ansaldo green tech

Modello di Organizzazione Gestione e Controllo ai sensi del Decreto Legislativo 8 giugno 2001, N. 231

Approvato dal Consiglio di Amministrazione di Ansaldo Green Tech S.p.A. in data 13 marzo 2024

INDICE

ALLEGATI

I. Codice Etico.

II. Scheda di evidenza e Dichiarazione periodica.

III. Struttura organizzativa.

IV. Prospetto delle Procure.

V. Framework normativo.

VI. Articoli del sistema sanzionatorio dei contratti stipulati con le Organizzazioni Sindacali per i dipendenti.

VII. Organigramma della sicurezza *ex* D.Lgs. 81/08.

VIII. Documento di Valutazione dei Rischi.

PARTE GENERALE

1. IL DECRETO LEGISLATIVO N. 231/2001 E LA NORMA RILEVANTE

1.1 Il regime di responsabilità previsto a carico delle persone giuridiche

Il Decreto Legislativo 8 giugno 2001, n. 231 (di seguito "Decreto" o "D.Lgs. 231/01") ha introdotto nell'ordinamento italiano un regime di responsabilità, a carico di società ed associazioni con o senza personalità giuridica (di seguito denominate "Enti"), per alcuni reati commessi, nell'interesse o a vantaggio degli stessi, da:

- persone fisiche che rivestono funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro funzione centrale e struttura operativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche, di fatto, la gestione e il controllo degli Enti medesimi;
- persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

La responsabilità della persona giuridica comporta l'applicazione di sanzioni che si aggiungono a quelle penali per la persona fisica che ha materialmente commesso il reato e sono entrambe, per quanto possibile, oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale.

L'Ente non risponde quando ha adottato ed efficacemente attuato un modello di organizzazione e gestione idoneo a prevenire reati della specie di quello verificatosi.

L'elenco dei reati che danno luogo alla responsabilità dell'Ente è tassativamente previsto dalla legge e solo con legge può essere modificato. Alla data di approvazione del presente documento, è costituito dalle seguenti tipologie di condotte illecite richiamate espressamente nel Decreto:

- art. 24 (indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture);
- art. 24-*bis* (delitti informatici e trattamento illecito di dati);
- art. 24-*ter* (delitti di criminalità organizzata);
- art. 25 (peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio);
- art. 25-*bis* (falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento);
- art. 25-*bis*.1 (delitti contro l'industria e il commercio);
- art. 25-*ter* (reati societari);
- art. 25-*quater* (delitti con finalità di terrorismo o di eversione dell'ordine democratico);
- art. 25-*quater*.1 (pratiche di mutilazione degli organi genitali femminili);
- art. 25-*quinquies* (delitti contro la personalità individuale);
- art. 25-*sexies* (abusi di mercato);
- art. 25-*septies* (omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro);
- art. 25-*octies* (ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio);
- art. 25-*octies.1*(strumenti di pagamento diversi dai contanti);

- art. 25-*novies* (delitti in materia di violazione del diritto d'autore);
- art. 25-*decies* (induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria);
- art. 25-*undecies* (reati ambientali) e art. 256-*bis* D.Lgs. 152/2006 (combustione illecita di rifiuti);
- art. 25-*duodecies* (impiego di cittadini di Paesi terzi il cui soggiorno è irregolare);
- art. 25-*terdecies* (razzismo e xenofobia);
- art. 25-*quaterdecies* (frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati);
- art. 25-*quinquiesdecies* (reati tributari);
- art. 25-*sexiesdecies* (contrabbando);
- art. 25-*septiesdecies* (delitti contro il patrimonio culturale);
- art. 25-*duodevicies* (riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici).

1.2 Sanzioni

Le sanzioni previste per gli illeciti amministrativi dipendenti da reato sono:

- sanzioni pecuniarie;
- sanzioni interdittive;
- confisca;
- pubblicazione della sentenza.

In particolare, le sanzioni interdittive di durata non inferiore a tre mesi e non superiore a due anni (fatto salvo quanto indicato successivamente con riferimento alle sanzioni applicabili per i reati previsti dall'art. 25 del Decreto), hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'Ente e sono costituite da:

- l'interdizione dall'esercizio dell'attività;
- il divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- la sospensione o la revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- l'esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive sono applicate nelle ipotesi tassativamente indicate dal Decreto, solo se ricorre almeno una delle seguenti condizioni:

1) l'Ente ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso:
   - da soggetti in posizione apicale; ovvero
   - da soggetti sottoposti all'altrui direzione e vigilanza quando la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
2) in caso di reiterazione degli illeciti.

Il tipo e la durata delle sanzioni interdittive sono stabiliti dal giudice tenendo conto della gravità del fatto, del grado di responsabilità dell'Ente e dell'attività svolta dall'Ente per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. In luogo dell'applicazione della sanzione, il giudice può disporre la prosecuzione dell'attività dell'Ente da parte di un commissario giudiziale.

Le sanzioni interdittive possono essere applicate all'Ente in via cautelare, quando sussistono gravi indizi per ritenere l'esistenza della responsabilità dell'Ente nella commissione del reato e vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa natura di quello per cui si procede (art. 45). Anche in tale ipotesi, in luogo della misura cautelare interdittiva, il giudice può nominare un commissario giudiziale.

L'inosservanza delle sanzioni interdittive costituisce un reato autonomo previsto dal Decreto come fonte di possibile responsabilità dell'Ente (art. 23).

Le sanzioni pecuniarie, applicabili a tutti gli illeciti, sono determinate attraverso un sistema basato su "*quote*" in numero non inferiore a cento e non superiore a mille, e di importo variabile fra un minimo di euro 258,23 ed un massimo di euro 1.549,37. Il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'Ente, nonché dell'attività svolta per eliminare od attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. L'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente, allo scopo di assicurare l'efficacia della sanzione (art. 11).

È sempre disposta la confisca del prezzo o del profitto del reato, che può avere ad oggetto anche beni o altre utilità di valore equivalente, nonché la pubblicazione della sentenza di condanna in presenza di una sanzione interdittiva.

La Legge n. 3 del 2019 ha aumentato significativamente le sanzioni interdittive nei casi di condanna per delitti previsti dall'art. 25 del Decreto, vale a dire delitti di corruzione, concussione, induzione indebita a dare o promettere utilità e istigazione alla corruzione.

Ha poi previsto, con riferimento ai citati delitti, una particolare forma di attenuazione della sanzioni interdittive nel caso in cui, prima della sentenza di primo grado, l'Ente si sia efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione dei responsabili ovvero per il sequestro delle somme o altre utilità trasferite e abbia eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi.

1.3 Delitti tentati

L'Ente risponde anche degli illeciti dipendenti da delitti tentati. Nelle ipotesi di commissione nella forma del tentativo dei delitti indicati nel Capo I del Decreto, le sanzioni pecuniarie e le sanzioni interdittive sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'Ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento. Si tratta di un'ipotesi particolare di c.d. "recesso attivo", previsto dall'art. 56, co. 4, c.p.

1.4 Reati commessi all'estero

In base al disposto dell'art. 4 del Decreto, l'Ente che abbia sede in Italia può essere chiamato a rispondere dei reati commessi all'estero, al fine di non lasciare sfornita di sanzione una condotta criminosa di frequente verificazione, nonché al fine di evitare facili elusioni dell'intero impianto normativo in oggetto.

I presupposti su cui si fonda la responsabilità dell'Ente per reati commessi all'estero sono:

a) il reato deve essere commesso all'estero da un soggetto funzionalmente legato all'Ente, ai sensi dell'art. 5, comma 1, del Decreto;
b) l'Ente deve avere la propria sede principale nel territorio dello Stato italiano;
c) l'Ente può rispondere solo nei casi e alle condizioni previste dagli artt. 7, 8, 9, 10 c.p.

Se sussistono i casi e le condizioni di cui ai predetti articoli del codice penale, l'Ente risponde, purché nei suoi confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

1.5 Procedimento di accertamento dell'illecito e sindacato di idoneità del giudice

La responsabilità per illecito amministrativo derivante da reato viene accertata nell'ambito di un procedimento penale e, per regola, è ispirata a ragioni di effettività, omogeneità ed economia processuale. Il processo nei confronti dell'Ente dovrà rimanere riunito, per quanto possibile, al processo penale instaurato nei confronti dell'autore del reato presupposto della responsabilità dell'Ente.
L'accertamento della responsabilità della società, attribuito al giudice penale, avviene mediante:

- la verifica della sussistenza del reato presupposto per la responsabilità della società;
- l'accertamento in ordine alla sussistenza dell'interesse o vantaggio dell'Ente alla commissione del reato da parte del suo dipendente o apicale;
- il sindacato di idoneità sui modelli organizzativi adottati.

Il sindacato del giudice circa l'astratta idoneità del modello organizzativo a prevenire i reati di cui al Decreto è condotto secondo il criterio della c.d. "prognosi postuma". Il giudizio di idoneità è, cioè, formulato secondo un criterio sostanzialmente *ex ante*, per cui il giudice si colloca, idealmente, nella realtà aziendale nel momento in cui si è verificato l'illecito per saggiare la congruenza del modello adottato.

1.6 Azioni esimenti dalla responsabilità

Gli artt. 6 e 7 del Decreto prevedono forme specifiche di esonero dalla responsabilità dell'Ente per i reati commessi nell'interesse o a vantaggio dell'Ente sia da soggetti apicali sia da dipendenti.

Nel caso di reati commessi da soggetti in posizione apicale, l'art. 6 prevede l'esonero qualora l'Ente stesso dimostri che:

a) l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi;
b) il compito di vigilare sul funzionamento e l'osservanza del modello di organizzazione, gestione e controllo, nonché di proporne l'aggiornamento sia stato affidato ad un Organismo di Vigilanza dell'Ente, dotato di autonomi poteri di iniziativa e controllo;
c) le persone che hanno commesso il reato abbiano agito eludendo fraudolentemente il suddetto modello;
d) non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Per quanto concerne i dipendenti non apicali, l'art. 7 prevede l'esonero nel caso in cui l'Ente abbia adottato ed efficacemente attuato prima della commissione del reato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Il modello di organizzazione, gestione e controllo, deve rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito esiste la possibilità che siano commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello di organizzazione, gestione e controllo.

I modelli di organizzazione, gestione e controllo possono essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria.

2. ADOZIONE DEL MODELLO DA PARTE DI ANSALDO GREEN TECH S.P.A.

2.1 Obiettivi e mission aziendale

Ansaldo Green Tech S.p.A. (di seguito Ansaldo Green Tech, la Società o l'Azienda), Società controllata al 100% da Ansaldo Energia S.p.A (di seguito Ansaldo Energia, Capogruppo o Controllante) è stata costituita il 1 luglio 2021, come spin-off di Ansaldo Energia S.p.A., con focus sul business delle energie rinnovabili.

Ansaldo Green Tech ha per oggetto sociale l'esercizio in Italia e all'estero, sia direttamente che indirettamente, di attività industriali, commerciali, di progettazione, fornitura, montaggio, avviamento e service nel settore degli impianti e dei componenti per la produzione di energia, anche da fonti rinnovabili, per la stabilizzazione delle reti elettriche, per la produzione di idrogeno ed il suo utilizzo in impianti di generazione, nonché in settori affini, oltre alla realizzazione di tutte le opere connesse con le attività di cui sopra.

Ansaldo Green Tech persegue la propria missione nel rispetto rigoroso dell'obiettivo di creazione di valore per i propri azionisti e puntando a rafforzare le competenze nazionali nei diversi settori di business.

2.2 Modello di Governance

La *corporate governance* di Ansaldo Green Tech, basata sul modello tradizionale, è così articolata:

- ASSEMBLEA DEGLI AZIONISTI, competente a deliberare in sede ordinaria e straordinaria sulle materie alla stessa riservate dalla Legge o dallo Statuto;
- CONSIGLIO DI AMMINISTRAZIONE, investito dei più ampi poteri per l'amministrazione della Società, con facoltà di compiere tutti gli atti opportuni per il raggiungimento degli scopi sociali, ad esclusione degli atti riservati – dalla Legge e dallo Statuto – all'Assemblea degli Azionisti;
- COLLEGIO SINDACALE, cui spetta il compito di vigilare sulla:
    - osservanza della legge e dell'atto costitutivo, nonché sul rispetto dei principi di corretta amministrazione;
    - adeguatezza della struttura organizzativa della Società, del sistema di controllo interno e del sistema amministrativo contabile, anche in riferimento

all'affidabilità di quest'ultimo nel rappresentare correttamente i fatti di gestione;

- SOCIETÀ DI REVISIONE, iscritta nell'albo tenuto dal Ministero dell'Economia e delle Finanze, all'uopo incaricata dall'Assemblea degli Azionisti allo svolgimento dell'attività di revisione legale dei conti.

2.3 Assetto organizzativo

La struttura organizzativa di Ansaldo Green Tech è ispirata all'attuazione di una separazione di compiti, ruoli e responsabilità tra le funzioni operative e quelle di controllo.

La Società opera attraverso un Sistema di Gestione Aziendale che soddisfa i requisiti delle norme internazionali ISO 9001:2015 per la Qualità, ISO 14001:2015 per l'Ambiente e ISO 45001:2018 per la salute e sicurezza dei lavoratori.

Il Sistema Organizzativo di Ansaldo Green Tech è definito e sistematicamente aggiornato in specifici documenti aziendali, che si assumono come facenti parte del presente documento. La formalizzazione e diffusione di tali documenti viene assicurata attraverso la pubblicazione sull'intranet aziendale, nonché tramite comunicazione per posta elettronica ai dipendenti.

Costituiscono parte integrante del sistema documentale anche le direttive, policy e procedure di gruppo applicabili ad Ansaldo Green Tech anche ai sensi del contratto di servizi in essere tra la Società e Ansaldo Energia S.p.A. Difatti, tramite tale contratto, la Società ha affidato a Capogruppo lo svolgimento di alcune attività, per cui, nell'ambito delle aree a rischio identificate (si rinvia alle successive Parti Speciali), le attività possono essere realizzate anche da Strutture di Ansaldo Energia S.p.A. che operano per conto di Ansaldo Green Tech e che, in tal senso, sono tenute al rispetto del presente documento.

2.4 Motivazioni di Ansaldo Green Tech S.p.A. nell'adozione del Modello e sue finalità

Ansaldo Green Tech, per assicurare che il comportamento di coloro che operano per conto o nell'interesse della Società sia sempre conforme ai principi di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, secondo quanto è contenuto nel Codice Etico del Gruppo Ansaldo Energia, che qui viene esplicitamente richiamato, ha ritenuto opportuno procedere in data … all'adozione del Modello in linea con le prescrizioni del Decreto e con le indicazioni della giurisprudenza in materia, nonché sulla base delle Linee Guida emanate da Confindustria.

Tale iniziativa è stata assunta nella convinzione che l'adozione di tale Modello, possa costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano nell'interesse o a vantaggio di Ansaldo Green Tech o in collaborazione con la stessa.

In particolare, si considerano Destinatari del presente Modello e, come tali e nell'ambito delle specifiche competenze, tenuti alla sua conoscenza ed osservanza:

- i componenti del Consiglio di Amministrazione (di seguito anche "C.d.A.");
- i componenti del Collegio Sindacale;
- i Dirigenti;
- i dipendenti, ancorché distaccati per lo svolgimento dell'attività.

Sono inoltre tenuti al rispetto delle linee di condotta del presente Modello anche tutti coloro che intrattengono con la Società rapporti di qualsiasi natura (di seguito anche "soci in affari").

Il Modello si propone come finalità quelle di:

- migliorare il sistema di Corporate Governance;
- esprimere il rifiuto della corruzione in tutte le sue forme da parte della Società. Al riguardo, Ansaldo Green Tech non distingue tra funzionari pubblici e persone private, né tra corruzione attiva e passiva;
- predisporre un sistema strutturato ed organico di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività aziendale;
- determinare, in tutti coloro che operano in nome e per conto di Ansaldo Green Tech nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei propri confronti, ma anche nei confronti dell'Azienda;
- richiedere ai Destinatari il rispetto del Modello e l'impegno a soddisfarne i requisiti;
- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o, comunque, nell'interesse di Ansaldo Green Tech, che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni disciplinari/contrattuali fino alla risoluzione del rapporto;
- ribadire che Ansaldo Green Tech non tollera comportamenti illeciti, ovvero non in linea con il Modello, non rilevando in alcun modo la finalità perseguita, ovvero l'erroneo convincimento di agire nell'interesse o a vantaggio della Società, in quanto tali comportamenti sono, comunque, contrari ai principi etici cui Ansaldo Green Tech intende attenersi e, dunque, in contrasto con l'interesse della stessa;
- censurare fattivamente i comportamenti posti in essere in violazione del Modello attraverso la comminazione di sanzioni disciplinari e/o contrattuali.

2.5 Il processo di predisposizione ed aggiornamento del Modello

Ansaldo Green Tech, in considerazione delle esigenze poste dal Decreto, ha avviato un progetto interno finalizzato a garantire la predisposizione del presente Modello.

Conseguentemente, la predisposizione del presente Modello è stata preceduta da una serie di attività, suddivise in differenti fasi, dirette alla costruzione di un sistema di prevenzione e gestione dei rischi, che vengono qui di seguito descritte.

1) **Mappatura delle attività a rischio**. Obiettivo di questa fase è stata l'analisi del contesto aziendale, al fine di mappare le aree di attività della Società e, tra queste, individuare i processi e le attività in cui potessero - in astratto - essere realizzati i reati previsti dal Decreto. L'identificazione delle attività aziendali e dei processi/attività a rischio è stata attuata attraverso l'esame della documentazione aziendale (organigrammi, procure, processi principali, ecc.) e la condivisione con i soggetti-chiave nell'ambito della struttura aziendale. Il risultato di tale attività è stato rappresentato nel riquadro "Profilo di rischio" del documento denominato "Schede *ex* D.Lgs. 231/01: profilo di rischio e presidi esistenti", contenente la mappa delle principali attività aziendali ritenute in via astratta a rischio.

2) **Analisi dei rischi potenziali**. Con riferimento alla mappatura delle attività, sono stati individuati i reati potenzialmente realizzabili nell'ambito dell'attività aziendale, e per ciascun reato sono state identificate le occasioni, le finalità e le modalità di commissione della condotta illecita. Il risultato di tale attività è riepilogato nei riquadri "Profilo di rischio" del documento denominato "Schede *ex* D.Lgs. 231/01: profilo di rischio e presidi esistenti" (Risk Assessment), in cui è rappresentata, per ogni area a rischio reato, l'analisi dei rischi potenziali, con riguardo ad alcune delle possibili modalità attuative dei reati nello specifico contesto aziendale.

3) **"As-is analysis"**. Individuati i rischi potenziali, si è proceduto ad analizzare il sistema di controlli preventivi esistenti nei processi/attività a rischio, al fine di esprimere il successivo giudizio di idoneità dello stesso ai fini della prevenzione dei rischi di reato. In tale fase, si è, pertanto, provveduto alla rilevazione degli attuali presidi di controllo interno esistenti (procedure formali e/o prassi adottate, verificabilità, documentabilità o "tracciabilità" delle operazioni e dei controlli, separazione o segregazione delle funzioni, ecc.) attraverso l'esame delle informazioni e della documentazione fornite dalle Unità aziendali. Il risultato di tali attività è contenuto nei riquadri "Presidi esistenti" del documento denominato "Schede *ex* D.Lgs. 231/01: profilo di rischio e presidi esistenti" (Risk Assessment).

4) **Predisposizione ed aggiornamento del Modello**. In considerazione degli esiti delle fasi sopra descritte, la Società ha provveduto alla predisposizione del Modello.

2.6 Struttura del Documento

Il presente Documento è costituito da una "Parte Generale" e dalle "Parti Speciali A, B, C, D, E, F, G, H, I, L, M, N".

Nella "Parte Generale", dopo un richiamo ai principi del Decreto, nonché alle motivazioni di adozione del Modello da parte della Società, vengono illustrate:

- le componenti essenziali del Modello con particolare riferimento all'Organismo di Vigilanza istituito ai sensi dell'art. 6, lettera b del Decreto;
- la formazione del personale e diffusione del Modello nel contesto aziendale ed *extra*-aziendale;
- il sistema disciplinare e le misure da adottare in caso di mancata osservanza delle prescrizioni dello stesso;
- i principi generali di comportamento per i reati non trattati nelle Parti Speciali.

Le Parti Speciali sono distinte per tipologie di reato e ciascuna di esse riporta, oltre ai reati di riferimento, le aree di attività a rischio ed i principi generali di comportamento e le procedure da seguire.

Inoltre, costituiscono parte integrante del Modello adottato da Ansaldo Green Tech i seguenti documenti riportati in allegato:

- Codice Etico (allegato I).
- Scheda di evidenza e Dichiarazione periodica (allegato II).
- Struttura organizzativa (allegato III).
- Prospetto delle procure (allegato IV).
- Framework normativo (allegato V).
- Articoli del sistema sanzionatorio dei contratti stipulati con le Organizzazioni Sindacali per i dipendenti (allegato VI).
- Organigramma della sicurezza *ex* D.Lgs. 81/08 (allegato VII).
- Documento di Valutazione dei Rischi (allegato VIII).

2.7 Elementi del Modello

Di seguito vengono descritti gli elementi su cui si fonda il Modello di Ansaldo Green Tech.

