. Flussi informativi verso l'organismo di vigilanza

Sussiste a carico di tutti i Destinatari del MOG (soggetti apicali, sottoposti, consulenti, etc.) l'**obbligo di segnalazione immediata all'OdV** in caso di notizie rilevanti sulla vita dell'Ente, violazioni del Modello, della presente Parte Speciale o situazioni di riscontrata inadeguatezza e/o non conformità di comportamenti ai principi contenuti nelle procedure/istruzioni aziendali e nel Codice Etico.
Le segnalazioni di illeciti, secondo le istruzioni impartite dall'OdV, dovranno avvenire con le modalità indicate nell'apposita **Procedura "*Flussi Informativi*",** nel rispetto della normativa in tema di *Whistleblowing*.

Con riferimento ai controlli periodici sui processi aziendali e allo svolgimento delle normali attività il D.Lgs. n. 231/01 prevede **flussi informativi con cadenze determinate** verso l'OdV da parte di specifici soggetti. Si rinvia alla **Procedura "*Flussi Informativi*",** allegata al Modello, per la descrizione delle specifiche modalità operative con cui dovranno essere inviati i suddetti flussi