Sistema Organizzativo. Il Sistema Organizzativo di primo livello della Società (strutture/posizioni organizzative, missioni ed aree di responsabilità) è definito attraverso l'emanazione di documenti organizzativi da parte dell'Amministratore Delegato. Per quanto riguarda i livelli successivi al primo, i documenti organizzativi di riferimento sono approvati dal Responsabile di primo livello competente. Documenti organizzativi sono emanati anche per fornire informazioni/disposizioni per fatti organizzativi specifici o di breve durata e definire l'assegnazione di personale ad unità organizzative temporanee. La formalizzazione e la diffusione dei documenti organizzativi viene assicurata dall'Unità di Ansaldo Energia che si occupa di risorse umane (di seguito anche Unità Human Resources di Ansaldo Energia), la quale provvede periodicamente all'aggiornamento dell'organigramma della Società. Sulla base delle disposizioni organizzative sono definite le missioni e responsabilità di ciascuna Unità Organizzativa. Inoltre, la Società emana e diffonde anche comunicazioni interne/di servizio, le quali hanno ad oggetto aspetti organizzativi ed operativi dell'organizzazione aziendale.
I documenti relativi al sistema organizzativo sono diffusi a tutto il personale aziendale attraverso la pubblicazione sulla intranet aziendale e tramite apposita comunicazione via email a tutto il personale.
La Procedura di Gruppo AE-PR-001 "Ansaldo Energia Group Management System Documents" definisce l'iter di approvazione dei documenti organizzativi (Organisational Announcement, Appointment Notice e Organisational Chart) e delle Direttive, nonché dei documenti di gestione (Manuali, Procedure, Istruzioni e Form sheet).

Sistema Autorizzativo. Il Sistema Autorizzativo della Società è impostato nel rispetto dei seguenti requisiti:

- le deleghe e le procure coniugano il potere alla relativa area di responsabilità;
- ciascuna delega e procura definisce in maniera univoca i poteri del delegato, precisandone i limiti;
- i poteri gestionali assegnati con le deleghe/procure sono coerenti con gli obiettivi aziendali;
- tutti coloro che agiscono in nome e per conto di Ansaldo Green Tech nei confronti di terzi, ed in particolare della Pubblica Amministrazione, devono essere in possesso di specifica delega e/o formale procura a rappresentare la Società.

In particolare, il sistema prevede l'attribuzione di:

- poteri di rappresentanza permanente, attribuibili tramite procure notarili registrate in relazione all'espletamento delle attività connesse alle responsabilità permanenti previste nell'organizzazione aziendale;
- poteri relativi a singoli affari, conferiti con procure notarili o altre forme di delega in relazione al loro contenuto; l'attribuzione di tali poteri avviene con il supporto dell'Unità competente della Capogruppo, nel rispetto delle leggi che definiscono le forme di rappresentanza, in coerenza con le tipologie dei singoli atti da stipulare; per quanto possibile, saranno previsti contenuti/clausole standard nelle procure speciali per categorie di atti predefiniti.

Il procedimento per il conferimento/revoca delle procure permanenti, finalizzato a disciplinare l'identificazione delle Unità Organizzative coinvolte nel processo e l'individuazione dei compiti e responsabilità, si attiva al verificarsi di importanti variazioni dell'assetto organizzativo o dei processi aziendali o di modifiche di fattori esterni quali leggi, normative, ecc. (opportunamente segnalati dagli Enti competenti).
In questi casi il presidio dell'Unità Human Resources di Ansaldo Energia effettua un'analisi per la rilevazione di eventuali esigenze di attribuzione o ampliamento di poteri, della loro limitazione o revoca, sottoponendola all'approvazione dell'Amministratore Delegato.

La Struttura di Ansaldo Energia che si occupa di affari legali e societari assicura il riscontro degli aspetti legali,–concordando eventuali adeguamenti con l'Unità Human Resources di Ansaldo Energia*,* predispone il testo della procura e lo sottopone alle valutazioni dell'Amministratore Delegato di Ansaldo Green Tech. La Struttura di Ansaldo Energia che si occupa di affari legali e societari cura le formalità notarili per il conferimento/revoca della procura, rubrica in ordine progressivo l'atto stipulato e comunica al procuratore l'avvenuto/a conferimento/revoca, le regole e gli eventuali ulteriori limiti nell'esercizio dei poteri stessi, tramite la lettera d'istruzioni. Quindi inoltra copia dell'atto e della lettera di istruzioni all'Unità Human Resources di Ansaldo Energia*.*

Procedure aziendali nelle aree a rischio (o protocolli), intese più in generale come documenti di gestione delle aree a rischio. Le procedure interne sono caratterizzate dai seguenti elementi:

- separazione, per quanto possibile, all'interno di ciascun processo, tra il soggetto che assume la decisione (impulso decisionale), il soggetto che la autorizza, il soggetto che esegue tale decisione ed il soggetto cui è affidato il controllo del processo (c.d. "segregazione delle funzioni");
- traccia scritta di ciascun passaggio rilevante del processo, incluso il controllo (c.d. "tracciabilità");
- adeguato livello di formalizzazione.

Controllo di gestione. Il sistema di controllo di gestione adottato da Ansaldo Green Tech è articolato nelle diverse fasi di elaborazione del budget annuale, di analisi dei consuntivi periodici e di elaborazione delle previsioni a livello di Società. Il sistema garantisce la:

- pluralità di soggetti coinvolti, in termini di congrua segregazione delle funzioni per l'elaborazione e la trasmissione delle informazioni;
- capacità di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità attraverso un adeguato e tempestivo sistema di flussi informativi e di reporting.

Gestione della documentazione. Tutta la documentazione, interna ed esterna, di Ansaldo Green Tech deve essere gestita con modalità che disciplinano, a seconda dei casi, l'aggiornamento, la distribuzione, le registrazioni, l'archiviazione e la gestione della sicurezza dei documenti e delle registrazioni.

Flussi finanziari. La gestione di tali flussi è definita sulla base di principi improntati ad una sostanziale segregazione delle funzioni, tale da garantire che tutti gli esborsi siano richiesti, effettuati e controllati da funzioni indipendenti o soggetti per quanto possibile distinti, ai quali, inoltre, non sono assegnate altre responsabilità tali da determinare potenziali conflitti di interesse.
Infine, la gestione della liquidità è ispirata a criteri di conservazione del patrimonio, con connesso divieto di effettuare operazioni finanziarie a rischio, ed eventuale doppia firma per impiego di liquidità per importi superiori a soglie predeterminate.

2.8 Modifiche ed integrazioni del Modello

In ragione del fatto che il presente Modello è un atto di emanazione dell'organo amministrativo (in conformità alle prescrizioni dell'art. 6, comma 1, lettera a del Decreto), la sua adozione, così come le successive modifiche ed integrazioni, sono rimesse alla competenza del Consiglio di Amministrazione di Ansaldo Green Tech. Tuttavia, modifiche od integrazioni non sostanziali (comprese quelle relative all'introduzione ed eliminazione di

una procedura) da apportare al presente Modello vengono direttamente recepite nello stesso, a cura dell'Organismo di Vigilanza. Tali modifiche verranno, quindi, comunicate al Consiglio di Amministrazione.

3. ORGANISMO DI VIGILANZA

3.1 Identificazione dell'Organismo di Vigilanza

L'Organismo di Vigilanza istituito ai sensi dell'art. 6, lettera b del Decreto, è un organismo monosoggettivo (l'"Organismo" o "O.d.V.").

Tale Organismo potrà avvalersi, nello svolgimento dei propri compiti, delle Strutture Corporate and Legal Affairs and Risk Management ed Internal Auditing della Controllante, di altre Strutture di Ansaldo Energia e/o di Ansaldo Green Tech e/o di consulenti esterni che, di volta in volta, saranno ritenuti utili allo svolgimento delle attività indicate.

L'O.d.V. è dotato di un apposito Regolamento volto a disciplinare, in particolare, le regole di convocazione e funzionamento, i rapporti con le Funzioni aziendali e quelle della Capogruppo ed i soggetti terzi, le modalità e tempistiche di programmazione delle attività, le procedure di segnalazione, nonché il trattamento dei relativi dati.

L'O.d.V. di Ansaldo Green Tech è dotato, ai sensi dell'art. 6 del Decreto, di "autonomi poteri di iniziativa e controllo" e, pertanto, gli sono garantite la necessaria autonomia ed indipendenza.

In particolare:

- l'**autonomia ed indipendenza** delle quali l'Organismo deve necessariamente disporre, sono assicurate dalla presenza da un organismo monocratico esterno, privo, dunque, di mansioni operative e di interessi che possano confliggere con l'incarico, condizionandone l'autonomia di giudizio e valutazione, nonché dalla circostanza che l'O.d.V. opera in assenza di vincoli gerarchici nel contesto della corporate governance societaria, riportando direttamente al Consiglio di Amministrazione ed al Presidente. Inoltre, le attività poste in essere dall'O.d.V. non possono essere sindacate da alcun altro organismo o struttura aziendale, fatto ovviamente salvo il potere-dovere del Consiglio di Amministrazione di vigilare sull'adeguatezza dell'intervento posto in essere dall'O.d.V.. Inoltre, l'Organismo comunica al Consiglio di Amministrazione il budget occorrente, da impiegare esclusivamente per le spese necessarie all'esercizio delle funzioni che gli sono affidate;
- la **professionalità** è assicurata dalle specifiche competenze in materia dei suoi componenti e dalla facoltà riconosciuta all'Organismo di avvalersi, al fine dello svolgimento del suo incarico e con assoluta autonomia di budget, delle specifiche professionalità sia delle varie Strutture aziendali/della Capogruppo sia di consulenti esterni. Ad ogni modo i componenti esterni sono individuati tra accademici e professionisti di comprovata competenza ed esperienza nelle tematiche giuridiche, finanziarie e di controllo interno e hanno maturato un'adeguata e comprovata esperienza nell'ambito di applicazione del Decreto;
- la **continuità di azione** è garantita dalla circostanza che l'Organismo opera per il tramite del proprio componente interno, stabilmente presso la Società per lo svolgimento dell'incarico assegnatogli.

L'Organismo resta in carica per tre anni; ad eventuali membri esterni può essere rinnovato l'incarico per due sole volte, mantenendo il proprio ruolo fino alla nomina del successore.

L'O.d.V. riferisce direttamente al Presidente ed al Consiglio di Amministrazione di Ansaldo Green Tech ed informa della sua attività il Collegio Sindacale.

La nomina quale membro dell'O.d.V. è condizionata, come detto, alla presenza di determinati requisiti soggettivi, nonché all'assenza di cause di incompatibilità con la nomina stessa e di potenziali conflitti di interesse con il ruolo ed i compiti che andrebbe a svolgere. In tale contesto, costituiscono motivi di ineleggibilità dei membri dell'O.d.V.:

- avere rapporti di coniugio, parentela o di affinità entro il quarto grado con gli Amministratori, con i membri del Collegio Sindacale o con altri membri dell'O.d.V. di Ansaldo Green Tech;
- intrattenere, direttamente o indirettamente, relazioni economiche e/o rapporti contrattuali, a titolo oneroso o gratuito, con Ansaldo Green Tech, con Società controllate e/o con i rispettivi Amministratori, di rilevanza tale da condizionarne l'autonomia di giudizio;
- essere titolare, direttamente o indirettamente, di partecipazioni azionarie in Ansaldo Green Tech o Società controllanti, controllate o collegate tali da permettere di esercitare il controllo o un'influenza notevole sulla Società, ovvero, comunque, da comprometterne l'indipendenza;
- trovarsi nella condizione giuridica di interdetto, inabilitato, fallito o condannato a una pena che importi l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità ad esercitare uffici direttivi;
- essere stato sottoposto a misure di prevenzione disposte dall'autorità giudiziaria, salvi gli effetti della riabilitazione;
- essere sottoposti a procedimenti penali, condannati o soggetti a pena ai sensi degli artt. 444 e ss. c.p.p., salvi gli effetti della riabilitazione, in relazione ad uno dei reati previsti dal D.Lgs. 231/01;
- essere destinatari di un provvedimento di applicazione di una sanzione per uno dei reati di cui agli articoli 185 e 187-*bis* del TUF;
- essere colpiti da cause di ineleggibilità ai sensi degli artt. 2399 lett. c e 2409-*septiesdecies* c.c..

La cessazione dalla carica può essere determinata da rinuncia, decadenza o revoca.

La rinuncia può essere esercitata in qualsiasi momento e deve essere comunicata al Consiglio di Amministrazione e al Collegio Sindacale per iscritto.

La decadenza è prevista:

- qualora vengano meno i requisiti precedentemente riportati, ovvero
- nel caso di grave infermità che lo renda inidoneo a svolgere le proprie funzioni di vigilanza, o un'infermità che, comunque, ne determini l'assenza per un periodo superiore a sei mesi.

In questi casi, il Consiglio di Amministrazione, esperiti gli opportuni accertamenti, sentito l'interessato, stabilisce un termine non inferiore a 30 giorni entro il quale deve cessare la situazione di decadenza. Trascorso tale termine senza che la predetta situazione sia cessata deve dichiarare l'avvenuta decadenza ed assumere le opportune deliberazioni.

Al fine di garantire la necessaria stabilità dell'O.d.V. e di tutelarne il legittimo svolgimento delle funzioni da una rimozione ingiustificata, la revoca dei poteri propri dell'O.d.V. e l'attribuzione di tali poteri ad altro soggetto, potrà avvenire soltanto per giusta causa, mediante un'apposita delibera del Consiglio di Amministrazione e sentito il Collegio Sindacale.

A tale proposito, per "giusta causa" di revoca dei poteri connessi con l'incarico di O.d.V., devono intendersi:

- un grave inadempimento dei propri doveri così come definiti nel presente Modello;

- una sentenza di condanna o di patteggiamento emessa nei confronti di uno dei membri dell'Organismo per aver commesso illeciti previsti dal Decreto;
- un provvedimento di condanna della Società per uno degli illeciti previsti dal Decreto, ove risulti l'"omessa o insufficiente vigilanza" da parte dell'Organismo, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;
- la violazione degli obblighi di riservatezza cui sono tenuti i componenti dell'O.d.V. in ordine alle notizie ed informazioni acquisite nell'esercizio delle loro funzioni, fatti salvi gli obblighi di informazione espressamente previsti dal presente Modello. In particolare, i componenti dell'Organismo devono assicurare la riservatezza delle informazioni di cui vengono in possesso - con particolare riferimento alle segnalazioni che agli stessi dovessero pervenire in ordine a presunte violazioni del Modello – ed astenersi dal ricercare ed utilizzare informazioni riservate, per fini diversi da quelli indicati dall'art. 6 del Decreto. In ogni caso, ogni informazione in possesso dei membri dell'Organismo deve essere trattata in conformità con la legislazione vigente in materia ed, in particolare, in conformità con le norme sulla privacy.

Qualora la revoca venga esercitata, il Consiglio di Amministrazione provvederà senza indugio alla sostituzione dei membri revocati.

Ove sussistano gravi ragioni di convenienza, il Consiglio di Amministrazione, sentito il Collegio Sindacale (qualora non siano tutti coinvolti), potrà disporre la sospensione dalle funzioni dell'O.d.V., provvedendo tempestivamente alla nomina di un nuovo Organismo *ad interim*.

In caso di rinuncia, decadenza o revoca dell'Organismo, il Consiglio di Amministrazione deve provvedere senza indugio alla sua sostituzione.

3.2 Funzioni e poteri dell'Organismo di Vigilanza

La "*mission*" dell'O.d.V. di Ansaldo Green Tech consiste nella vigilanza sull'effettività del Modello, nell'esame dell'adeguatezza del Modello, nell'analisi circa il mantenimento nel tempo dei requisiti di solidità e funzionamento del Modello e nella cura del necessario aggiornamento del Modello, nell'ipotesi in cui le analisi operate rendano necessario effettuare correzione ed adeguamenti.

Più in particolare, è compito dell'O.d.V.:

- effettuare, tramite apposita programmazione degli interventi, una ricognizione delle attività aziendali con l'obiettivo di individuare le aree a rischio di reato ai sensi del D.Lgs. 231/01 e proporne l'aggiornamento e l'integrazione, ove se ne evidenzi la necessità;
- monitorare, sulla base del piano di attività approvato, la validità nel tempo del Modello, promuovendo, anche previa consultazione delle altre Strutture aziendali interessate, tutte le azioni necessarie al fine di assicurarne l'efficacia. Tale compito comprende la formulazione di proposte di adeguamento da inoltrare alle Strutture aziendali/della Capogruppo competenti ed al Presidente e di verificare successivamente l'attuazione e la funzionalità delle soluzioni proposte;
- valutare, sulla base del piano di attività approvato, il mantenimento nel tempo dei requisiti di solidità e funzionalità del Modello, attraverso l'istituzione di un sistema di dichiarazioni periodiche da parte dei Destinatari del Modello con cui si conferma che non sono state poste in essere azioni non in linea con il Modello;
- effettuare, tramite apposita programmazione degli interventi, nonché tramite controlli specifici, la verifica del corretto svolgimento presso le Strutture aziendali/della Capogruppo ritenute a rischio di reato delle attività sociali, in

conformità al Modello adottato, anche coordinando, a tali fini, le competenti Strutture aziendali;

- verificare l'attuazione e l'effettiva funzionalità delle soluzioni proposte, mediante un'attività di *follow-up*;
- effettuare, sulla base del piano di attività approvato, una verifica dei poteri autorizzativi e di firma esistenti, al fine di accertare la loro coerenza con le responsabilità organizzative e gestionali definite e proporre il loro aggiornamento e/o modifica ove necessario;
- proporre, sulla base dei risultati ottenuti, alle Strutture aziendali/ della Capogruppo competenti, l'opportunità di elaborare, d'integrare e modificare procedure operative e di controllo, che regolamentino adeguatamente lo svolgimento delle attività, al fine di implementare un idoneo Modello;
- definire il flusso informativo che consenta all'O.d.V. di essere periodicamente aggiornato dalle Strutture aziendali interessate sulle attività valutate a rischio di reato, nonché stabilire modalità di comunicazione, al fine di acquisire conoscenza delle eventuali violazioni del Modello;
- attuare, in conformità al Modello, un efficace flusso informativo nei confronti degli organi sociali competenti che consenta all'Organismo di riferire agli stessi in merito all'efficacia e all'osservanza del Modello;
- promuovere, di concerto con l'Unità Human Resources di Ansaldo Energia, presso le competenti Strutture aziendali un adeguato processo formativo del personale attraverso idonee iniziative per la diffusione della conoscenza e della comprensione del Modello;
- promuovere e coordinare le iniziative volte ad agevolare la conoscenza del Modello e delle procedure ad esso relative da parte di tutti coloro che operano per conto della Società;
- espletare l'attività di verifica e di approfondimento delle segnalazioni ricevute, predisponendo, nel caso in cui la segnalazione sia fondata, una apposita relazione per il soggetto preposto a valutare se comminare sanzioni.

Per lo svolgimento degli adempimenti sopra elencati, all'Organismo sono attribuiti i poteri qui di seguito indicati:

- accedere ad ogni documento e/o informazione aziendale rilevante per lo svolgimento delle funzioni attribuite all'Organismo ai sensi del Decreto;
- ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di competenza, osservando quanto previsto per l'assegnazione di incarichi di consulenza;
- assicurarsi che i Responsabili delle Unità Organizzative forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste;
- procedere, qualora si renda necessario, all'audizione diretta dei dipendenti, degli amministratori e dei membri del Collegio Sindacale della Società;
- richiedere informazioni al Collegio Sindacale ed ai soci in affari.

Ai fini di un migliore e più efficace espletamento dei compiti e delle funzioni attribuiti, l'Organismo può avvalersi, per lo svolgimento della propria attività operativa, delle risorse allocate presso la controllante Ansaldo Energia, sulla base di un predefinito rapporto contrattuale con la stessa, come previsto dalle linee guida di Confindustria, e di quelle altre Unità Organizzative di Ansaldo Green Tech che, di volta in volta, si potranno rendere utili allo svolgimento delle attività indicate.

Per quanto concerne in particolare le tematiche di tutela della salute e sicurezza sul lavoro, l'O.d.V. può avvalersi di tutte le risorse attivate per la gestione dei relativi aspetti.

3.3 Informativa dell'Organismo di Vigilanza nei confronti degli organi societari

In merito all'attività di reporting, l'O.d.V. di Ansaldo Green Tech provvede ad inviare al Consiglio di Amministrazione:

- un'informativa scritta semestrale che avrà ad oggetto:
  - l'attività complessivamente svolta nel corso del periodo, con particolare riferimento a quella di verifica;
  - le criticità emerse sia in termini di comportamenti o eventi interni alla Società, sia in termini di efficacia del Modello;
  - le segnalazioni ricevute nel corso del semestre e le azioni intraprese dall'O.d.V. stesso e dagli altri soggetti interessati;
  - le attività cui non si è potuto procedere per giustificate ragioni di tempo e/o risorse;
  - lo stato dell'attuazione del Modello in Ansaldo Green Tech, con l'indicazione dei necessari e/o opportuni interventi correttivi e migliorativi dello stesso ed il loro livello di implementazione;
- il piano delle attività per l'anno successivo ed il budget per lo svolgimento della propria attività.

L'Organismo dovrà riferire tempestivamente al Presidente del Consiglio di Amministrazione in merito ad ogni informazione ritenuta utile ai fini dell'assunzione di determinazioni urgenti da parte del Presidente.

3.4 Flussi informativi nei confronti dell'Organismo di Vigilanza

L'art. 6, comma 2, lett d) del Decreto impone la previsione nel modello di organizzazione, gestione e controllo di obblighi informativi nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza del modello stesso.

L'obbligo di un flusso informativo strutturato è concepito quale strumento per garantire l'attività di vigilanza sull'efficacia ed effettività del Modello e per l'eventuale accertamento a posteriori delle cause che hanno reso possibile il verificarsi dei reati previsti dal Decreto, nonché allo scopo di conferire maggiore autorevolezza alle richieste di documentazione che si rendono necessarie all'Organismo nel corso delle sue verifiche.

È possibile contattare l'Organismo di Vigilanza indirizzando la comunicazione a "Organismo di Vigilanza Ansaldo Green Tech S.p.A.", presso Ansaldo Green Tech, Via Nicola Lorenzi, 8 16162 Genova. Al fine di facilitare il flusso di segnalazioni ed informazioni verso l'O.d.V., è stata istituita una casella postale dedicata (odvansaldogreentech.dlgs231-01@agt.ansaldoenergia.com).

L'accesso a tale casella è consentito esclusivamente all'O.d.V. e alla segreteria dell'O.d.V. e qualsiasi violazione è considerata grave e soggetta a sanzione.

3.4.1 SEGNALAZIONI DI WHISTLEBLOWING

Le segnalazioni sono gestite da Ansaldo Green Tech nel rispetto delle prescrizioni normative in materia di Whistleblowing (D.lgs. n. 24/2023 e Direttiva UE 2019/1937) riguardanti la protezione delle persone che effettuano le segnalazioni.

I soggetti di cui all'art. 3 del D.lgs. 24/2023 (lavoratori, collaboratori, liberi professionisti, consulenti, volontari, tirocinanti, azionisti, persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza), che nel proprio contesto lavorativo all'interno di Ansaldo Green Tech sono venuti a conoscenza di condotte illecite rilevanti ai sensi del D.lgs. 231/2001 o violazioni del Modello o violazioni di disposizioni normative nazionali o dell'Unione europea cosi come individuate all'art. 2 comma 1 lett.a) Dlgs 24/23 sono tenuti ad effettuare una segnalazione solamente attraverso il canale istituito presso Ansaldo Green Tech, ovvero attraverso la piattaforma informatica accessibile dall'indirizzo https://www.ansaldoenergia.integrityline.com/ gestita dal Compliance Officer della Capogruppo.

Restano vigenti per ulteriori esigenze di comunicazione i seguenti canali:

- casella postale odvagt.dlgs231-01@aen.ansaldo.it gestita dall'OdV;
- e-mail: reports@ansaldoenergia.com gestita dal Compliance Officer della Capogruppo;
- posta ordinaria indirizzata all'attenzione del Compliance Officer di Gruppo, presso la sede legale di Ansaldo Energia, Via Nicola Lorenzi, 8 16162 Genova, specificando sulla busta "Whistleblowing".

Le segnalazioni possono essere effettuate anche in forma orale tramite:

- piattaforma informatica accessibile dall'indirizzo https://www.ansaldoenergia.integrityline.com/, che consente di lasciare messaggi vocali;
- richiesta di incontro diretto, che sarà fissato entro un termine ragionevole. La richiesta di incontro deve essere inviata al seguente indirizzo e-mail: reports@ansaldoenergia.com.

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

La ricezione delle Segnalazioni è attribuita al Compliance Officer di Ansaldo Energia. Qualora la segnalazione afferisca ambiti riguardanti il Modello o condotte rilevanti ai sensi del D.Lgs. 231/01, la segnalazione è inviata all'OdV di Ansaldo Green Tech, che assicura lo svolgimento delle opportune e necessarie verifiche sui fatti segnalati, garantendo che queste siano svolte nel rispetto della privacy e della riservatezza del segnalato e del segnalante, nel minor tempo possibile e nel rispetto dei principi di obiettività, imparzialità, indipendenza, competenza e diligenza professionale

Ansaldo Green Tech vieta qualsiasi atto di ritorsione o discriminatorio, diretto o indiretto, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla Segnalazione effettuata (ad esempio licenziamento, mobbing, demansionamento, ecc.).

Nel caso in cui, a seguito delle verifiche svolte, sia accertata la fondatezza dei fatti segnalati, l'OdV comunica gli esiti degli approfondimenti svolti alle funzioni aziendali competenti, affinché siano intrapresi i più opportuni provvedimenti sanzionatori, secondo quanto descritto nel paragrafo "Sistema disciplinare e misure in caso di mancata osservanza delle prescrizioni del modello" del presente documento.

Per quanto non espressamente richiamato nel presente paragrafo, si rinvia alla Direttiva di Gruppo "Reporting Management - Whistleblowing".

Tutte le informazioni attinenti alle Segnalazioni sono conservate per un periodo non superiore ai cinque anni.

3.4.2 OBBLIGHI DI INFORMATIVA

Oltre alle segnalazioni di cui al paragrafo precedente, devono essere obbligatoriamente trasmesse all'O.d.V. - altre informazioni con cadenza *ad hoc* o periodica.

3.4.2.1 OBBLIGHI DI INFORMATIVA *AD HOC*

Di seguito si riportano le informazioni che devono essere trasmesse all'O.d.V. al verificarsi dell'evento:

- i provvedimenti e/o notizie provenienti dall'autorità giudiziaria, o da qualsiasi altra autorità dai quali si evinca lo svolgimento di indagini/accertamenti, anche nei confronti di ignoti, per i reati o gli illeciti amministrativi di cui al Decreto; l'invio è a cura della Struttura di Ansaldo Energia che si occupa degli aspetti legali e societari;
- i processi verbali di constatazione ricevuti dall'Agenzia delle Entrate / Guardia di Finanza; l'invio è a cura dell'Unità di Ansaldo Energia che si occupa di amministrazione, finanza e controllo;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti e/o da *ex*-dirigenti e/o *ex*-dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto; l'invio è a cura della Strutture di Ansaldo Energia che si occupano degli aspetti legali e societari o di Human Resources;
- i procedimenti disciplinari svolti e le eventuali sanzioni irrogate, ovvero i provvedimenti di archiviazione di tali procedimenti con le relative motivazioni; l'invio è a cura di chi è chiamato a decidere sull'irrogazione o meno della sanzione nel procedimento disciplinare (a tal proposito si rimanda al capitolo 5);
- le valutazioni che hanno condotto alla scelta della Società di Revisione e le dichiarazioni atte a verificare l'insussistenza di cause di incompatibilità tra la medesima Società di Revisione ed Ansaldo Green Tech; l'invio è a cura delle Strutture di Ansaldo Energia che si occupano rispettivamente degli aspetti legali e societari e di amministrazione, finanza e controllo;
- la comunicazione di qualsiasi altro incarico che si intenda conferire alla stessa Società di Revisione, nel rispetto delle norme vigenti in materia, che sia aggiuntivo rispetto a quello della revisione legale del bilancio; l'invio è a cura della Struttura Ansaldo Energia che si occupa di amministrazione, finanza e controllo;
- report delle operazioni infragruppo che comportino acquisto o cessione di beni o servizi a valori diversi da quelli di mercato, con espressa indicazione delle relative motivazioni; l'invio è a cura della Struttura di Ansaldo Energia che si occupa di amministrazione, finanza e controllo o della Struttura che ha condotto l'operazione;
- ogni eventuale significativa anomalia in ambito D.Lgs. 231/01 riscontrata nell'attività di verifica svolta dalla Struttura Internal Auditing di Ansaldo Energia; l'invio è a cura della Struttura Internal Auditing di Ansaldo Energia;
- documentazione relativa all'attività di informazione e formazione svolta in attuazione del Modello e alla partecipazione alla medesima da parte del personale; l'invio è a cura dell'Unità Human Resources di Ansaldo Energia;
- gli infortuni con prognosi iniziale superiore a 40 giorni da comunicare tempestivamente e gli infortuni con prognosi complessiva superiore ai 40 giorni da

comunicare entro una settimana dal superamento del periodo; l'invio è a cura del responsabile del servizio di prevenzione e protezione.

3.4.2.2 OBBLIGHI DI INFORMATIVA PERIODICA

Di seguito si riportano i flussi informativi che devono essere trasmessi all'Organismo con cadenza annuale:

- articolazione dei poteri e sistema delle deleghe adottato dalla Società, a cura della Struttura di Ansaldo Energia che si occupa degli aspetti legali e societari;
- elenco delle procedure di Ansaldo Green Tech, a cura dell'Unità di Ansaldo Energia che si occupa della gestione del sistema documentale;
- report annuali dei contenziosi:
    - penali;
    - civili e amministrativi in essere di importo superiore a 100 mila euro, a cura della Struttura di Ansaldo Energia che si occupa degli aspetti legali e societari;
    - giuslavoristici in essere di importo superiore a 100 mila euro, a cura dell'Unità Human Resources di Ansaldo Energia;

  in questi report andrà indicato, tra l'altro, il legale incaricato di seguire ciascun contenzioso, nonché eventuali accordi transattivi conclusi;
- report relativo alle assunzioni effettuate, con l'indicazione dell'assenza di conflitti di interesse degli stessi, a cura dell'Unità Human Resources di Ansaldo Energia;
- report relativo alle erogazioni pubbliche ottenute, a cura della Struttura di Ansaldo Energia che si occupa di:
    - risorse umane per i finanziamenti relativi al personale;
    - amministrazione, finanza e controllo per gli altri finanziamenti;
- report in materia di salute e sicurezza sul lavoro, a cura del responsabile del servizio di prevenzione e protezione (RSPP);
- report in materia ambientale, a cura dell'Unità di Ansaldo Energia che si occupa di ambiente;
- report annuale relativo alle sponsorizzazioni effettuate e agli spazi pubblicitari acquisiti, a cura della Struttura di Ansaldo Energia che si occupa di relazioni esterne;
- report annuale riguardante le mostre e fiere a cui si è partecipato nel periodo di riferimento, a cura della Struttura di Ansaldo Energia che si occupa di relazioni esterne;
- report annuale relativo ai contratti in essere con i promotori commerciali, a cura della Struttura di Ansaldo Energia che si occupa di aspetti legali e societari.

3.4.2.3 INDIVIDUAZIONE DEI RESPONSABILI INTERNI, SCHEDE DI EVIDENZA E DICHIARAZIONI PERIODICHE

A completamento dei flussi periodici indicati nel paragrafo 3.4.2.2, sono da considerarsi le Schede di Evidenza e le Dichiarazioni Periodiche.

Il Presidente del Consiglio di Amministrazione, l'Amministratore Delegato, i Responsabili delle Unità Organizzative aziendali direttamente da essi dipendenti e delle Strutture di

Ansaldo Energia coinvolte, divengono Responsabili interni delle operazioni a rischio da loro direttamente svolte o attuate nell'ambito dell'Unità Organizzativa a loro facente capo.

Nell'ambito delle attività a rischio, i rapporti intrattenuti con la Pubblica Amministrazione debbono essere portati a conoscenza dell'O.d.V. dai suddetti Responsabili tramite la compilazione di una Scheda di Evidenza, che dovrà essere inviata su base semestrale (allegato II A).

E', inoltre, previsto l'invio semestrale all'O.d.V. di Dichiarazioni (relative a tutti i reati considerati potenzialmente a rischio dalla Società) da parte dei Responsabili interni circa l'esercizio dei poteri attribuiti in linea con le disposizioni organizzative, le procedure operative ed il disposto del Modello e del Codice Etico (allegato II B).

3.4.3 RACCOLTA, CONSERVAZIONE E ACCESSO ALL'ARCHIVIO DELL'O.D.V.

Ogni informazione, segnalazione, report previsti nel Modello sono conservati dall'O.d.V., presso la Segreteria tecnica dello stesso, in un apposito archivio, il cui accesso è consentito ai componenti dell'Organismo di Vigilanza e alla segreteria dell'O.d.V..

4. FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO NEL CONTESTO AZIENDALE E ALL'ESTERNO

4.1 Comunicazione/formazione al/del personale

Ansaldo Green Tech promuove la conoscenza del Modello, delle relative procedure aziendali e dei loro aggiornamenti tra tutti i dipendenti che sono pertanto tenuti a conoscerne il contenuto, ad osservarli e contribuire alla loro attuazione.

L'Unità Human Resources di Ansaldo Energia, in cooperazione con l'Organismo, gestisce, la comunicazione/formazione al/del personale sui contenuti del D.Lgs. 231/01 e sull'attuazione del Modello attraverso uno specifico piano.

In tale contesto, le azioni comunicative sono relative a:

- inserimento del Modello e del Codice Etico nell'intranet aziendale e nel sito internet della Società;
- distribuzione del Codice Etico a tutto il personale in forza ed ai nuovi assunti al momento dell'assunzione;
- informazione sui corsi relativi ai contenuti del D.Lgs. 231/01, del Modello e del Codice Etico;
- comunicazione sul portale intranet dell'avvenuto aggiornamento del Modello e/o del Codice Etico.

Il percorso di formazione prevede seminari formativi ed informativi in aula, su base regolare ed a intervalli pianificati, al personale direttivo e a quello titolare di procure. Per il resto del personale le modalità di formazione prevedono anche l'utilizzo di modalità "e-learning". La partecipazione alle sessioni di formazione è obbligatoria.

La tracciabilità della partecipazione ai seminari formativi in aula è attuata attraverso la predisposizione di un verbale della sessione formativa nel quale sono evidenziati i partecipanti e gli argomenti trattati. È responsabilità dell'Unità Human Resources di Ansaldo Energia garantire l'archiviazione dei verbali delle sessioni formative.

Eventuali sessioni formative di aggiornamento saranno effettuate in caso di rilevanti modifiche apportate al Modello, al Codice Etico o relative a sopravvenute variazioni normative rilevanti per l'attività della Società, ove l'O.d.V. non ritenga sufficiente, in

ragione della complessità della tematica, la semplice diffusione della modifica con le modalità sopra descritte.

4.2 Informativa e sensibilizzazione dei soci in affari

Ansaldo Green Tech promuove la conoscenza e l'osservanza delle linee di condotta del Modello anche tra i soci in affari della Società.

Ansaldo Green Tech provvede ad inserire nei contratti con terze parti apposite clausole contrattuali che prevedono, in caso di inosservanza dei principi etici stabiliti, opportune sanzioni sino alla risoluzione degli obblighi negoziali.

5. SISTEMA DISCIPLINARE E MISURE IN CASO DI MANCATA OSSERVANZA DELLE PRESCRIZIONI DEL MODELLO

5.1 Principi generali

La predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello è condizione essenziale per assicurare l'effettività del Modello stesso.

Al riguardo, infatti l'articolo 6, comma 2, lettera e) del Decreto prevede che i Modelli di organizzazione e gestione devono *"introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello"*;

Ai fini del presente sistema disciplinare, e nel rispetto delle previsioni di cui alla contrattazione collettiva, laddove applicabili, costituiscono condotte oggetto di sanzione le azioni o i comportamenti posti in essere in violazione del Modello; in particolare la violazione delle procedure è considerata violazione del Modello, per cui deve essere segnalata all'O.d.V. affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

L'applicazione delle sanzioni disciplinari prescinde dall'avvio e/o dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte da Ansaldo Green Tech in piena autonomia ed indipendentemente dalla tipologia di illecito che le violazioni del Modello stesso possano determinare.

L'individuazione delle sanzioni da applicare deve tener conto dei principi di proporzionalità e di adeguatezza rispetto alla violazione contestata. A tale proposito, assumono rilievo le seguenti circostanze:

- tipologia dell'illecito contestato;
- circostanze concrete in cui si è realizzato l'illecito;
- modalità di commissione della condotta;
- gravità della violazione, anche tenendo conto dell'atteggiamento soggettivo dell'agente;
- eventuale commissione di più violazioni nell'ambito della medesima condotta;
- eventuale concorso di più soggetti nella commissione della violazione;
- eventuale recidività dell'autore.

Il sistema disciplinare viene costantemente monitorato dall'O.d.V. e dall'Unità Human Resources di Ansaldo Energia.

5.2 Sanzioni per i lavoratori dipendenti

5.2.1 IMPIEGATI, OPERAI E QUADRI

Le sanzioni irrogabili nei riguardi dei lavoratori dipendenti sono assunte in conformità a quanto previsto dal Codice Disciplinare aziendale e nel rispetto delle procedure previste dall'articolo 7 dello Statuto dei lavoratori ed eventuali norme speciali applicabili.

In particolare, in conformità a quanto previsto dal vigente Contratto Collettivo Nazionale dei Lavoratori Metalmeccanici, anche in relazione al principio di applicazione dei provvedimenti disciplinari secondo la gravità dell'infrazione, si prevede che:

- incorre nei provvedimenti di richiamo verbale, ammonizione scritta, multa o sospensione dal lavoro e dalla retribuzione, secondo la gravità della violazione, il lavoratore che violi le procedure interne previste dal presente Modello (ad es. che non osservi le procedure prescritte, ometta di dare comunicazione all'O.d.V. delle informazioni previste, ometta di svolgere controlli, ecc.), dovendosi ravvisare in tali comportamenti una violazione del contratto che comporta un pregiudizio alla disciplina e morale dell'Azienda;
- incorre nel provvedimento di licenziamento con preavviso, il lavoratore che adotti, nell'espletamento delle attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del presente Modello e diretto in modo univoco al compimento di un reato sanzionato dal Decreto, dovendosi ravvisare in tale comportamento un'insubordinazione rispetto alle prescrizioni imposte dall'Azienda;
- incorre, nel provvedimento di licenziamento senza preavviso il lavoratore che adotti, nell'espletamento delle attività nelle aree a rischio, un comportamento palesemente in violazione delle prescrizioni del presente Modello, tale da determinare il pericolo o la concreta applicazione a carico della Società di misure previste dal Decreto, dovendosi ravvisare nel suddetto comportamento, una condotta tale da provocare all'Azienda "grave nocumento morale e/o materiale", nonché da costituire "delitto a termine di legge".

5.2.2 DIRIGENTI

Le sanzioni applicabili ai dirigenti sono assunte in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti industriali.

In particolare:

- in caso di violazione non grave di una o più regole procedurali o comportamentali previste nel Modello, il dirigente incorre nel richiamo scritto all'osservanza del Modello, la quale costituisce condizione necessaria per il mantenimento del rapporto fiduciario con la Società;
- in caso di grave violazione di una o più prescrizioni del Modello tale da configurare un notevole inadempimento, il dirigente incorre nel provvedimento del licenziamento con preavviso;
- laddove la violazione di una o più prescrizioni del Modello sia di gravità tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione anche provvisoria del rapporto di lavoro, il lavoratore incorre nel provvedimento del licenziamento senza preavviso.

5.3 Misure nei confronti degli Amministratori e dei Sindaci

Nel caso di violazione del Modello da parte degli Amministratori o dei Sindaci di Ansaldo Green Tech, nonché del Consiglio di Amministrazione o del Collegio Sindacale, l'O.d.V. ne informerà il Consiglio di Amministrazione o il Collegio Sindacale, i quali – a seconda delle

rispettive competenze – procederanno ad assumere le iniziative più opportune ed adeguate coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo Statuto.

5.4 Misure nei confronti dei soci in affari

Ogni comportamento posto in essere nell'ambito di un rapporto contrattuale dai soci in affari in contrasto con le linee di condotta indicate dal presente Modello, potrà determinare, grazie all'attivazione di opportune clausole, la risoluzione del rapporto contrattuale.

La Struttura della Capogruppo che si occupa di affari legali e societari, con la collaborazione della Struttura Internal Auditing di Ansaldo Energia, cura l'elaborazione, l'aggiornamento e l'inserimento nelle lettere di incarico o negli accordi negoziali o di partnership di tali specifiche clausole contrattuali.

5.5 Procedimento di applicazione delle sanzioni

Il procedimento di irrogazione delle sanzioni conseguenti alla violazione del Modello si differenzia con riguardo a ciascuna categoria di soggetti Destinatari quanto alla fase:

- della contestazione della violazione all'interessato;
- di determinazione e di successiva irrogazione della sanzione.

Il procedimento di irrogazione ha, in ogni caso, inizio a seguito della ricezione, da parte degli organi aziendali di volta in volta competenti e di seguito indicati, della comunicazione con cui l'O.d.V. segnala l'avvenuta violazione del Modello.

Più precisamente, in tutti i casi in cui riceva una segnalazione - ovvero acquisisca, nel corso delle proprie attività di vigilanza e di verifica, gli elementi idonei a configurare il pericolo di una violazione del Modello -, l'O.d.V. ha l'obbligo di attivarsi al fine di espletare gli accertamenti ed i controlli rientranti nell'ambito della propria attività.

Con riferimento all'attività di approfondimento della segnalazione svolta dall'O.d.V., la Società richiede al personale interessato una fattiva cooperazione nelle indagini.

5.5.1 IL PROCEDIMENTO DISCIPLINARE NEI CONFRONTI DI DIRIGENTI E DIPENDENTI

Nel caso la segnalazione riguardi dirigenti della Società, l'O.d.V., all'esito degli accertamenti e controlli di sua competenza, trasmette al Responsabile dell'Unità Human Resources di Ansaldo Energia una relazione contenente:

- le generalità del soggetto indagato come responsabile della violazione;
- la descrizione della condotta contestata;
- l'indicazione delle previsioni del Modello che risultano essere state violate;
- gli eventuali documenti ed elementi a supporto della contestazione.

Il procedimento di applicazione della sanzione nei confronti di Dirigenti e Dipendenti avviene, a cura della Società, tramite l'Unità Human Resources di Ansaldo Energia, nel rispetto delle norme e dei poteri vigenti.

5.5.2 IL PROCEDIMENTO DISCIPLINARE NEI CONFRONTI DEGLI AMMINISTRATORI E DEI SINDACI

Qualora riscontri la violazione del Modello da parte di un soggetto che rivesta la carica di Amministratore, il quale non sia legato alla Società da rapporto di lavoro subordinato,

l'O.d.V. trasmette al Consiglio di Amministrazione ed al Collegio Sindacale una relazione contenente:

- la descrizione della condotta constatata;
- l'indicazione delle previsioni del Modello che risultano essere state violate;
- le generalità del soggetto indicato come responsabile della violazione;
- gli eventuali documenti comprovanti la violazione e/o gli altri elementi di riscontro.

Entro dieci giorni dall'acquisizione della relazione dell'O.d.V., il Consiglio di Amministrazione convoca il membro indicato dall'O.d.V. per un'adunanza del Consiglio, da tenersi entro e non oltre trenta giorni dalla ricezione della relazione stessa.

La convocazione deve:

- essere effettuata per iscritto;
- comunicare che sono a sua disposizione tutti gli atti e i documenti a base della contestazione, l'avviso della facoltà di formulare eventuali rilievi e/o deduzioni, sia scritte e sia verbali, nonché di farsi assistere da persona di sua fiducia. La convocazione deve essere sottoscritta dal Presidente o da almeno due membri del Consiglio di Amministrazione.

In occasione dell'adunanza del Consiglio di Amministrazione, a cui sono invitati a partecipare anche i membri dell'O.d.V., vengono disposti l'audizione dell'interessato, l'acquisizione delle eventuali deduzioni da quest'ultimo formulate e l'espletamento degli eventuali ulteriori accertamenti ritenuti opportuni.

Il Consiglio di Amministrazione, sulla scorta degli elementi acquisiti, decide se applicare o meno una sanzione, motivando il provvedimento.

Il procedimento sopra descritto trova applicazione anche qualora sia riscontrata la violazione del Modello da parte di un componente del Collegio Sindacale, nei limiti consentiti dalle norme di legge applicabili.

In tutti i casi in cui è riscontrata la violazione del Modello da parte di un Amministratore legato alla Società da un rapporto di lavoro subordinato, sarà instaurato anche il procedimento previsto con riguardo ai Dirigenti/Dipendenti.

Qualora all'esito di tale procedimento sia comminata una sanzione, il Consiglio di Amministrazione convocherà senza indugio l'Assemblea dei Soci per deliberare i provvedimenti conseguenti.

La delibera del Consiglio di Amministrazione e/o quella dell'Assemblea, a seconda dei casi, viene comunicata per iscritto, a cura del Consiglio di Amministrazione, all'interessato nonché all'O.d.V..

5.5.3 IL PROCEDIMENTO NEI CONFRONTI DEI SOCI IN AFFARI

Al fine di consentire l'assunzione delle iniziative previste dalle clausole contrattuali indicate al paragrafo 5.4, l'O.d.V. trasmette al Responsabile della Struttura/della Capogruppo che gestisce il rapporto contrattuale e, per conoscenza al Presidente, una relazione contenente:

- gli estremi del soggetto che indica come responsabile della violazione;
- la descrizione della condotta contestata;
- l'indicazione delle previsioni del Modello che risultano essere state violate;
- gli eventuali documenti ed elementi a supporto della contestazione.

La suddetta relazione, qualora il contratto sia stato deliberato dal Consiglio di Amministrazione o dall'Assemblea dei Soci di Ansaldo Green Tech, dovrà essere trasmessa anche alla loro attenzione e a quella del Collegio Sindacale.

Il Responsabile della Struttura aziendale della Capogruppo che gestisce il rapporto contrattuale, d'intesa con la Struttura di Ansaldo Energia che si occupa di affari legali e e societari e sulla base delle eventuali determinazioni nel frattempo assunte dal Presidente, nonché dal C.d.A. / Assemblea dei Soci e dal Collegio Sindacale nei casi in cui l'incarico sia stato conferito dal C.d.A. / Assemblea dei Soci, assume le opportune iniziative.

6. PRINCIPI GENERALI DI COMPORTAMENTO PER I REATI NON TRATTATI NELLE PARTI SPECIALI

Nel presente paragrafo vengono indicate delle norme generali di comportamento relative alle fattispecie di reato previste dal Decreto per le quali non si è ritenuto necessario predisporre una Parte Speciale, pur ritenendo che i relativi rischi appaiano già bene presidiati dalle regole comportamentali indicati nel Codice Etico, da alcune delle regole previste nelle Parti Speciali del presente Modello e nelle procedure aziendali.

Al fine della prevenzione dei rischi di commissione dei reati con finalità di terrorismo e contro la personalità individuale, la Società:

- si dota di strumenti informatici che impediscano l'accesso e/o la ricezione di materiale non attinente all'attività sociale;
- fissa richiami netti ed inequivocabili ad un corretto utilizzo degli strumenti informatici in possesso dei propri dipendenti;
- dedica particolare attenzione nelle valutazioni di possibili partnership o attività di investimento;
- adempie con diligenza tutti gli accertamenti sui clienti/fornitori:
  - relativi all'accertamento dei soci effettivi della controparte;
  - per quel che riguarda i rapporti con i Clienti, relativi alla verifica del destinatario ultimo della fornitura e all'affidabilità del Cliente sulla base di documenti, dati o informazioni ottenuti da fonti affidabili ed indipendenti.

Inoltre, allo scopo di prevenire la commissione dei reati contro la personalità individuale attraverso il procacciamento illegale della forza lavoro, tramite il traffico di migranti, la tratta degli schiavi ed il caporalato, Ansaldo Green Tech:

- richiede e verifica che i propri fornitori/appaltatori rispettino gli obblighi di legge in tema di:
  - tutela del lavoro minorile e delle donne;
  - condizioni igienico-sanitarie e di sicurezza;
  - diritti sindacali o comunque di associazione e rappresentanza;
  - tutela contro le pratiche di sfruttamento del lavoro;
- prevede adeguate sanzioni contrattuali nei confronti dei fornitori/appaltatori che violino le norme di cui al punto precedente.

Infine, in aggiunta ai principi sopra richiamati, allo scopo di prevenire la commissione del reato di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare, la Società:

- nel caso di assunzione di stranieri, richiede e verifica l'esistenza e la validità del permesso di soggiorno;

- nel caso di fornitori/appaltatori, Partner e/o consulenti/prestatori professionali stranieri e/o personale straniero da loro impiegato, si fa rilasciare apposita dichiarazione di regolarità in materia.

PARTE SPECIALE "A"

Reati contro la Pubblica Amministrazione e delitti di corruzione tra privati e di istigazione alla corruzione tra privati

A.1 PREMESSA

La presente Parte Speciale è dedicata alla trattazione dei reati previsti dagli articoli 24, 25 e 25-ter c. 1 lett. s-bis del Decreto, tra cui quelli di corruzione.

A.2 LA TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE, (ARTT. 24 e 25 del Decreto) I DELITTI DI CORRUZIONE TRA PRIVATI E DI ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI (ART. 25-*TER* COMMA 1 LETTERA S-*BIS* DEL DECRETO)

Si riporta di seguito una breve descrizione dei reati contemplati negli artt. 24 e 25 e nell'art. 25-*ter* lettera s-*bis* del Decreto.

A.2.1 MALVERSAZIONE DI EROGAZIONI PUBBLICHE (ART. 316-*BIS* C.P.)

Il reato punisce il fatto di chi, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato, da altro ente pubblico o dalle Comunità Europee, contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, destinati alla realizzazione di una o più finalità, non li destina alle finalità previste.

Si pensi alla richiesta ed all'ottenimento di un finanziamento pubblico erogato in vista dell'assunzione presso la Società di personale appartenente a categorie privilegiate, ovvero alla ristrutturazione di immobili danneggiati in occasione di calamità naturali che, una volta conseguito, non venga destinato a dette finalità.

A.2.2 INDEBITA PERCEZIONE DI EROGAZIONI PUBBLICHE (ART. 316-*TER* C.P.)

Il reato si configura nei casi in cui chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee.

In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316-*bis* c.p.), non assume alcun rilievo la destinazione dei finanziamenti pubblici erogati, poiché il reato si consuma al momento del loro – indebito – ottenimento.

Va evidenziato che tale reato, avendo natura residuale, si configura solo qualora la condotta non integri gli estremi del più grave delitto di truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* c.p.).

A titolo esemplificativo, si citano, in particolare, le ipotesi di indebito ottenimento di un finanziamento pubblico finalizzato al sostegno delle attività imprenditoriali in determinati settori, mediante l'allegazione di false fatture attestanti prestazioni inesistenti; ovvero mediante la produzione di documentazione attestante la sussistenza dei requisiti per l'ottenimento del finanziamento.

A.2.3 TRUFFA IN DANNO DELLO STATO O DI ENTI PUBBLICI (ART. 640, COMMA 2 N. 1, C.P.)

Il reato si configura qualora, utilizzando artifici o raggiri e in tal modo inducendo taluno in errore, si consegua un ingiusto profitto, in danno dello Stato, di altro ente pubblico o dell'Unione Europea.

Tale reato può realizzarsi quando, ad esempio, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione

informazioni non veritiere (ad esempio supportate da documentazione artefatta), al fine di ottenerne l'aggiudicazione. Si pensi, ancora, alla trasmissione all'amministrazione finanziaria di documentazione contenente false informazioni al fine di ottenere un rimborso fiscale non dovuto; ovvero, più in generale, all'invio ad enti previdenziali, amministrazioni locali o ripartizioni di queste, di comunicazioni contenenti dati falsi in vista di un qualsiasi vantaggio o agevolazione da parte della Società.

A.2.4 TRUFFA AGGRAVATA PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE (ART. 640-*BIS* C.P.)

Il reato si configura qualora la condotta di truffa precedentemente descritta abbia ad oggetto contributi, sovvenzioni, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europea.

Si evidenzia che, in ogni caso, le norme prendono in considerazione tutte le erogazioni caratterizzate da una vantaggiosità rispetto alle condizioni praticate dal mercato.

Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici, finalizzati, ad esempio alla ricerca o a sostenere l'occupazione, o ancora alla realizzazione di progetti di rilevanza pubblica.

A.2.5 FRODE INFORMATICA (ART. 640-*TER* C.P.)

Tale ipotesi di reato si configura nel caso in cui, alterando 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, si ottenga un ingiusto profitto arrecando ad altri danno. L'interferenza può realizzarsi in varie forme: in fase di raccolta ed inserimento dei dati, in fase di elaborazione, in fase di emissione. In tutti questi casi l'intervento avviene sulla memoria di un elaboratore sul cui corretto funzionamento l'autore materiale del reato interferisce in modo da ricavarne un indebito arricchimento in danno dello Stato o di altro ente pubblico.

Ad esempio, integra il reato la modificazione delle informazioni relative alla situazione contabile di un rapporto contrattuale in essere con un ente pubblico, ovvero l'alterazione dei dati fiscali e/o previdenziali contenuti in una banca dati facente capo alla Pubblica Amministrazione.

Per ulteriori approfondimenti su tale reato, si veda anche la Parte Speciale "E".

A.2.6 LA NOZIONE DI PUBBLICO UFFICIALE E INCARICATO DI PUBBLICO SERVIZIO (ARTT. 357-358-322-*BIS* C.P.)

Preliminare all'analisi dei delitti che seguono è la nozione di pubblico ufficiale e incaricato di pubblico servizio, soggetti coinvolti in detti reati.

Si precisa che le norme e la giurisprudenza hanno adottato una definizione molto ampia, partendo dal dato legislativo degli artt. 357, 358, 322 *bis* del Codice Penale.

Sono pubblici ufficiali o incaricati di pubblico servizio coloro che esercitano pubbliche funzioni legislative (ad es. i parlamentari), giudiziarie (i magistrati) o amministrative (sindaci, polizia, vigili urbani, dipendenti INPS ed INAIL, ASL).

Sono in particolare da tenere presente come pubblici ufficiali o incaricati di pubblico servizio quei soggetti che, pur non appartenenti alla Pubblica Amministrazione, esercitano funzioni

pubbliche con poteri autoritativi o certificativi (ad es. funzionari di Banca, concessionari di pubblici servizi, funzionari delle Ferrovie, funzionari SACE, funzionari dell'ENEL o dell'ENI).

Infine, la legge italiana in adempimento di trattati internazionali ha ritenuto di estendere la qualifica di Pubblici Ufficiali ed Incaricati di Pubblico Servizio ai funzionari delle Comunità Europee ed in generale a tutti i soggetti che nell'ambito di Stati esteri o organizzazioni pubbliche internazionali esercitano funzioni corrispondenti a quelle dei pubblici ufficiali italiani.

A.2.7 CONCUSSIONE (ART. 317 C.P.)

Il reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio, abusando della sua qualità o del suo potere, costringa taluno a dare o promettere indebitamente, a sé o ad altri, denaro o altra utilità.

Il reato in esame presenta profili di rischio contenuti ai fini del D.Lgs. 231/01: trattandosi, infatti, di un reato proprio di soggetti qualificati, la responsabilità dell'Ente potrà ravvisarsi solo nei casi in cui un dipendente od un agente della Società, nell'interesse o a vantaggio della stessa, "concorra" nel reato del pubblico ufficiale o dell'incaricato di pubblico servizio, che, approfittando della sua posizione, esiga prestazioni non dovute; ovvero nell'ipotesi in cui l'esponente aziendale svolga concretamente pubblici uffici o pubblici servizi e, in tale veste, favorisca la Società abusando del suo ufficio.

A.2.8 CORRUZIONE (ARTT. 318-319-320 C.P.)

Il reato di corruzione (attiva) si configura quando un soggetto promette (momento consumativo del reato) o dà, anche per interposta persona, ad un pubblico ufficiale o incaricato di pubblico servizio, denaro o altra utilità per esercitare le sue funzioni, omettere o ritardare atti del suo ufficio ovvero per compiere atti contrari ai suoi doveri di ufficio (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia nel caso in cui compia un atto contrario ai suoi doveri (ad esempio: garantire l'illegittima aggiudicazione di una gara).

Il reato si configura altresì nel caso in cui l'indebita offerta o promessa sia formulata con riferimento ad atti – conformi o contrari ai doveri d'ufficio – già compiuti dal pubblico agente.

A norma dell'art. 321 c.p., le pene previste per i pubblici ufficiali e gli incaricati di pubblico servizio si applicano anche ai privati che danno o promettono a quest'ultimi denaro o altra utilità.

A.2.9 CORRUZIONE IN ATTI GIUDIZIARI (ART. 319-*TER* C.P.)

Il reato si configura nel caso in cui taluno offra o prometta ad un pubblico ufficiale denaro o altra utilità al fine di favorire o danneggiare una parte in un processo civile, penale o amministrativo.

Potrà, dunque, essere chiamata a rispondere del reato la Società che, essendo parte in un procedimento giudiziario, corrompa, anche tramite interposta persona (ad esempio, il proprio difensore) un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario, o un testimone) al fine di ottenerne la positiva definizione.

A.2.10 INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ (ART. 319-*QUATER* C.P.)

Il reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induca taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

La norma sanziona non solo il pubblico ufficiale o incaricato di pubblico servizio, ma anche colui che dà o promette denaro o altra utilità.

Tale reato si differenzia da quello di concussione, in quanto il soggetto indotto non è più considerato come vittima, ma come coautore del reato che persegue un risultato illegittimo a lui favorevole.

A.2.11 ISTIGAZIONE ALLA CORRUZIONE (ART. 322 C.P.)

La pena prevista per tale reato si applica a chiunque offra o prometta denaro ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri o per omettere o ritardare un atto del suo ufficio oppure per compiere un atto contrario ai suoi doveri, qualora la promessa o l'offerta non vengano accettate.

A.2.12 CORRUZIONE TRA PRIVATI E ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI (ARTT. 2635 C.C. – 2635-*BIS* C.C.)

Le norme sanzionano gli amministratori, i Sindaci, i dirigenti ed i soggetti che sono sottoposti alla loro direzione e vigilanza, che offrono, promettono, danno o sollecitano/accettano denaro o altra utilità per compiere o omettere un atto contrario al loro ufficio o agli obblighi di fedeltà verso l'azienda, reato punito più gravemente se l'offerta viene accettata, meno gravemente nel caso contrario.

La norma non fa differenza fra corruzione attiva (promettere o dare) e corruzione passiva (sollecitare o accettare la promessa o ricevere). La fattispecie di corruzione passiva non è rilevante ai sensi delle sanzioni del Decreto, perché teoricamente non commessa nell'interesse della Società.

A.2.13 TRAFFICO DI INFLUENZE ILLECITE (ART. 346-*BIS* C.P.)

Commette il delitto di traffico di influenze illecite chi, fuori dei casi di concorso nei reati di corruzione per l'esercizio della funzione, corruzione per atto contrario ai doveri di ufficio o corruzione in atti giudiziari e nei reati di corruzione di cui all'articolo 322-bis, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o con un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'art. 322-bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità , come prezzo della propria mediazione illecita verso il pubblico ufficiale o l'incaricato di un pubblico servizio o l'altro soggetto di cui all'art. 322-bis, ovvero per remunerarlo, in relazione all'esercizio delle sue funzioni o dei suoi poteri, o al compimento di un atto contrario ai doveri di ufficio o all'omissione o al ritardo di un atto del suo ufficio. È punito anche colui che indebitamente dà o promette denaro o altra utilità.

La disposizione pone in essere una forma di tutela anticipata dell'interesse alla legalità, buon andamento e imparzialità della pubblica amministrazione determinando una tutela penale prima che l'accordo corruttivo vada in porto, punendo colui che funge come tramite tra corrotto e corruttore mediante la propria influenza.

Il fondamento giuridico della norma è quello di evitare che gli incarichi pubblici possano sedimentare un tessuto di relazioni con i pubblici ufficiali/incaricati di pubblico servizio su

cui il privato possa fare leva nello svolgimento della sua attività di intermediazione verso la Pubblica Amministrazione, oltre che nella volontà d'impedire l'esercizio di pressioni indebite sui pubblici funzionari ed anche l'illecito arricchimento dell'intermediario.

A.2.14 FRODE NELLE PUBBLICHE FORNITURE (ART. 356 C.P.)

La norma sanziona la frode nell'esecuzione di forniture o nell'adempimento degli altri obblighi contrattuali contratti con lo Stato, o con la Comunità Europea o con un altro ente pubblico ovvero con un'impresa esercente servizi pubblici o di pubblica necessità. La norma offre, in generale, ampie possibilità di impiego in forza dell'interpretazione estensiva seguita dalla giurisprudenza nel valutare come pubbliche o esercenti servizi pubblici anche imprese private.

Per quanto attiene al contenuto della norma il ricorso all'espressione frode sta a significare che non è sufficiente per la sussistenza del reato un semplice inadempimento contrattuale, ma allo stesso tempo non è necessaria la presenza di artifici o raggiri come nella truffa, rispetto alla quale rappresenta un'ipotesi di maggior facilità di impiego.

A.2.15 PECULATO (ART. 314 C.P.)

La fattispecie prevista dal codice penale si riferisce al comportamento del pubblico ufficiale o dell'incaricato di pubblico servizio che ha nella sua disponibilità una *res* di proprietà della pubblica amministrazione, e finisce per comportarsi nell'utilizzo della stessa come se ne fosse il proprietario, disponendo di quella *res* ben al di là di quelle che sono le corrispondenti destinazioni funzionali.

Si tratta quindi di un reato cd "proprio" previsto a carico del soggetto pubblico che può essere imputato al privato a titolo di concorso sulla base della consapevolezza della proprietà pubblica della *res* e della "conoscibilità della qualifica soggettiva del soggetto agente".

Inoltre, si ricorda che il reato rileva ai sensi del D.lgs. 231/01 solo quando il fatto offende gli interessi finanziari dell'Unione europea.

A.2.16 PECULATO MEDIANTE PROFITTO DELL'ERRORE ALTRUI (ART. 316 C.P.)

Il reato si configura nel caso in cui il pubblico ufficiale o l'incaricato di un pubblico servizio, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità.

Anche in questo caso, come per il peculato "semplice", si tratta di reato cd "proprio" previsto a carico del soggetto pubblico che può essere imputato al privato a titolo di concorso sulla base della consapevolezza della proprietà pubblica della *res* e della "conoscibilità della qualifica soggettiva del soggetto agente".

Inoltre, si ricorda che il reato rileva ai sensi del D.lgs. 231/01 solo quando il fatto offende gli interessi finanziari dell'Unione europea.

A.2.17 ABUSO D'UFFICIO (ART. 323 C.P.)

Incorre nel reato di abuso d'ufficio, salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico sevizio che, nello svolgimento delle funzioni o del servizio, in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo

congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto.

Nel delitto in esame possono concorrere anche i privati che siano destinatari dei benefici conseguenti all'atto abusivo, laddove tramite la loro condotta, abbiano avuto un ruolo causalmente rilevante nella realizzazione del reato e sempre che fossero a conoscenza della qualità di pubblico ufficiale/incaricato di pubblico servizio del loro concorrente.

Si ricorda che il reato rileva ai sensi del D.lgs. 231/01 solo quando il fatto offende gli interessi finanziari dell'Unione europea.

A.2.18 TURBATA LIBERTÀ DEGLI INCANTI (ART. 353 C.P.)

Incorre nel reato di turbata libertà degli incanti chiunque, con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche Amministrazioni, ovvero ne allontanagli offerenti.

Il bene giuridico oggetto di tutela è l'interesse della pubblica amministrazione al libero ed ordinario svolgersi dei pubblici incanti e delle licitazioni private nonché la tutela della libera concorrenza.

A.2.19 TURBATA LIBERTÀ DEL PROCEDIMENTO DI SCELTA DEL CONTRAENTE (ART. 353-*BIS* C.P.)

Salvo che il fatto costituisca più grave reato, incorre nel reato di turbata libertà di scelta del contraente chiunque con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, turba il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione.

La norma in esame punisce le condotte prodromiche al compimento di atti in grado di turbare la libertà di scelta del contraente da parte della pubblica amministrazione, turbando il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente.

La presente disposizione rappresenta un'ipotesi di reato di pericolo, che si consuma indipendentemente dall'effettivo conseguimento del risultato, e per il cui perfezionamento, quindi, occorre che sia posta concretamente in pericolo la correttezza della procedura di predisposizione del bando di gara, ma non anche che il contenuto dell'atto di indizione del concorso venga effettivamente modificato in modo da interferire sull'individuazione dell'aggiudicatario.

A.3 AREE A RISCHIO

I reati trattati nel paragrafo A.2 trovano come presupposto l'instaurazione di rapporti, diretti o indiretti, con la Pubblica Amministrazione (intesa in senso lato e tale da comprendere anche la Pubblica Amministrazione di Stati esteri), oltre che con il privato per quanto riguarda i reati di corruzione tra privati e istigazione alla corruzione tra privati.

Tenuto conto, pertanto, della molteplicità dei rapporti che Ansaldo Green Tech intrattiene con le Amministrazioni Pubbliche in Italia ed all'estero e con soggetti privati, sono state individuate le seguenti aree di attività ritenute più specificamente a rischio:

1. Attività di vendita.
2. Approvvigionamenti e appalti.

3. Gestione dei rapporti con istituzioni ed enti pubblici.
4. Gestione del contenzioso.
5. Erogazioni pubbliche.
6. Gestione delle commesse
7. Gestione degli affari societari.
8. Gestione della salute e sicurezza sui luoghi di lavoro.
9. Rapporti con la Società di Revisione ed il Collegio Sindacale.
10. Gestione delle informazioni / operazioni relative a strumenti finanziari quotati e non.
11. Gestione dell'ambiente.
12. Tenuta della contabilità, redazione del bilancio e gestione della fiscalità.
13. Gestione dei contratti di consulenza.
14. Selezione del personale.
15. Sistema di gestione, incentivazione e sviluppo del personale.
16. Gestione dei flussi finanziari.
17. Promotori commerciali.
18. Omaggi, spese di rappresentanza e di ospitalità, organizzazione di eventi e fiere, sponsorizzazioni e pubblicità.
19. Gestione delle partnership.
20. Gestione dei rapporti con parti correlate.
21. Sistemi informativi.

Con riferimento alle suddette aree a rischio reato vengono di seguito elencate in forma sintetica le principali attività che le caratterizzano.

A.3.1 ATTIVITÀ DI VENDITA

Le principali attività a rischio connesse con la gestione del processo di vendita sono:

- monitoraggio del mercato al fine di individuare le opportunità di vendita;
- analisi delle richieste di offerta ricevute/bandi di gara di potenziale interesse;
- effettuazione della scelta (*bid / no bid*);
- elaborazione dell'offerta attraverso il contributo specifico delle Unità interessate e predisposizione della Scheda di Offerta;
- negoziazione con il Cliente degli aspetti tecnico-economici dell'offerta;
- conclusione del contratto con il Cliente;
- contrattualizzazione delle nuove richieste da parte del Cliente emerse durante la realizzazione della commessa;
- gestione delle chiamate di emergenza del Cliente (es. richiesta manutenzione e/o parti di ricambio a seguito di un fermo impianto) e formalizzazione dell'offerta/ordine;
- proposta di attivazione di contratti con promotori commerciali;
- scelta dei promotori commerciali, definizione e sottoscrizione del contratto;

- monitoraggio dell'attività dei promotori commerciali e gestione della rendicontazione dei compensi degli stessi;
- individuazione dei potenziali partners e definizione di accordi con gli stessi.

A.3.2 APPROVVIGIONAMENTI E APPALTI

Le attività individuate dalla Società a potenziale rischio nel processo di approvvigionamento di beni/servizi e di gestione degli appalti sono:

- attivazione del processo di approvvigionamento per il materiale necessario alla realizzazione del prodotto e definizione delle specifiche di fornitura (quantità, tempi, qualità);
- creazione, autorizzazione e rilascio della Richiesta di Acquisto;
- *scouting* sul mercato circa i potenziali fornitori (nazionali ed internazionali) e valutazione dei requisiti richiesti al fine di qualificare i fornitori ritenuti più idonei;
- ricezione delle offerte e valutazione, per quel che riguarda gli aspetti tecnici, con l'Unità Richiedente;
- gestione delle trattative economiche con i fornitori, dopo il benestare sugli aspetti tecnici dell'Unità Richiedente;
- selezione del fornitore e redazione del Modulo di Aggiudicazione;
- formalizzazione del rapporto di fornitura (ordine di acquisto, contratto, convenzioni, contratto quadro, ecc.) ricevendo conferma in originale dai fornitori;
- gestione delle attività di monitoraggio della fornitura e di controllo dei fornitori;
- approvazione da un punto di vista tecnico delle forniture e valutazione della prestazione del fornitore (tipologia, quantità, tempi, ecc.), effettuando i controlli in merito alla qualità dei materiali in ingresso nel cantiere e provvedendo eventualmente all'emissione di un Rapporto di Non Conformità;
- gestione della logistica;
- ricezione/emissione di eventuali claim dei/nei confronti dei fornitori ed individuazione di possibili soluzioni;
- gestione degli acquisti tramite casse cantiere e di sede;
- ricezione delle fatture passive e verifica della corrispondenza con le condizioni previste nell'ordine;
- verifica da parte dell'Unità Organizzativa richiedente dell'effettiva erogazione di servizi professionali;
- autorizzazione al pagamento di fornitori.

A.3.3 GESTIONE DEI RAPPORTI CON ISTITUZIONI ED ENTI PUBBLICI

L'attività svolta dalla Società comporta l'intrattenimento di contatti costanti con la P.A., fra cui si evidenziano a titolo esemplificativo i seguenti:

- monitoraggio del mercato al fine di individuare le opportunità di vendita;
- studio delle opportunità di Partnership;
- richiesta di provvedimenti amministrativi occasionali/*ad hoc* necessari allo svolgimento di attività strumentali a quelle tipiche aziendali e richiesta di

autorizzazioni e licenze (in ambito personale – ad esempio per visite doganali – sicurezza, ambiente, ecc.);

- organizzazione e partecipazione a convegni, mostre e fiere e gestione della pubblicità/sponsorizzazioni;
- gestione dei rapporti con le istituzioni (regione, ecc.);
- gestione dei rapporti di collaborazione con università ed altri centri tecnico-scientifici (ad esempio attivazioni di convenzioni per stage o attività di ricerca);
- gestione delle pratiche di contenzioso;
- gestione dei trattamenti previdenziali e predisposizione delle dichiarazioni funzionali alla liquidazione di tributi;
- gestione delle assunzioni di personale con particolare riferimento a quello appartenente a categorie protette o la cui assunzione è agevolata;
- gestione dei rapporti con il committente pubblico per tutto ciò che concerne l'avanzamento dei lavori;
- gestione delle varianti tecnico/economiche della commessa;
- gestione degli eventuali conflitti/*claim* con il Cliente durante la realizzazione della commessa ed individuazione delle possibili soluzioni;
- consegna del componente/sistema al Cliente;
- gestione degli adempimenti e delle fasi di ispezione per gli aspetti che riguardano la legge sulla Privacy (Regolamento UE 679/2016);
- gestione della fiscalità d'impresa nazionale ed internazionale e delle eventuali ispezioni dell'Autorità competente;
- gestione delle ispezioni dell'INAIL, INPS ed Ispettorato del Lavoro;
- gestione delle attività connesse con l'esecuzione di delibere consiliari ed assembleari che comportano lo svolgimento di adempimenti nei confronti di Pubbliche Amministrazioni;
- richiesta e gestione dei finanziamenti pubblici ad es. per l'attività formativa (Fondo Sociale Europeo; Fondimpresa e Fondirigenti) o per la ricerca;
- gestione delle eventuali visite ispettive connesse con la predisposizione/aggiornamento della documentazione prevista dalla legge (es. documento di analisi dei rischi) ed effettuazione delle relative attività previste in materia di salute e sicurezza sul lavoro (es. visite mediche, adeguata attività di formazione ed informazione dei dipendenti, ecc.) e controllo dell'effettiva applicazione delle relative prescrizioni aziendali;
- gestione di eventuali verifiche in materia di rispetto delle norme ambientali.

A.3.4 GESTIONE DEL CONTENZIOSO

In tale ambito rientrano le attività inerenti i diversi tipi di contenzioso, quali i procedimenti in materia giuslavoristica, amministrativa, tributaria, penale o civile, ivi compresi gli arbitrati rituali. In questa area le principali attività a rischio identificate sono:

- individuazione dei legali esterni cui affidare le pratiche di contenzioso, affidamento e formalizzazione dell'incarico al legale individuato;
- gestione delle pratiche di contenzioso;

- approvazione di transazioni volte alla conclusione del contenzioso;
- valutazione dell'attività del legale e concessione del benestare al pagamento della fattura.

A.3.5 EROGAZIONI PUBBLICHE

Le attività rientranti nell'area a rischio di erogazioni pubbliche identificate dalla Società sono:

- l'individuazione dell'erogazione pubblica per l'attività di ricerca e sviluppo e relativa decisione di richiesta;
- la preparazione della documentazione necessaria per ottenere l'erogazione;
- il monitoraggio dell'istruttoria dell'ente finanziatore e la stipula del contratto;
- la gestione del contratto dell'erogazione ottenuta;
- la valutazione della possibilità di ottenere finanziamenti per l'attività formativa (Fondo Sociale Europeo; Fondimpresa e Fondirigenti);
- l'erogazione dei corsi di formazione;
- la rendicontazione delle spese.

A.3.6 GESTIONE DELLE COMMESSE

Il processo di gestione delle commesse si estrinseca in molteplici attività. Quelle individuate dalla Società come a potenziale rischio sono quelle relative a:

- sviluppo della commessa nella sua parte tecnica, progettando il prodotto, provvedendo alla sua vestizione e predisponendo la documentazione necessaria alla sua realizzazione;
- ricezione/emissione di eventuali *claim* dei / nei confronti dei fornitori ed individuazione di possibili soluzioni;
- gestione del rapporto con il Cliente per tutto ciò che concerne l'avanzamento dei lavori;
- gestione delle varianti tecnico/economiche della commessa;
- gestione di eventuali conflitti/*claim* con il Cliente durante la realizzazione della commessa ed individuazione delle possibili soluzioni;
- elaborazione della documentazione/reportistica contrattuale per il Cliente;
- recepimento o meno delle eventuali richieste di change order espresse dal Cliente in corso d'opera;
- gestione delle richieste di emergenza da parte del Cliente;
- richiesta al Cliente della documentazione necessaria per l'apertura del cantiere ed invio della comunicazione agli enti competenti di avvio lavori;
- pianificazione e realizzazione delle attività di installazione e montaggio / attività di service ed emissione dei documenti di programmazione (es. planning attività, POS);
- gestione della sicurezza di cantiere (sia per quel che riguarda gli accessi al cantiere sia il rispetto delle indicazioni del POS);
- pianificazione ed effettuazione delle attività di prove, controlli e collaudi necessari a completare l'attività certificativa del progetto;

- gestione delle non conformità ed emissione dei relativi rapporti;
- pianificazione e realizzazione delle attività tecniche di avviamento secondo la sequenza e i requisiti prestabiliti;
- esecuzione delle prove e predisposizione della documentazione di accettazione;
- elaborazione del Piano di Avanzamento fisico della commessa ed aggiornamento dello stesso;
- controllo del processo di consuntivazione dei costi e revisione periodica della stima costi/margini a finire;
- consegna della macchina / impianto e/o parti di ricambio al Cliente;
- ottenimento dell'autorizzazione del Cliente all'emissione della fattura;
- attivazione del processo di fatturazione, emissione e registrazione delle fatture attive;
- elaborazione e aggiornamento della reportistica relativa alla fatturazione e agli incassi;
- monitoraggio degli incassi e segnalazione dei mancati incassi;
- recupero delle garanzie connesse alla commessa;
- gestione delle casse cantiere.

A.3.7 GESTIONE DEGLI AFFARI SOCIETARI

Le attività relative alla gestione degli affari societari che presentano un potenziale rischio reato sono:

- predisposizione della documentazione di supporto per la convocazione e le deliberazioni del C.d.A. e dell'Assemblea dei Soci;
- attività connesse con l'esecuzione di delibere consiliari ed assembleari che comportano lo svolgimento di adempimenti nei confronti di Pubbliche Amministrazioni;
- coordinamento delle attività connesse con gli affari societari delle società controllate;
- gestione delle operazioni sul capitale (es. acquisto o sottoscrizione azioni proprie, riduzioni di capitale, ecc.);
- operazioni straordinarie di acquisizioni di Società (ad esempio tramite fusioni e/o scissione di attività).

A.3.8 GESTIONE DELLA SALUTE E SICUREZZA SUI LUOGHI DI LAVORO

La puntuale disciplina delle norme in materia di salute e sicurezza nel lavoro rende necessario un contatto con gli organi di vigilanza sia in occasione della richiesta d'autorizzazioni che in occasione d'ispezioni, sopralluoghi o controlli.

A.3.9 RAPPORTI CON LA SOCIETÀ DI REVISIONE ED IL COLLEGIO SINDACALE

Tra le attività individuate dalla Società come a rischio di commissione dei reati in analisi, rientra la gestione dei rapporti con la Società di Revisione ed il Collegio Sindacale.

A.3.10 GESTIONE DELLE INFORMAZIONI / OPERAZIONI RELATIVE A STRUMENTI FINANZIARI QUOTATI E NON

Le attività individuate dalla Società come a potenziale rischio sono:

- gestione dei rapporti con i media;
- comunicazione di informazioni riservate e price sensitive.

A.3.11 GESTIONE DELLE ATTIVITÀ CONNESSE ALLA TUTELA DELL'AMBIENTE

La puntuale disciplina delle norme in materia di tutela ambientale rende necessario un contatto con gli organi di vigilanza sia in occasione della richiesta d'autorizzazioni che in occasione d'ispezioni, sopralluoghi o controlli.

A.3.12 TENUTA DELLA CONTABILITÀ, REDAZIONE DEL BILANCIO E GESTIONE DELLA FISCALITÀ

Le attività relative alla tenuta della contabilità, redazione del bilancio e gestione della fiscalità che presentano un potenziale rischio reato per la Società sono:

- cura della contabilità generale e predisposizione delle scritture di chiusura (infrannuali ed annuali);
- redazione del progetto di Bilancio (infrannuale ed annuale);
- gestione della fiscalità d'impresa nazionale ed internazionale;
- gestione ed aggiornamento dei libri contabili;
- emissione e registrazione delle fatture attive;
- ricezione delle fatture passive e verifica della corrispondenza con le condizioni previste nell'ordine;
- verifica da parte dell'Unità Organizzativa richiedente dell'effettiva erogazione di servizi professionali;
- autorizzazione al pagamento di fornitori/consulenti;
- effettuazione dei pagamenti e registrazione degli stessi.

A.3.13 GESTIONE DEI CONTRATTI DI CONSULENZA

Le principali attività a potenziale rischio nel processo di assegnazione di contratti di consulenza sono:

- selezione del consulente ed emissione del relativo Ordine di Acquisto;
- gestione dei rapporti con il consulente nell'ambito dello svolgimento delle attività ad esso attribuite;
- valutazione dell'attività del consulente e concessione del benestare al pagamento della sua prestazione;
- individuazione dei legali esterni cui affidare le pratiche di contenzioso, affidamento e formalizzazione dell'incarico;
- valutazione dell'attività del legale e concessione del benestare al pagamento della fattura.

A.3.14 SELEZIONE DEL PERSONALE

Le attività individuate dalla Società come a potenziale rischio nel processo di selezione del personale sono:

- screening dei curricula sulla base delle esperienze e delle competenze maturate;
- effettuazione di un primo colloquio di tipo motivazionale e predisposizione di una valutazione iniziale;
- organizzazione di un secondo colloquio di tipo tecnico con i Responsabili delle Unità richiedenti;
- effettuazione del secondo colloquio di tipo tecnico con le Unità Richiedenti;
- predisposizione di una valutazione conclusiva;
- assunzione della risorsa individuata ed archiviazione della documentazione di selezione (CV con gli allegati delle prove sostenute) e della lettera di assunzione;
- gestione delle assunzioni di personale con particolare riferimento a quello appartenente a categorie protette o la cui assunzione è agevolata o di personale di Paesi terzi;
- gestione dei rapporti con le università per l'attivazione di convenzioni ad esempio per stage;
- gestione dell'anagrafica del personale e dei libri obbligatori per legge (matricola, infortuni).

A.3.15 SISTEMA DI GESTIONE, INCENTIVAZIONE E SVILUPPO DEL PERSONALE

Le attività che la Società ha individuato come a potenziale rischio nel processo di gestione, incentivazione e sviluppo del personale sono:

- definizione dei piani di carriera per il personale e gestione dei passaggi di livello;
- definizione dei sistemi incentivanti (variabili di retribuzioni/premi, provvedimenti "*una tantum*", etc.);
- effettuazione delle valutazioni delle risorse aziendali;
- pagamento di stipendi/salari e bonus/*una tantum* ai dipendenti.

A.3.16 GESTIONE DEI FLUSSI FINANZIARI

Le attività che la Società ha individuato come potenzialmente a rischio nella gestione dei flussi finanziari sono:

- gestione della tesoreria;
- rendicontazione e riconciliazione delle operazioni di finanza/tesoreria;
- strutturazione di prodotti finanziari di copertura per mitigare il rischio di cambio;
- elaborazione e controllo delle paghe/oneri/contributi e delle relative trattenute e produzione di tutta la documentazione obbligatoria per legge (sia verso terzi che verso i dipendenti);
- preparazione delle lettere di bonifico stipendi, versamento oneri, contributi e trattenute fiscali e consegna delle stesse alla tesoreria;
- predisposizione e autorizzazione dei bonifici;

- scelta delle controparti con cui stipulare le fideiussioni/lettere di credito e cura dell'attività di ottenimento delle stesse;
- gestione delle casse cantiere e di sede;
- gestione delle carte di credito aziendali;
- gestione dei rimborsi per le spese di trasferta;
- gestione delle spese di rappresentanza e di ospitalità.

A.3.17 PROMOTORI COMMERCIALI

Le attività che la Società ha individuato come potenzialmente a rischio nella gestione dei promotori commerciali sono:

- proposta di attivazione di contratti con promotori commerciali;
- scelta dei promotori commerciali da attivare, definizione e sottoscrizione del contratto;
- monitoraggio dell'attività dei promotori commerciali e gestione della rendicontazione dei compensi degli stessi.

A.3.18 OMAGGI, SPESE DI RAPPRESENTANZA E DI OSPITALITÀ, ORGANIZZAZIONE DI EVENTI E FIERE, SPONSORIZZAZIONI E PUBBLICITÀ

Le attività per le quali la Società ravvisa in via astratta un potenziale rischio sono:

- organizzazione e partecipazione a convegni, mostre e fiere e gestione della pubblicità e delle sponsorizzazioni aziendali;
- gestione delle spese di rappresentanza e di ospitalità;
- gestione dell'omaggistica aziendale.

A.3.19 GESTIONE DELLE PARTNERSHIP

Le attività a rischio rilevate dalla Società sono le seguenti:

- individuazione dei potenziali partners e definizione degli accordi con gli stessi;
- studio delle opportunità di partnership.

A.3.20 GESTIONE DEI RAPPORTI CON PARTI CORRELATE

Le attività che la Società ha individuato come potenzialmente a rischio sono:

- regolamentazione contrattuale degli accordi infragruppo (di acquisto, di vendita, di distacco di personale, ecc.);
- gestione dei flussi finanziari;
- gestione degli investimenti nell'ambito delle Società controllate;
- realizzazione di operazioni che impattano sul valore di mercato;
- tenuta della contabilità generale e predisposizione delle scritture di chiusura (infrannuali e annuali).

A.3.21 SISTEMI INFORMATIVI

Le attività che presentano potenziali profili di rischio per la Società sono le seguenti:

- gestione della sicurezza dei sistemi: elaborazione di politiche di sicurezza (accesso ai sistemi e ai dati) per garantire la *segregation of duties*; definizione ed applicazione di un processo di gestione degli identificativi (account); monitoraggio delle attività effettuate da Ansaldo Energia attraverso gli Outsourcer in merito alla gestione degli incidenti sulla sicurezza ICT, all'implementazione ed aggiornamento delle tecniche e dei controlli procedurali per proteggere i sistemi, i dati ed il flusso di informazioni attraverso la rete ed alla gestione della sicurezza fisica delle infrastrutture e dei data center;
- gestione delle modifiche: autorizzazione delle modifiche dal punto di vista tecnico e gestione del processo di approvazione dal lato business; verifica della pianificazione e della certificazione delle soluzioni e delle modifiche, attraverso test mirati e con il coinvolgimento degli utenti finali, effettuata da Ansaldo Energia, anche attraverso i suoi fornitori; definizione degli allegati tecnici con la Capogruppo e loro revisione periodica;
- gestione dei *backup / restore*: pianificazione con la Capogruppo, anche attraverso i suoi Outsourcer, delle regole di *backup*, di protezione e di conservazione dei dati, di *restore* di dati / programmi.

A.4 PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITÀ A RISCHIO

A.4.1 PRINCIPI DI COMPORTAMENTO DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

La presente Parte Speciale prevede l'espresso divieto a carico dei destinatari che operano nelle aree di attività a rischio di porre in essere comportamenti:

- tali da integrare le fattispecie di reato sopra considerate (artt. 24, 25 e 25-*ter* comma 1 lettera s-*bis* del Decreto);
- che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- non conformi alle procedure aziendali o, comunque, non in linea con i principi espressi dal presente Modello e del Codice Etico;
- tali da favorire qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione o di un privato in relazione a quanto previsto dalle suddette ipotesi di reato.

Nell'ambito dei suddetti comportamenti è fatto divieto in particolare di:

- effettuare elargizioni a pubblici funzionari o soggetti privati;
- promettere o offrire, anche per interposta persona, denaro, beni o altre utilità a pubblici ufficiali o incaricati di pubblico servizio o soggetti privati, in relazione al compimento di atti d'ufficio;
- distribuire o ricevere omaggi e regali al di fuori di quanto previsto nel Codice Etico e dalla procedura aziendale o comunque per acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale;
- accordare altri vantaggi di qualsiasi natura (promesse di assunzione, utilizzo di beni aziendali, ecc.) in favore di pubblici ufficiali o incaricati di un pubblico servizio o soggetti privati che possano determinare le stesse conseguenze previste al punto precedente;

- effettuare prestazioni in favore dei Partner e/o consulenti che non trovino adeguata giustificazione nel contesto del rapporto associativo/contrattuale costituito con gli stessi;
- riconoscere compensi in favore dei Collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- esercitare indebite pressioni o sollecitazioni su pubblici agenti o soggetti privati in vista del compimento di attività inerenti l'ufficio;
- presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.

Ai fini dell'attuazione dei comportamenti di cui sopra:

- i rapporti nei confronti della PA per le attività a rischio devono essere gestiti nel rispetto delle procedure aziendali ed essere tracciati nelle Schede di evidenza dai Responsabili interni delle aree potenzialmente a rischio reato;
- gli accordi con i promotori commerciali, i Partner e/o altri soggetti terzi sono definiti per iscritto con l'evidenziazione di tutte le condizioni dell'accordo stesso - in particolare per quanto concerne le condizioni economiche concordate - e sono verificati ed approvati in base alle vigenti procedure e nel rispetto dei poteri conferiti;
- i pagamenti per cassa devono essere effettuati sulla base delle procedure aziendali. Nessun tipo di pagamento può esser effettuato in natura;
- le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'O.d.V. eventuali situazioni di irregolarità;
- i rapporti con le eventuali società controllate e partecipate, direttamente o indirettamente, nonché con le collegate devono essere gestiti nel rispetto dei principi di autonomia gestionale, correttezza, trasparenza ed effettività;
- le attività connesse con la gestione degli affari societari sono regolate da apposita procedura operativa, che evidenzia, tra l'altro ruoli e responsabilità dei soggetti coinvolti con particolare riferimento alla gestione dei Consigli di Amministrazione e delle Assemblee;
- eventuali situazioni di incertezza in ordine ai comportamenti da tenere (anche in ragione dell'eventuale condotta illecita o semplicemente scorretta del pubblico agente), all'interpretazione delle norme vigenti e delle procedure interne devono essere sottoposte all'attenzione del superiore gerarchico e/o dell'Organismo di Vigilanza.

Nell'intraprendere e gestire qualsiasi rapporto con la Pubblica Amministrazione e/o con i privati, le singole procedure prevedono che i Destinatari debbano conformarsi ai seguenti principi:

- rispetto dei principi di correttezza e trasparenza e garanzia dell'integrità e della reputazione delle parti;
- osservanza delle leggi, dei regolamenti vigenti, dei principi etici, e delle procedure esistenti;
- tracciabilità e documentazione dei rapporti intrattenuti con pubblici funzionari/privati;
- sottoscrizione di accordi nel rispetto dei poteri conferiti;
- gestione dei rapporti con la Pubblica Amministrazione e con i privati da parte di chi ne ha il potere;
- completo rispetto delle competenze aziendali e del sistema delle deleghe in essere, anche con riferimento ai limiti di spesa relativi alle funzioni ed alle modalità di gestione delle risorse finanziarie;
- corretto utilizzo delle procedure informatiche, tenendo conto delle più avanzate tecnologie acquisite in tale settore;
- tempestiva segnalazione all'Organismo di Vigilanza di ogni situazione anomala.

Con riferimento ai rapporti negoziali:

- in occasione di trattative private con la Pubblica Amministrazione o con i privati, occorre evitare di esercitare ogni tipo di pressione o, comunque, di influenzare indebitamente la scelta della controparte;
- nel caso di partecipazione a gare di qualsiasi tipo indette dalla Pubblica Amministrazione e/o da soggetti privati, è necessario osservare tutte le disposizioni di legge e di regolamento che disciplinano la gara, astenendosi da comportamenti che possano comunque turbare o influenzare indebitamente lo svolgimento della gara;
- nell'esecuzione dei rapporti contrattuali, occorrerà uniformare il proprio comportamento ad assoluta correttezza, adempiendo scrupolosamente agli obblighi assunti. Eventuali criticità o difficoltà di qualsiasi genere nell'esecuzione, ivi inclusi eventuali inadempimenti o adempimenti parziali di obbligazioni contrattuali, dovranno essere evidenziati in forma scritta e gestiti dalle funzioni competenti in conformità agli accordi contrattuali, nonché nel rispetto della legge e delle altre norme vigenti in materia.

Con riferimento alla gestione dei rapporti con le autorità giudiziarie, amministrative, finanziarie e di vigilanza, ai fini della gestione del contenzioso, nonché delle richieste e della gestione di autorizzazioni, licenze e concessioni amministrative:

- la gestione dei rapporti in esame dovrà avvenire nel rispetto delle procedure aziendali, esclusivamente ad opera delle Strutture competenti;
- la scelta di legali e consulenti dovrà avvenire sulla base di criteri di serietà e competenza del professionista;
- il legale ed il consulente dovranno prendere visione delle linee di condotta del Modello della Società ed accettare di uniformarsi alle stesse;
- l'attività prestata dai consulenti e dai legali deve essere debitamente documentata e l'Ente che si è avvalso della loro opera deve, prima della liquidazione dei relativi onorari, attestare l'effettività della prestazione;
- la corresponsione dei compensi ai consulenti ed ai legali esterni deve avvenire sulla base di una descrizione delle attività svolte, che permetta di valutare la conformità dell'onorario al valore della prestazione resa;

- le procedure relative al rilascio ed alla gestione di licenze, autorizzazioni o concessioni, nonché i rapporti con le autorità e con i pubblici funzionari che svolgono funzioni giudiziarie, ispettive o di vigilanza, o funzioni comunque connesse al contenzioso amministrativo o giudiziario, devono essere curate esclusivamente dalle funzioni competenti e devono essere improntate alla massima trasparenza, correttezza e collaborazione, nel rispetto delle leggi e delle altre norme vigenti in materia. In particolare, occorre evitare di esercitare ogni tipo di pressione o comunque di influenzare indebitamente le determinazioni di detti organi;
- le attività aziendali devono essere svolte nel rispetto dei limiti della concessione, dell'autorizzazione o della licenza ottenute. Eventuali criticità o difficoltà di qualsiasi genere, dovranno essere evidenziate in forma scritta e gestite dalle Strutture competenti nel rispetto della legge e delle altre norme vigenti in materia e delle procedure aziendali.

Si evidenzia inoltre che:

- ogni atto della Società deve essere previamente autorizzato dagli uffici competenti garantendo la sua rispondenza all'interesse della Società, la congruità del costo, l'effettiva e completa destinazione delle somme erogate ed il pieno rispetto delle procedure aziendali;
- i rapporti con le parti correlate debbono essere improntati a correttezza e trasparenza, nel rispetto del principio di autonomia delle società controllate e dei principi di corretta gestione, trasparenza contabile, separatezza patrimoniale, in modo da garantire la tutela degli stakeholders di tutte le società correlate;
- la selezione del personale deve avvenire nel rispetto della procedura aziendale e garantire che la valutazione dei candidati sia curata da differenti Unità Organizzative e avvenga nel rispetto dei seguenti principi:
  - effettiva esigenza di nuove risorse;
  - acquisizione del curriculum del candidato e svolgimento di colloqui attitudinali, nel corso dei quali deve essere richiesta al candidato la sottoscrizione di una lettera di assenza di conflitti di interesse;
  - valutazione comparativa sulla base dei criteri di professionalità, preparazione e attitudine in relazione alle mansioni per le quali avviene l'assunzione.
- la scelta del socio in affari dovrà avvenire sulla base di criteri di serietà e competenza del professionista/della Società e nel rispetto delle procedure aziendali;
- il fornitore/consulente/promotore commerciale dovrà prendere visione del Modello della Società ed accettare di uniformarsi ai principi in esso contenuti;
- l'attività prestata dal fornitore/consulente/promotore commerciale deve essere debitamente documentata e l'Ente che si è avvalso della loro opera deve, prima della liquidazione dei relativi onorari, attestare l'effettività della prestazione;
- i flussi finanziari in uscita devono essere autorizzati in base alle procure della Società e gestiti in base alle procedure aziendali. Più in generale, la Società ha impostato l'insieme dei controlli sui flussi finanziari, indicati nelle procedure della Società, sui seguenti principi:
  - tracciabilità dei flussi finanziari, da intendersi come possibilità di ricostruire *ex* post con esattezza il percorso decisionale e formale del flusso relativo al pagamento / incasso;
  - attuazione di una separazione dei compiti, in modo che un pagamento non possa essere avviato ed approvato dalla stessa persona;

- approvazione, da parte di una risorsa aziendale a ciò addetta, dell'attività svolta dal beneficiario, preventiva all'effettuazione del pagamento;
- presenza di adeguata documentazione di supporto alle approvazioni di pagamento;
- restrizione dell'uso del contante ed attuazione di metodi efficaci di controllo dello stesso;
- classificazioni e descrizioni dei pagamenti nei conti accurate e chiare;
- attuazione di un riesame gestionale periodico delle transazioni finanziarie più significative;
- revisione periodica dei bilanci e delle transazioni sottostanti da parte di una Società di Revisione ed avvicendamento, a cadenze regolari, della persona responsabile della revisione e dell'organizzazione che esegue tale attività;
- individuazione delle Funzioni tenute ad archiviare la documentazione dei flussi finanziari.

La Società non consente l'effettuazione di pagamenti al di fuori delle regole di comportamento previste, salvo eccezioni appositamente motivate dal Responsabile della Struttura di Ansaldo Energia che si occupa di amministrazione, finanza e controllo;

- la determinazione degli obiettivi aziendali ed i relativi programmi di incentivazione deve essere condotta nel rispetto della procedura aziendale ed in conformità ai principi di correttezza ed equilibrio, non individuando obiettivi eccessivamente ambiziosi e/o difficilmente realizzabili attraverso l'ordinaria operatività e che possano indurre a comportamenti indebiti;
- i premi di risultato, gli obiettivi di performance e gli altri elementi incentivanti di remunerazione sono rivisti, di norma annualmente, per verificare che vi siano ragionevoli garanzie per impedire che costituiscano incentivi alla corruzione. È compito del Responsabile della Unità Organizzativa Human Resources di Ansaldo Energia svolgere tale verifica;
- la gestione dei sistemi informativi per quel che riguarda la sicurezza dei sistemi, la gestione delle modifiche e la gestione dei *backup* deve avvenire nel rispetto delle procedure aziendali;
- la Società prevede che il personale non debba subire ritorsioni, discriminazione o azioni disciplinari per:
  - il rifiuto di partecipare a qualsiasi attività per la quale abbia ragionevolmente giudicato che vi sia un rischio di corruzione che non è stato mitigato dal Sistema;
  - aver effettuato segnalazioni in buona fede, o sulla base di una convinzione ragionevole, di un tentato atto corruttivo o violazione del Sistema.

Con riferimento alla gestione ed all'utilizzo dei sistemi informativi, si rimanda ai principi di comportamento ed alle modalità di presidio e controllo delle attività descritti nella **Parte Speciale E** "Reati Informatici e trattamento illecito di dati e violazioni del diritto d'autore".

A.4.2 PROCEDURE DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Tutte le aree individuate come aree a rischio sono presidiate da procedure la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'O.d.V. affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si riportano di seguito le direttive, le policy e le procedure da seguire nelle aree di attività a rischio individuate nella presente Parte Speciale.

Direttive e policy di riferimento:

- AE GROUP-DI-001 Code of Conduct for ICT Users;
- AE GROUP-DI-002 Export Compliance;
- AE GROUP-DI-003 Litigation Management;
- AE GROUP-DI-004 Appointment of Sales Promoters;
- AE GROUP-DI-005 Anti-Bribery and Corruption;
- AE GROUP-DI-006 Privacy;
- AE GROUP-DI-007 Managing Intellectual Property Assets;
- AE GROUP-DI-008 Information Security;
- AE GROUP-DI-009 Antitrust Directive;
- AE GROUP-DI-010 Delegation of Authority;
- AE GROUP-DI-012 Whistleblowing;
- AE GROUP-PL-003 AE Group Information & Cyber Security Policy;
- AE GROUP-PL-005 Anti-Bribery and Corruption policy.

Procedure di riferimento:

- AE-PR-001 Ansaldo Energia Group Management System Documents;
- AE-PR-016 Information Technology Management Process;
- AE-PR-017 Information Technology Management Process-IT Demand Management;
- AE-PR-018 Information Technology Management Process-IT Service Execution;
- AE-PR-021 Accounts Receivable Process;
- AE-PR-022 Accounts Payable Process;
- AE-PR-023 Fixed Assets Process;
- AE-PR-024 General Ledger Process;
- AE-PR-025 Tax Management Process;
- AE-PR-026 Consolidation Process;
- AE-PR-027 Treasury and Trade Finance Process;
- AE-PR-031 Management of powers attorney;
- AE-PR-033 Information & Cyber Security Process - Security Incident Management;
- AE-PR-034 External and Internal Communication;
- AE-PR-035 Management of hospitality and entertainment expenses, corporate gifts, sponsorships and donations;
- AE-PR-037 Ansaldo Energia Group Travel Management;
- AE-PR-043 Professional Services and Consulting Assignments required without RdA;
- AE-PR-044 Supply Chain management;
- AE-PR-046 Intercompany Transfer Pricing Policy;

- AE-PR-047 Management of Inside Information;
- AE-PR-048 Information Classification;
- AE-PR-050 Intellectual Property Process;
- AE-PR-051 Intellectual Property Process – IP Constitution;
- AE-PR-057 IT Access Management;
- AE-PR-058 IT Security Operating Handbook;
- AE-PR-064 Project Claims Management Process;
- AE-PR-069 Intellectual Property Transfer process – Manage Non-Disclosure Agreements;
- AE-PR-070 Intellectual Property Transfer process – Manage Collaborative Research;
- AE-PR-071 Vendor Rating Process;
- AE-PR-072 Vendor Qualification Process;
- AE-PR-075 Indipendent Auditors management;
- AE-PR-080 Recruitment Process;
- AE-PR-081 Privacy;
- AE-PR-082 Due Diligence;
- AE-PR-101 Compliance with EHS legislative regulations and other requirements;
- AE-PR-102 EHS Requisites for Procurement;
- AE-PR-103 Health and Safety Risk Assessment;
- AE-PR-104 Environmental aspects identification and management;
- AE-PR-105 EHS Training;
- AE-PR-106 EHS Communication and consultation;
- AE-PR-107 EHS Surveillance and Performance Measurement;
- AE-PR-108 EHS Non Conformity and corrective actions;
- AE-PR-201 Waste Management;
- AE-PR-202 Air Emission Control;
- AE-PR-205 Soil and groundwater protection and management of possible spillage;
- AE-PR-206 Hazardous Materials Management;
- AE-PR-208 Industrial Hygiene;
- AE-PR-209 Personal Protective Equipment;
- AE-PR-210 EHS Incident and near miss management;
- AE-PR-211 EHS Project Plan (Sites);
- AE-PR-212 EHS System implementation on sites;
- AE-PR-213 Contractor and Outsourcer Performance Inspection;
- AE-PR-214 Emergency preparedness and management;
- AE-PR-215 Machinery equipment and tool safety;
- AE-PR-218 Working at height;

- AE-PR-219 Lifting Operations and lifting accessories;
- AE-PR-220 Electrical safety;
- AE-PR-222 Sicurezza nelle aree a rischio esplosione;
- AE-PR-223 Hot works;
- AE-PR-225 Safety in professional travelling;
- AE-PR-226 Medical surveillance;
- AE-PR-227 Ergonomics;
- AE-PR-228 Traffic Management in a Site;
- AE-PR-229 Housekeeping;
- AE-IN-001 Business travel management;
- AE-IN-004 Purchase Request approval flow e rules;
- AE-IN-006 Passive Payments – Operational Checks Against Supplier Data Cyber Frauds;
- AE-IN-016 Guidelines for the management of company phone;
- AGT-PR-001 Sales process;
- AGT-PR-002 Supply Management;
- AGT-PR-005 Project Management;
- AGT-PR-006 Phase Review Management;
- AGT-PR-007 Product Development Design Review process;
- AGT-ENV-001 Servizio di raccolta e smaltimento dei rifiuti speciali di Ansaldo Green tech S.p.A. stabilimento di C.so Perrone 118.

A.5 SINGOLE OPERAZIONI A RISCHIO NELL'AMBITO DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE: INDIVIDUAZIONE DEI RESPONSABILI INTERNI E SCHEDE DI EVIDENZA

Occorre dare debita evidenza delle operazioni svolte nelle aree a rischio della commissione dei reati contro la Pubblica Amministrazione.

A tal fine, come già evidenziato nel paragrafo 3.4.2.3 il Presidente del Consiglio di Amministrazione, l'Amministratore Delegato, i Responsabili delle Unità Organizzative aziendali direttamente da essi dipendenti ed i Responsabili delle Strutture di Ansaldo Energia, divengono *Responsabili interni* di ogni singola operazione a rischio da loro direttamente svolta o attuata nell'ambito dell'Unità Organizzativa a loro facente capo. I suddetti:

- divengono i soggetti referenti dell'operazione a rischio;
- sono responsabili in particolare dei rapporti con la PA, per le attività con essa svolte.

Nell'ambito delle attività a rischio, i rapporti con la Pubblica Amministrazione devono essere portati a conoscenza dell'O.d.V. dai Responsabili interni tramite la compilazione di una Scheda di Evidenza che dovrà essere inviata su base semestrale (v. allegato II A) da cui risulti:

- la dichiarazione rilasciata dal Responsabile interno - per sé e per i suoi collaboratori delegati a svolgere attività che comportano rapporti con la PA - da cui risulti che lo stesso, da un lato, è pienamente a conoscenza degli adempimenti da espletare e

degli obblighi da osservare nello svolgimento delle operazioni e, dall'altro, che non è incorso in reati rilevanti ai sensi del Decreto;

- l'indicazione della PA con la quale si sono intrattenuti rapporti, incontri e/o attività - considerate "operazioni a rischio" - nel periodo ad oggetto della rilevazione.

PARTE SPECIALE "B"

Reati societari e di abuso di mercato e relativi illeciti amministrativi di cui al Testo Unico della Finanza

B.1 LA TIPOLOGIA DEI REATI SOCIETARI, DI MARKET ABUSE E DEI RELATIVI ILLECITI AMMINISTRATIVI (artt. 25-*ter* e 25-*sexies* del Decreto, art. 187-*quinquies* TUF)

Si riporta di seguito una breve descrizione dei reati, tra quelli contemplati negli artt. 25-*ter e 25-sexies* del Decreto e degli illeciti amministrativi di abuso di mercato di cui al testo unico della finanza, considerati potenzialmente a rischio per la Società.

B.1.1 FALSE COMUNICAZIONI SOCIALI (ART. 2621 C.C.)

La falsità nelle comunicazioni sociali si realizza con la consapevole esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali rilevanti non rispondenti al vero, ovvero omissione di fatti materiali rilevanti la cui comunicazione è imposta dalla legge, sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo concretamente idoneo ad indurre altri in errore.

Si precisa che:

- nella nozione di "comunicazione sociale" rientrano tutte le comunicazioni previste dalla legge dirette ai soci o al pubblico, ivi compresi il progetto di bilancio, le relazioni, i documenti da pubblicare ai sensi degli artt. 2501-*ter* e 2504-*novies* c.c. in caso di fusione o scissione, ovvero in caso di acconti sui dividendi, a norma dell'art. 2433-*bis* c.c.;
- le informazioni false o omesse devono essere rilevanti;
- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto, realizzata consapevolmente e concretamente idonea a trarre in inganno;
- un bilancio falso, rilevante in sede penale, non significa necessariamente bilancio invalido in senso civilistico;
- si tratta di reato di pericolo e quindi perseguibile indipendentemente dal verificarsi di un danno; inoltre, la perseguibilità è d'ufficio;
- la Legge 69/2015 ha eliminato le soglie quantitative, precedentemente previste, di non punibilità rispetto a discostamenti contabili non tali da alterare significativamente la rappresentazione societaria;
- la Legge di cui al punto precedente ha comunque introdotto l'articolo 2621-*bis* relativo a fatti di lieve entità (ripreso dal D.Lgs. 231/01 con l'introduzione, nell'art. 25-*ter* comma 1, della lettera a-*bis*)), secondo cui le pene previste sono ridotte *"se i fatti di cui all'art. 2621 sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta"* nonché se *"i fatti di cui all'articolo 2621 riguardano società che non superano i limiti indicati dal secondo comma dell'articolo 1 del regio decreto 16 marzo 1942, n. 267".* Nel secondo caso *"il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale";*
- la responsabilità si estende anche all'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Soggetti attivi del reato sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci ed i liquidatori (reato proprio).

B.1.2 FALSITÀ NELLE RELAZIONI O NELLE COMUNICAZIONI DELLA SOCIETÀ DI REVISIONE (ART. 2624 C.C.)[1]

Il reato consiste in false attestazioni od occultamento di informazioni, da parte dei responsabili della revisione, concernenti la situazione economica patrimoniale o finanziaria della società al fine di conseguire per sé o per gli altri un ingiusto profitto.

La sanzione è più grave se la condotta ha cagionato un danno patrimoniale ai destinatari delle comunicazioni.

Soggetti attivi sono i responsabili della Società di Revisione (reato proprio), ma i componenti degli organi di amministrazione di Ansaldo Green Tech ed i suoi dipendenti possono essere coinvolti a titolo di concorso nel reato. E', infatti, ipotizzabile il concorso eventuale, ai sensi dell'art. 110 c.p., degli amministratori, dei sindaci, o di altri soggetti della società revisionata, che abbiano determinato o istigato la condotta illecita del responsabile della Società di Revisione.

B.1.3 IMPEDITO CONTROLLO (ART. 2625 C.C.)

Il reato consiste nell'ostacolare o impedire lo svolgimento delle attività di controllo - legalmente attribuite ai soci o ad organi sociali - attraverso l'occultamento di documenti od altri idonei artifici.

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

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

Ai fini della presente norma, vengono in considerazione le attività poste in essere dai componenti del Consiglio di Amministrazione, nonché dai dipendenti che prestino collaborazione a questi ultimi, che possono avere influenza sulle iniziative e sulle attività di controllo spettanti ai soci o agli altri organi sociali.

Si tratta, più precisamente, delle attività che influiscono:

- sulle iniziative di controllo dei soci previste dal codice civile e dagli altri atti normativi, quali ad esempio l'art. 2422 c.c. che prevede il diritto dei soci di ispezionare i libri sociali;
- sulle attività di controllo del collegio sindacale, previste dal codice civile e dalle altre norme, quali ad esempio gli artt. 2403 e 2403-*bis* che prevedono il potere dei membri del Collegio sindacale di procedere ad atti di ispezione e di controllo e di

[1] Il D.Lgs. 27 gennaio 2010, n. 39, nel riformare l'intera materia della revisione legale, ha disposto l'abrogazione dell'art. 2624 (falsità nelle relazioni o nelle comunicazioni delle società di revisione), fattispecie sostituita dall'art. 27 del medesimo D.Lgs.. L'abrogazione della norma del codice civile non è stata però accompagnata dalla sostituzione, nell'art. 25-*ter,* del riferimento all'art. 2624 con il riferimento alla nuova fattispecie di reato di cui all'art. 27 D.Lgs. n. 39 del 2010 (falsità nelle relazioni o nelle comunicazioni dei responsabili della revisione legale). Ciò comporterebbe la non applicabilità della nuova fattispecie di reato nell'ambito del D.Lgs. 231/2001. In tal senso si è anche espressa la Corte di Cassazione (Sezioni Unite Penali, sentenza n. 34476 del 23 giugno 2011), stabilendo che: "*il d.lgs. 27 gennaio 2010, n. 39, nell'abrogare e riformulare il contenuto precettivo dell'art. 174-bis T.U.F. (Falsità nelle relazioni o nelle comunicazioni delle società di revisione), non ha influenzato in alcun modo la disciplina propria della responsabilità amministrativa da reato dettata dall'art. 25-ter d.lgs. n. 231 del 2001, poiché le relative fattispecie non sono richiamate da questo testo normativo e non possono conseguentemente costituire fondamento di siffatta responsabilità*".

richiedere agli amministratori notizie sull'andamento delle operazioni sociali o di determinati affari.

B.1.4 OPERAZIONI IN PREGIUDIZIO DEI CREDITORI (ART. 2629 C.C.)

La norma punisce gli amministratori che effettuino operazioni di riduzione del capitale sociale o di fusione o scissione, con modalità tali da cagionare un danno ai creditori.

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

Con riferimento alle operazioni di riduzione del capitale sociale, si possono citare i seguenti esempi di condotte penalmente rilevanti: esecuzione della delibera di riduzione del capitale sociale nonostante l'opposizione dei creditori sociali o in mancanza della delibera da parte del Tribunale.

Con riferimento alle operazioni di fusione o di scissione, si possono ricordare l'esecuzione di dette operazioni prima del termine di cui all'art. 2503, comma 1, ove non ricorrano le eccezioni ivi previste ovvero in presenza di opposizione e senza l'autorizzazione del Tribunale.

Particolari profili di rischio si rinvengono quanto alle attività relative alle:

- operazioni di riduzione del capitale sociale (vedi, ad esempio, riduzione del capitale sociale per esuberanza, art. 2445 c.c.);
- operazioni di fusione o scissione della Società (vedi, ad esempio, artt. 2503 e 2506-*ter* c.c.).

B.1.5 OMESSA COMUNICAZIONE DEL CONFLITTO D'INTERESSI (ART.2629-*BIS* C.C.)

Il reato in esame si configura allorché un componente del consiglio di amministrazione o del consiglio di gestione di una società, violando la disciplina in materia di interessi degli amministratori prevista dal codice civile, rechi alla stessa o a terzi un danno.

In particolare, l'art. 2391 c.c. impone ai membri del consiglio di amministrazione di comunicare (agli altri membri del consiglio e ai sindaci) ogni interesse che i medesimi, per conto proprio o di terzi, abbiano in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata.

L'amministratore che sia portatore di un interesse in una determinata operazione della società deve astenersi dalla stessa, rimettendola alle determinazioni dell'intero consiglio.

In entrambi i casi, la deliberazione del Consiglio di Amministrazione deve adeguatamente motivare le ragioni e la convenienza dell'operazione.

Ai fini che qui rilevano, vengono in considerazione solo le ipotesi in cui il reato sia commesso nell'interesse o a vantaggio della società, ipotesi che può sussistere, in particolare nel caso in cui un amministratore di Ansaldo Green Tech abbia agito in violazione dell'art. 2391 c.c., nell'intento di recare un vantaggio alla Società, ancorché dalla sua condotta sia poi in realtà derivato un danno alla Società medesima.

B.1.6 ILLECITA INFLUENZA SULL'ASSEMBLEA (ART. 2636 C.C.)

Il reato si realizza quando con atti simulati o con frode si determina la maggioranza in assemblea, allo scopo di conseguire, per sé o per altri, un ingiusto profitto; si tratta di un "reato comune", che può, quindi, essere commesso da chiunque.

La norma mira ad evitare che, attraverso condotte fraudolente, si influisca illegittimamente sulla formazione della maggioranza assembleare.

Ai fini della norma in esame vengono in considerazione le condotte volte alla convocazione dell'assemblea, all'ammissione alla partecipazione all'assemblea e al computo dei voti per la deliberazione, nonché le relative attività di supporto.

B.1.7 AGGIOTAGGIO (ART. 2637 C.C.) E MANIPOLAZIONE DEL MERCATO (ARTT. 185 E 187-*TER* TUF)

L'abuso di mercato realizzato attraverso l'alterazione delle dinamiche relative alla corretta formazione del prezzo di strumenti finanziari viene oggi punito, sia come reato, dagli artt. 2637 c.c. (aggiotaggio) e 185 TUF (manipolazione del mercato), sia da un illecito amministrativo, previsto dall'art. 187-*ter* TUF.

Le due ipotesi di reato si distinguono in relazione alla natura degli strumenti finanziari il cui prezzo potrebbe essere influenzato dalle condotte punite. Nel caso dell'aggiotaggio, vengono presi in considerazione strumenti finanziari non quotati o per i quali non sia stata presentata domanda di ammissione alla negoziazione in un mercato regolamentato; nel caso del reato e dell'illecito amministrativo di manipolazione del mercato, si tratta di strumenti finanziari quotati per i quali sia stata presentata richiesta di ammissione alla negoziazione su mercati regolamentati.

La condotta costitutiva dei reati di aggiotaggio e manipolazione del mercato consiste:

- nella diffusione di notizie false (*information based manipulation*);
- nel compimento di operazioni simulate o di altri artifici idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari quotati o non quotati (*action based manipulation*).

Inoltre, il reato di aggiotaggio punisce anche le condotte volte ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.

L'illecito amministrativo di manipolazione del mercato (art. 187-*ter*) si configura, invece, nelle ipotesi di:

- diffusione, tramite mezzi di informazione, compreso Internet o ogni altro mezzo, di informazioni, voci o notizie false o fuorvianti che forniscano o siano suscettibili di fornire indicazioni false ovvero fuorvianti in merito agli strumenti finanziari;
- compimento di operazioni od ordini di compravendita che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari;
- compimento di operazioni od ordini di compravendita che consentono, tramite l'azione di una o più persone che agiscono di concerto, di fissare il prezzo di mercato di uno o più strumenti finanziari ad un livello anomalo o artificiale;

- realizzazione di altri artifizi idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

L'illecito amministrativo ha una sfera di applicazione molto più ampia rispetto al reato, dal quale si distingue in quanto:

- è punibile anche a titolo di semplice colpa e, dunque, per aver posto in essere le condotte sopra indicate per imprudenza, negligenza o imperizia;
- non richiede l'idoneità delle informazioni, delle operazioni o degli artifici a provocare una sensibile alterazione del prezzo di strumenti finanziari.

La manipolazione del mercato può essere realizzata nell'interesse dell'Ente sia nell'ipotesi in cui esso operi quale emittente di strumenti finanziari, sia nell'ambito di un rapporto negoziale di consulenza, intermediazione o finanziario con terzi.

B.1.8 OSTACOLO ALL'ESERCIZIO DELLE FUNZIONI DELLE AUTORITÀ PUBBLICHE DI VIGILANZA (ART. 2638 C.C.)

Il reato può realizzarsi attraverso due distinte modalità, entrambe finalizzate ad ostacolare l'attività di vigilanza delle autorità pubbliche preposte:

- attraverso comunicazioni alle Autorità di Vigilanza di fatti, sulla situazione economica, patrimoniale o finanziaria, non corrispondenti al vero, ovvero con l'occultamento, in tutto o in parte, con altri mezzi fraudolenti, di fatti che avrebbero dovuto essere comunicati concernenti la situazione medesima;
- attraverso il semplice ostacolo all'esercizio delle funzioni di vigilanza, attuato consapevolmente, in qualsiasi modo.

B.1.9 ABUSO O COMUNICAZIONE ILLECITA DI INFORMAZIONI PRIVILEGIATE. RACCOMANDAZIONE O INDUZIONE DI ALTRI ALLA COMMISSIONE DI ABUSO DI INFORMAZIONI PRIVILEGIATE (ART. 184 E 187-*QUATER* DEL D.LG. 58/98 TESTO UNICO DELLA FINANZA)

Le norme in esame puniscono l'abuso delle informazioni privilegiate conosciute in ragione dell'attività svolta o anche per ragioni diverse attraverso il compimento di operazioni sugli strumenti finanziari o altri prodotti oggetto di aste su piattaforme d'asta autorizzate (di seguito per brevità strumenti finanziari) cui le informazioni si riferiscono, ovvero attraverso la comunicazione – in forma diretta o indiretta – di dette informazioni.

Il reato e l'illecito amministrativo – meglio noti come *insider trading* – possono essere realizzati in vari modi:

- viene anzitutto in considerazione il c.d. trading, ossia l'acquisto, la vendita o il compimento di altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari, utilizzando informazioni privilegiate. E' opportuno al riguardo rimarcare che il divieto di utilizzazione comprende qualsiasi operazione su strumenti finanziari: non soltanto, dunque, l'acquisto o la vendita, ma anche riporti, permute, ecc.;
- si parla invece di *tipping* a proposito della indebita comunicazione delle informazioni privilegiate ad altri. Più in particolare, l'ipotesi ricorre nel caso il cui l'insider primario

comunichi la notizia privilegiata "*al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio*". Al riguardo, la comunicazione si ritiene lecita quando trova fondamento in norme che la consentano o la impongano, ovvero nel contesto di prassi o usanze consolidate. Più in particolare, in riferimento ai gruppi societari, si ravvisa una comunicazione afferente il normale esercizio dell'ufficio nella trasmissione dei dati necessari alla formazione del bilancio consolidato (art. 43 D.Lgs. 127 del 1991 e art. 25, co. 4, D. Lgs. 356 del 1990), nonché nelle comunicazioni scambiate nel contesto dell'attività di direzione e coordinamento che oggi compete alla holding ai sensi dell'art. 2497 c.c., ovvero diffuse ai sensi dell'art. 114 TUF che impone, "fermi gli obblighi di pubblicità previsti da specifiche disposizione di legge" agli emittenti quotati e ai soggetti che li controllano di comunicare al pubblico, senza indugio e secondo le modalità indicate dalla Consob, le informazioni privilegiate che riguardano direttamente detti emittenti e le società controllate;

- infine, viene in considerazione il c.d. *tuyautage*, ossia la raccomandazione o l'induzione di altri al compimento di una delle operazioni descritte in relazione ad informazioni privilegiate. In tale specifica ipotesi, l'insider non comunica a terzi l'informazione privilegiata, ma si limita – sulla base di questa – a consigliare o indurre terzi al compimento di una determinata operazione che egli sa, in virtù della notizia a sua conoscenza, idonea ad influire in modo sensibile sui prezzi di strumenti finanziari.

Quanto alla nozione di strumenti finanziari, l'art. 180 T.U.F. specifica che sono tali quelli previsti dall'art. 1, co. 2. T.U.F. "*ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altro Paese dell'Unione europea, nonché qualsiasi altro strumento ammesso o per il quale è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato di un Paese dell'Unione europea*".

Si precisa che l'art. 184, co. 5 T.U.F. precisa "*Le disposizioni del presente articolo si applicano anche quando i fatti di cui ai commi 1, 2 e 3 riguardano condotte od operazioni, comprese le offerte, relative alle aste su una piattaforma d'asta autorizzata, come un mercato regolamentato di quote di emissioni o di altri prodotti oggetto d'asta correlati, anche quando i prodotti oggetto d'asta non sono strumenti finanziari, ai sensi del regolamento (UE) n. 1031/2010 della Commissione, del 12 novembre 2010".*

E', invece, ai sensi dell'art. 181, co. 1, T.U.F., *informazione privilegiata*, quella "*di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari*". Lo stesso art. 180, al comma 4, precisa, altresì, la nozione di notizia *price sensitive*, definendola come "*un'informazione che presumibilmente un investitore ragionevole utilizzerebbe come uno degli elementi su cui fondare le proprie decisioni di investimento*".

Inoltre, l'informazione si ritiene di carattere preciso se: "*a) si riferisce ad un complesso di circostanze esistente o che si possa ragionevolmente prevedere che verrà ad esistenza o ad un evento verificatosi o che si possa ragionevolmente prevedere che si verificherà; b) è sufficientemente specifica da consentire di trarre conclusioni sul possibile effetto del complesso di circostanze o dell'evento di cui alla lettera a) sui prezzi degli strumenti finanziari*".

A tale definizione non sono riconducibili le ricerche o valutazioni, comprese quelle effettuate dalle società di *rating*, riguardanti strumenti finanziari, "*elaborate a partire da dati di dominio pubblico*" (v. 13° Considerando direttiva n. 592/89/CEE), posto che esse non

presentano la natura di *informazioni*.

In ogni caso, come oggi specificato dall'art. 114 TUF, "*i soggetti che producono o diffondono ricerche o valutazioni, comprese le società di rating, riguardanti strumenti finanziari, nonché i soggetti che producono o diffondono altre informazioni che raccomandano o propongono strategie di investimento destinate ai canali di divulgazione o al pubblico, devono presentare l'informazione in modo corretto e comunicare l'esistenza di ogni loro interesse o conflitto di interessi riguardo agli strumenti finanziari cui l'informazione si riferisce*".

L'art. 181 T.U.F. precisa, altresì, al comma 5, che "*nel caso di persone incaricate dell'esecuzione di ordini relativi a strumenti finanziari, per informazione privilegiata si intende anche l'informazione trasmessa da un cliente e concernente gli ordini del cliente in attesa di esecuzione, che ha un carattere preciso e che concerne, direttamente o indirettamente, uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari*".

Sul piano dell'elemento soggettivo, mentre il delitto è punibile soltanto a titolo di dolo, occorrendo dunque la consapevolezza e la volontà di sfruttare indebitamente le informazioni privilegiate di cui si è in possesso, l'illecito amministrativo è punibile anche a titolo di mera colpa, essendo dunque sufficiente la negligenza consistente nell'incauto utilizzo o la comunicazione a terzi della notizia privilegiata.

B.1.10 ILLECITE OPERAZIONI SULLE AZIONI O QUOTE SOCIALI O DELLA SOCIETÀ CONTROLLANTE (ART. 2628 C.C.)

Il reato consiste nel procedere – fuori dai casi consentiti dalla legge – all'acquisto od alla sottoscrizione di azioni o quote emesse dalla Società (o dalla società controllante) che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge. La ricostituzione del capitale sociale o delle riserve prima del termine previsto per l'approvazione del bilancio, relativo all'esercizio in relazione al quale è stata posta in essere la condotta, costituisce una modalità di estinzione del reato.

Soggetti attivi del reato sono gli amministratori. Inoltre, è configurabile una responsabilità a titolo di concorso degli amministratori della controllante con quelli della controllata, nell'ipotesi in cui le operazioni illecite sulle azioni della controllante medesima siano effettuate da questi ultimi su istigazione dei primi.

B.2 AREE A RISCHIO

Le aree di attività considerate a rischio in relazione ai reati societari sono ritenute le seguenti:

1. Gestione dei rapporti con istituzioni ed enti pubblici.
2. Gestione degli affari societari.
3. Rapporti con la Società di Revisione ed il Collegio Sindacale.
4. Gestione delle informazioni / operazioni relative a strumenti finanziari quotati e non.
5. Tenuta della contabilità, redazione del bilancio e gestione della fiscalità.
6. Gestione dei rapporti con parti correlate.

7. Sistemi informativi.

Per il dettaglio delle attività a potenziale rischio si rinvia a quanto indicato nei paragrafi A.3.3, A.3.7, A.3.9, A.3.10, A.3.12, A.3.20 e A.3.21.

B.3 PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITA' A RISCHIO

B.3.1 PRINCIPI DI COMPORTAMENTO DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Ai Destinatari è fatto espresso obbligo di:

- osservare una condotta improntata a principi di integrità, correttezza e trasparenza nell'attività di formazione del bilancio, delle relazioni e delle altre comunicazioni sociali previste dalla legge, in modo da fornire ai soci e al pubblico informazioni veritiere e corrette sulla situazione economica, patrimoniale e finanziaria della Società e del gruppo cui essa appartiene, nel rispetto di tutte le norme di legge, regolamentari e dei principi contabili applicativi;
- porre particolare attenzione nella stima delle poste contabili: i soggetti che intervengono nel procedimento di stima devono attenersi al rispetto del principio di ragionevolezza ed esporre con chiarezza i parametri di valutazione seguiti, fornendo ogni informazione complementare che sia necessaria a garantire la veridicità del documento. Il bilancio deve, inoltre, essere completo sotto il profilo dell'informazione societaria e deve contenere tutti gli elementi richiesti dalla legge e dalle eventuali Istruzioni di Vigilanza applicabili. Analoga correttezza è richiesta agli amministratori ed ai sindaci nella redazione di tutte le altre comunicazioni imposte o, comunque, previste dalla legge e dirette ai soci o al pubblico, affinché le stesse contengano informazioni chiare, precise, veritiere e complete. Con riferimento al bilancio consolidato la Società stessa assicura l'osservanza di criteri di redazione dei bilanci uniformi e si attiene, in sede di consolidamento, al rispetto dei principi di correttezza, ragionevolezza nella determinazione dei criteri, rifiutandosi di procedere al consolidamento ove ravvisi ipotesi di non perfetta osservanza da parte delle controllate dei suddetti criteri;
- osservare una condotta improntata a principi etici di integrità, correttezza e trasparenza nell'attività di formazione dei prospetti richiesti ai fini della sollecitazione all'investimento o dell'ammissione alla quotazione nei mercati regolamentati, ovvero dei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, per modo di consentire ai destinatari dei prospetti di pervenire ad un giudizio informato ed oggettivo sulla situazione economica, patrimoniale o finanziaria della Società, ovvero sugli strumenti finanziari emessi da quest'ultima e sui relativi diritti. A tale scopo, i prospetti informativi e/o i documenti in commento devono essere completi sotto il profilo dell'informazione e devono contenere tutti gli elementi, laddove previsto, richiesti dalla legge e dalle Istruzioni di vigilanza;
- osservare una condotta tesa a garantire il regolare funzionamento della Società, e la corretta interazione tra i suoi organi sociali, assicurando ed agevolando ogni forma di controllo sulla gestione sociale, nei modi previsti dalla legge, nonché la libera e regolare formazione della volontà assembleare;
- nel compimento di operazioni di qualsiasi natura su strumenti finanziari, ovvero nella diffusione di informazioni relative ai medesimi, attenersi al rispetto dei principi

di correttezza, trasparenza, completezza dell'informazione, tutela del mercato e rispetto delle dinamiche di libera determinazione del prezzo dei titoli. In tale prospettiva, è fatto assoluto divieto di diffondere, concorrere a diffondere, in qualunque modo, informazioni, notizie o dati falsi o porre in essere operazioni fraudolente o, comunque, fuorvianti in modo anche solo potenzialmente idoneo a provocare un'alterazione del prezzo di strumenti finanziari. Ansaldo Green Tech si impegna:

  - a comportarsi sempre con diligenza, correttezza e trasparenza, nell'interesse del pubblico degli investitori e del mercato;
  - organizzarsi in modo da escludere la ricorrenza di situazioni di conflitto di interesse e, in tali occasioni, assicurare comunque l'equilibrata tutela degli interessi in conflitto;
  - adottare misure affinché non si realizzi un'indebita circolazione/diffusione, all'interno della Società e del Gruppo, di informazioni rilevanti;

- improntare i rapporti con le Autorità di vigilanza a criteri di integrità, correttezza, trasparenza e collaborazione, evitando comportamenti che possano in qualsiasi modo considerarsi di ostacolo alle attività che tali Autorità sono chiamate a svolgere a garanzia del mercato. In tale prospettiva, gli Esponenti aziendali devono:
  - inviare alle Autorità di Vigilanza le segnalazioni previste dalla legge e dai regolamenti (incluse le Istruzioni di Vigilanza) o richieste ad altro titolo alla Società in modo tempestivo, completo ed accurato, trasmettendo a tal fine tutti i dati ed i documenti previsti o richiesti;
  - indicare nelle predette segnalazioni dati rispondenti al vero, completi e corretti, dando indicazioni di ogni fatto rilevante relativo alla situazione economica, patrimoniale o finanziaria della Società;
  - evitare ogni comportamento che possa ostacolare le Autorità di Vigilanza nell'esercizio delle proprie prerogative (attraverso, ad esempio, mancanza di collaborazione, comportamenti ostruzionistici, risposte reticenti o incomplete, ritardi pretestuosi).

Ai Destinatari è fatto, altresì, obbligo di garantire il puntuale rispetto di tutte le norme di legge che tutelano l'integrità e l'effettività del capitale sociale, al fine di non creare nocumento alle garanzie dei creditori e, più in generale, ai terzi nonché espresso divieto di:

- indicare o inviare per l'elaborazione o l'inserimento in dette comunicazioni, dati falsi, artefatti, incompleti o comunque non rispondenti al vero, sulla situazione economica, patrimoniale o finanziaria della Società. E' fatto, inoltre, divieto di porre in essere attività e/o operazioni volte a creare disponibilità extracontabili (ad esempio ricorrendo a fatture per operazioni inesistenti o alla sovra fatturazione), ovvero volte a creare "fondi neri" o "contabilità parallele", anche per valori inferiori alle soglie di rilevanza penale poste dagli artt. 2621 e 2622 c.c.;
- impedire od ostacolare in qualunque modo, anche occultando documenti o utilizzando altri idonei artifici, lo svolgimento delle attività istituzionali di controllo e di revisione, proprie del Collegio Sindacale e/o delle Società di Revisione;
- determinare o influenzare illecitamente l'assunzione delle delibere assembleari, ponendo a tal fine in essere atti simulati o fraudolenti che si propongano di alterare artificiosamente il normale e corretto procedimento di formazione della volontà assembleare.

Con riferimento alla tenuta della contabilità, redazione del bilancio e gestione della fiscalità, la redazione del bilancio annuale, la relazione sulla gestione, la relazione semestrale e la scelta della Società di Revisione debbono essere realizzate in base ai seguenti principi:

- rispetto dei principi di compilazione dei documenti contabili ai sensi dell'art. 2423 comma 2 c.c.;
- in sede di stima delle poste contabili, occorre attenersi ad un principio di ragionevolezza ed esporre con chiarezza i parametri di valutazione seguiti, fornendo ogni eventuale informazione complementare necessaria a garantire la veridicità del documento (v. artt. 2423 comma 3 e 2423-*bis* c.c.);
- assicurare la completezza del bilancio sotto il profilo dell'informazione societaria, indicando, in particolare, tutti gli elementi richiesti dalla legge, quali ad esempio, quelli previsti dall'art. 2424 c.c., per lo stato patrimoniale, dall'art. 2425 c.c., per il conto economico e dall'art. 2427 c.c. per la nota integrativa;
- analoga correttezza va posta nella redazione delle altre comunicazioni imposte o, comunque, previste dalla legge e dirette ai soci o al pubblico affinché le stesse contengano informazioni chiare, precise, veritiere e complete.

Con specifico riferimento alla predisposizione del bilancio, le procedure di Ansaldo Green Tech prevedono:

- l'elencazione dei dati e delle notizie che ciascuna Unità Organizzativa deve fornire, a quali altre Unità debbono essere trasmessi, i criteri per la loro elaborazione, la tempistica di consegna;
- la trasmissione dei dati ed informazioni all'Unità Organizzativa responsabile per via informatica in modo che restino tracciati i vari passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- la tempestiva trasmissione a tutti i membri del Consiglio di Amministrazione e del Collegio Sindacale della bozza di bilancio e della relazione della Società di Revisione, nonché un'idonea registrazione di tale trasmissione;
- riunioni periodiche tra la Società di Revisione ed il Collegio Sindacale, cui può essere invitato a partecipare anche l'O.d.V.;
- la puntuale verifica in ordine all'effettività e congruità delle prestazioni in relazioni alle quali viene rilasciata fattura alla Società, con coinvolgimento delle Unità Organizzative che hanno usufruito della prestazione al fine di acquisire attestazione dell'effettivo svolgimento della stessa e della sua rispondenza all'oggetto del contratto;
- l'obbligo di rispetto delle disposizioni previste dall'art. 2391 c.c. in tema di obblighi degli amministratori di comunicazione al Consiglio di eventuali situazioni di conflitto di interesse e di conseguente assunzione delle relative determinazioni con delibera adeguatamente motivata, e dall'art. 2428 c.c., in tema di obbligo di esposizione nella relazione sulla gestione delle più rilevanti operazioni intragruppo;
- la tracciabilità delle operazioni che comportino il trasferimento e/o deferimento di posizioni creditorie, attraverso le figure della surrogazione, cessione del credito, l'accollo di debiti, il ricorso alla figura della delegazione, le transazioni e/o rinunce alle posizioni creditorie e delle relative ragioni giustificatrici;
- la tracciabilità del processo relativo alle comunicazioni alle Autorità di Vigilanza da effettuare nel rispetto delle norme di legge e regolamenti, in vista degli obiettivi di trasparenza e corretta informazione. Agli eventuali incontri con le Autorità di Vigilanza (anche in sede ispettiva) devono intervenire i soggetti aziendali a ciò

espressamente autorizzati; ogni incontro deve essere debitamente documentato e deve avvenire alla presenza di almeno due rappresentati della Società. In caso di ispezione disposta dalle Autorità di Vigilanza, la Società assicura il coordinamento di tutte le Unità Organizzative interessate affinché sia garantita la più ampia e tempestiva collaborazione a dette Autorità, fornendo dati e documenti richiesti in modo tempestivo e completo;

- l'obbligo di inoltro di tempestiva comunicazione all'Autorità di Vigilanza in caso di errori, omissioni o imprecisioni in materia di comunicazioni od operazioni aventi ad oggetto strumenti finanziari o comunque fatti idonei ad influire sul mercato;
- l'individuazione dei soggetti legittimati al compimento delle operazioni aventi ad oggetto strumenti finanziari, nel rispetto della legge e delle norme interne;
- l'obbligo di eseguire le operazioni di investimento sulla base delle strategie previamente definite formalmente dai competenti Organi e/o Unità Organizzative.

Le attività soggette a vigilanza da parte delle pubbliche autorità devono essere svolte in base a specifici criteri che attribuiscono determinate responsabilità per:

- le segnalazioni periodiche alle autorità previste da leggi e regolamenti;
- la trasmissione alle autorità di dati e documenti richiesti;
- i rapporti da tenere nel corso delle verifiche ispettive.

Tutte le comunicazioni e l'informativa trasmessa alle Autorità di Vigilanza deve anche essere tenuta a disposizione dell'O.d.V..

Con specifico riferimento alla gestione dei rapporti con parti correlate, tali operazioni devono:

- essere svolte nel rispetto di criteri di correttezza sostanziale;
- essere previamente regolamentate sulla base di contratti stipulati in forma scritta, che devono essere trattenuti e conservati agli atti di ciascuna delle società contraenti. Dette condizioni devono essere regolate a condizioni di mercato, sulla base di valutazioni di reciproca convenienza economica, avuto peraltro riguardo al comune obiettivo di creare valore per l'intero Gruppo.

Con riferimento alla gestione dei sistemi informativi, le relative attività devono essere svolte nel rispetto dei principi riportati nella Parte Speciale E cui si fa rinvio.

Con riferimento alla gestione degli affari societari, le relative attività sono gestite in coerenza con la procedura aziendale volta, tra l'altro, a garantire la libera e regolare formazione della volontà assembleare prevedono l'espresso divieto di determinare od influenzare illecitamente l'assunzione delle delibere assembleari, ponendo a tal fine in essere atti simulati o fraudolenti che si propongano di alterare artificiosamente il normale e corretto procedimento di formazione della volontà assembleare.

Con riferimento alla gestione dei rapporti con la Società di Revisione ed il Collegio Sindacale, le relative attività devono essere svolte nel rispetto della procedura aziendale e dei seguenti principi:

- tempestiva trasmissione al Collegio Sindacale di tutti i documenti relativi ad argomenti posti all'ordine del giorno di Assemblee e Consigli di Amministrazione o sui quali il Collegio debba esprimere un parere;

- messa a disposizione del Collegio e della Società di Revisione dei documenti sulla gestione della Società per le verifiche proprie dei due organismi;
- previsione di riunioni periodiche tra Collegio Sindacale e Società di Revisione, cui può essere invitato a partecipare anche l'O.d.V. per verificare l'osservanza delle regole e procedure aziendali in tema di norme societarie.

Con riferimento alla gestione delle informazioni/operazioni relative a strumenti finanziari quotati e non, le relative attività devono essere svolte nel rispetto dei seguenti principi:

- l'esistenza di presidi volti a garantire che la circolazione delle informazioni privilegiate nell'ambito della Società avvenga nel rispetto del principio della oggettiva necessità di comunicazione in relazione all'attività svolta (c.d. "*need to know*");
- la previa individuazione delle condizioni per l'eventuale comunicazione a terzi di informazioni privilegiate;
- la preventiva approvazione della comunicazione a terzi di eventuali informazioni privilegiate, previa valutazione della sussistenza delle condizioni poste dalla Società per la comunicazione e l'individuazione dei soggetti autorizzati ad acquisire ed utilizzare dette informazioni. L'eventuale autorizzazione può essere rilasciata solo in forma scritta;
- adeguate cautele volte a garantire la protezione e custodia della documentazione contenente informazioni riservate in modo da impedire accessi indebiti.

La Società dispone il rispetto dei seguenti principi:

- operazioni personali: è fatto divieto di compiere operazioni personali, per conto proprio o per conto terzi anche per interposta persona, effettuate utilizzando informazioni privilegiate acquisite in ragione delle proprie funzioni, nonché il divieto di raccomandare o indurre altri a compiere operazioni utilizzando le predette informazioni privilegiate;
- rapporti con la stampa e comunicazioni esterne: i rapporti con la stampa e con gli altri mezzi di comunicazione di massa sono riservati ad uno specifico Ente aziendale e devono svolgersi secondo specifiche procedure preventivamente fissate, nell'ambito delle quali assume particolare rilievo la previsione di punti di controllo sulla correttezza della notizia;
- rapporti con altri soggetti esterni: in linea con quanto già evidenziato nella Parte Speciale A, i rapporti con le pubbliche amministrazioni, le organizzazioni politiche e sindacali e con altri soggetti esterni devono essere tenuti dai soggetti a ciò espressamente autorizzati e devono essere improntati a correttezza, integrità, imparzialità e indipendenza, non influenzando impropriamente le decisioni della controparte e non richiedendo trattamenti di favore. E' in ogni caso fatto divieto di promettere, erogare o ricevere favori, somme e benefici di qualsivoglia natura.

Le attività che comportino il trattamento di informazioni idonee ad influire sul mercato e il compimento di operazioni su strumenti finanziari devono essere svolte in base a procedure aziendali relative a:

- la gestione, la diffusione, il trattamento e le modalità di protezione rispetto ad indebiti accessi delle informazioni privilegiate relative alla Società, a società controllate o a terzi, attraverso anche la previsione di meccanismi di tracciabilità degli eventuali accessi alle stesse;
- la determinazione dei criteri per l'individuazione delle informazioni privilegiate;

- l'informazione, nei confronti delle persone che hanno accesso a informazioni privilegiate, in merito agli obblighi giuridici e che derivano dall'aver accesso alle informazioni privilegiate e alle possibili sanzioni in caso di abuso o diffusione non autorizzata delle informazioni cui hanno accesso;
- l'individuazione di un organo incaricato della verifica, autorizzazione e supervisione del processo di diffusione delle informazioni privilegiate;
- le modalità di formazione e diffusione delle notizie relative alla Società, attraverso l'individuazione dei soggetti cui compete il controllo sulla correttezza e diffondibilità dell'informazione e dei soggetti, diversi rispetto ai primi, espressamente autorizzati – funzionalmente o in relazione a casi specifici – ad intrattenere rapporti di carattere istituzionale con giornalisti, sindacati, analisti ed agenzie di rating e, più in generale, alla diffusione all'esterno – anche tramite comunicati stampa o il sito web – di dette notizie;
- le modalità di formazione, controllo e diffusione di comunicazioni sociali, studi, ricerche, piani strategici e finanziari e altre informazioni rilevanti relative alla Società;
- la comunicazione di informazioni e fatti rilevanti verificatisi all'interno delle Società controllate;
- la previsione di specifiche cautele contrattuali, volte a regolare il trattamento e l'accesso ad informazioni privilegiate da parte di consulenti/partner attraverso la previsione di specifiche clausole di riservatezza e di rispetto del Modello;
- i comportamenti e le responsabilità per la gestione delle situazioni di urgenza per il ripristino delle condizioni di simmetria informativa in presenza di rumor o informazioni privilegiate indebitamente diffuse e disponibili al pubblico;
- l'identificazione in via preventiva delle informazioni privilegiate per le quali è possibile procedere, in ritardo, alla comunicazione al fine di non pregiudicare i legittimi interessi della Società, nonché del relativo procedimento e dei soggetti responsabili.

Tutte le operazioni sul capitale sociale della Società, di destinazione di utili e riserve, di acquisto e cessione di partecipazioni e rami d'azienda, di fusione, scissione e scorporo, nonché tutte le operazioni, anche nell'ambito delle Società controllate, che possano potenzialmente ledere l'integrità del capitale sociale debbono essere ispirate ai seguenti principi:

- l'attribuzione al C.d.A. della preventiva approvazione di operazioni societarie che possano comportare significativi impatti sotto il profilo economico, patrimoniale e finanziario (ad esempio, operazioni sul capitale, fusioni, scissioni, trasformazioni, acquisti di azioni proprie, restituzione di conferimenti, acquisti o cessioni di rami d'azienda ecc.);
- l'assegnazione di responsabilità decisionali ed operative per le operazioni anzidette, nonché i meccanismi di coordinamento tra le diverse Strutture coinvolte;
- l'informativa da parte del Management aziendale e la discussione delle operazioni anzidette in riunioni tra il Collegio Sindacale, la Società di Revisione e l'O.d.V..

B.3.2 PROCEDURE DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Tutte le aree individuate come aree a rischio sono presidiate da procedure la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'O.d.V. affinché

provveda al suo accertamento e, quindi, a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si riportano di seguito le direttive, policy e procedure da seguire nelle aree di attività a rischio individuate nella presente Parte Speciale.

Direttive di riferimento:

- AE GROUP-DI-001 Code of Conduct for ICT Users;
- AE GROUP-DI-006 Privacy;
- AE GROUP-DI-007 Managing Intellectual Property Assets;
- AE GROUP-DI-008 Information Security;
- AE GROUP-DI-010 Delegation of Authority;
- AE GROUP-DI-012 Whistleblowing;
- AE GROUP-PL-003 AE Group Information & Cyber Security Policy.

Procedure di riferimento:

- AE-PR-016 Information Technology Management Process;
- AE-PR-017 Information Technology Management Process-IT Demand Management;
- AE-PR-018 Information Technology Management Process-IT Service Execution;
- AE-PR-021 Accounts Receivable Process;
- AE-PR-022 Accounts Payable Process;
- AE-PR-023 Fixed Assets Process;
- AE-PR-024 General Ledger Process;
- AE-PR-025 Tax Management Process;
- AE-PR-026 Consolidation Process;
- AE-PR-027 Treasury and Trade Finance Process;
- AE-PR-031 Management of powers attorney;
- AE-PR-033 Information & Cyber Security Process - Security Incident Management;
- AE-PR-034 External and Internal Communication;
- AE-PR-046 Intercompany Transfer Pricing Policy;
- AE-PR-047 Management of Inside Information;
- AE-PR-048 Information Classification;
- AE-PR-050 Intellectual Property Process;
- AE-PR-051 Intellectual Property Contitution Process;
- AE-PR-057 IT Access Management;
- AE-PR-058 IT Security Operating Handbook;
- AE-PR-069 Intellectual Property Transfer process – Manage Non-Disclosure Agreements;
- AE-PR-070 Intellectual Property Transfer process – Manage Collaborative Research;

- AE-PR-075 Independent Auditors management;
- AE-IN-006 Passive Payments – Operational Checks Against Supplier Data Cyber;
- AE-IN-016 Guidelines for the management of company phone.

PARTE SPECIALE "C"

Delitti relativi alla Salute e Sicurezza sul Lavoro

C.1 LA TIPOLOGIA DEI DELITTI RELATIVI ALLA SALUTE ED ALLA SICUREZZA SUL LAVORO (Art. 25-*septies* del Decreto)

La Società è impegnata a tutelare la salute e sicurezza dei lavoratori approntando le misure necessarie ed opportune alla stregua delle migliori conoscenze tecniche e scientifiche per la conformità delle attività lavorative ai più elevati standard di sicurezza ed igiene, diffondendo e consolidando la cultura della sicurezza e salute nei luoghi di lavoro e promuovendo comportamenti responsabili da parte di tutti i dipendenti e collaboratori.

L'art. 25-*septies* del decreto legislativo 231/2001 nella attuale formulazione, prevede sanzioni amministrative per le persone giuridiche nel caso di omicidio o lesioni colpose commessi con violazione delle norme in materia di sicurezza e salute nel lavoro. In particolare, il testo dell'art. 25-*septies* attualmente recita: "*Omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro".*

1. In relazione al delitto di cui all'articolo 589 del codice penale, commesso con violazione dell'articolo 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 123 del 2007 in materia di salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura pari a 1.000 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.

2. Salvo quanto previsto dal comma 1, in relazione al delitto di cui all'articolo 589 del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non inferiore a 250 quote e non superiore a 500 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.

3. In relazione al delitto di cui all'articolo 590, terzo comma, del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non superiore a 250 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non superiore a sei mesi"

Si riporta di seguito il testo dei reati richiamati dall'art. 25-*septies* del D.lgs 231/2001.

C.1.1 OMICIDIO COLPOSO (ART. 589 C.P.)

"*Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni.*

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

Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici".

C.1.2 LESIONI PERSONALI COLPOSE (ART. 590, COMMA 3, C.P.)

"*Chiunque cagiona ad altri, per colpa, una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309"*.

Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 a euro 619; se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309 a euro 1239.

Se i fatti di cui al precedente capoverso sono commessi 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 euro 500 a euro 2000; e la pena per 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.

Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale".

La lesione è considerata grave (art. 583 co. 1, c.p.) nei seguenti casi:

"1) *se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;*

2) se il fatto produce l'indebolimento permanente di un senso o di un organo."

La lesione è considerata invece gravissima se dal fatto deriva (art. 583 co. 2, c.p.):

"*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".

L'elemento comune alle fattispecie di reato è la colpa, così definita dall'art. 43 del c.p.:

"*Il delitto è doloso, o secondo l'intenzione, quando l'evento dannoso o pericoloso, che è il risultato dell'azione od omissione e da cui la legge fa dipendere l'esistenza del delitto, è dall'agente preveduto e voluto come conseguenza della propria azione od omissione*; *è preterintenzionale, o oltre l'intenzione, quando dall'azione od omissione deriva un evento dannoso o pericoloso più grave di quello voluto dall'agente; è colposo, o contro l'intenzione, quando l'evento, anche se preveduto, non è voluto dall'agente e si verifica a causa di negligenza o imprudenza o imperizia, ovvero per inosservanza di leggi, regolamenti, ordini o discipline [...]*".

Le due fattispecie delittuose assumono rilevanza in questa sede in quanto siano conseguenze di violazioni alle norme di prevenzione degli infortuni e delle malattie nei luoghi di lavoro, norme contenute nel decreto legislativo 81/08 (e sue modificazioni) che, quindi, costituisce il riferimento per la valutazione della colpa. In particolare, per fissare obblighi e responsabilità dal momento che nella maggior parte dei casi la colpa viene individuata nella omissione di un comportamento doveroso proprio sulla base di quelle norme.

Poiché l'interesse o il vantaggio della Società rappresentano il fondamento della sua responsabilità, la contraddizione fra l'involontarietà dell'evento infortunistico e la necessità dell'interesse è stata risolta dalla giurisprudenza ravvisando l'interesse o il vantaggio per la Società non nell'evento ma nella condotta colposa del responsabile, individuando di volta in volta il vantaggio nel risparmio di tempi o di risorse nel corso dell'esecuzione del lavoro.

Particolare rilevanza assume la irrogazione di sanzioni interdittive sempre disposta in caso di condanna.

C.2 AREE A RISCHIO

Ai fini della disciplina della presente sezione del Modello vengono assunte quali "aree a rischio" tutte quelle nelle quali personale di Ansaldo Green Tech esegue, sovrintende, dirige o coordina l'attività lavorativa secondo quanto previsto dalle norme in materia, dall'organizzazione aziendale e quanto in concreto avviene.

Il "livello di rischio" dei dipendenti è significativamente diverso, così come è evidente che nell'ambito dello stesso reparto possono coesistere diverse mansioni con altrettante diversità anche nel "livello di rischio". Su tali basi è stata sviluppata l'organizzazione di sicurezza e vengono redatti i documenti relativi, *in primis*, il Documento di valutazione dei rischi secondo quanto previsto dal D.lgs. 81/08.

C.2.1 L'ORGANIZZAZIONE

La Società, con la sua organizzazione assicura l'adozione e la concreta attuazione di un sistema aziendale in linea con quanto previsto dall'art. 30 del D.lgs. 81/08.

Il sistema nel suo complesso ha ottenuto, e mantiene, la certificazione di conformità alla norma ISO 45001:2018 che si presume conforme al dettato normativo, come previsto dal comma 5 dell'art. 30 del D.lgs. 81/08.

Tenuto conto della complessità dell'Azienda, considerata come unica Unità Produttiva, è stato adottato un sistema di deleghe, subdeleghe e lettere di responsabilità con il quale sono state precisate le attribuzioni e competenze di ciascuno in modo che datore di lavoro, dirigenti, preposti e lavoratori siano ciascuno edotto degli obblighi in materia di tutela della sicurezza e della salute nei luoghi di lavoro che la legge riserva loro in relazione ai compiti e alle funzioni attribuite.

Un organigramma di tale ripartizione di funzioni è allegato al presente Modello (allegato VII) e custodito nell'archivio dell'Organismo di Vigilanza.

La Società si avvale, inoltre, del supporto della Strutture di Ansaldo Energia, competenti in materia di ambiente e di salute e sicurezza sul lavoro.

C.2.2 LA DOCUMENTAZIONE DI SICUREZZA

Ogni attività di lavoro è assistita dai documenti di sicurezza previsti dalla legge, ciascuno specifico in relazione alle attività da svolgere, ed in particolare da:

- Documento di Valutazione dei Rischi (DVR): documento all'interno del quale il datore di lavoro, ai sensi dell'art. 17 e con le modalità di cui agli artt. 28 e 29 del D.Lgs. 81/08, ha formalizzato la valutazione di tutti i rischi per la sicurezza e salute dei lavoratori presenti nell'ambito dell'organizzazione e individuate le misure di prevenzione e protezione adeguate, ed elaborato il programma delle misure atte a garantire nel tempo il miglioramento dei livelli di sicurezza e salute. Il Documento viene conservato presso il Servizio Prevenzione e Protezione e una copia è allegata al presente Modello (allegato VIII);
- Documento Unico di Valutazione dei rischi da Interferenze (DUVRI), talora anche Documento di valutazione dei rischi da Interferenze Standard: documento emesso dal datore di lavoro o dal dirigente delegato in ottemperanza all'art. 26 comma 3

del D.Lgs. 81/08 per promuovere il coordinamento e la cooperazione fra le imprese appaltanti e appaltatrici per prevenire i rischi da interferenze;

- Piano di sicurezza e Coordinamento (PSC): documento redatto dal Coordinatore della progettazione nel caso di opere eseguite in cantieri temporanei o mobili;
- Piano Operativo di Sicurezza (POS): documento redatto dal datore di lavoro dell'impresa esecutrice nei lavori eseguiti in cantieri temporanei o mobili;
- Piano di Emergenza (PEI): documento emesso dal datore di lavoro che individua le tipologie di emergenza e definisce le modalità di preparazione e risposta alle emergenze.

All'apertura di ogni Cantiere in cui sono presenti lavoratori di Ansaldo Green Tech o in cui Ansaldo Green Tech è appaltatrice di lavori, viene redatto il corrispettivo piano di sicurezza in ottemperanza a quanto richiesto dalle norme.

Tutti i soggetti con posizione di garanzia hanno capacità professionale, esperienza, competenza e poteri adeguati alle funzioni che sono loro attribuite e ciascuno ha, come esplicitato nei documenti a lui diretti, il dovere di sospendere il lavoro o interrompere l'attività del lavoratore ove vengano meno le condizioni di sicurezza o comunque venga attuato un comportamento non conforme alle indicazioni di sicurezza impartite.

C.2.3 I SOGGETTI

Secondo quanto dispongono gli articoli 2, 3, 16, 17, 18, 19, 20, 22, 23, 24, 25, 33 del D.Lgs. 81/08 i soggetti interessati sono:

- il **datore di lavoro** è il soggetto che, in base al tipo e l'assetto dell'organizzazione, ne ha la responsabilità in quanto esercita i poteri decisionali e di spesa. Il Consiglio di Amministrazione della Società ha deliberato di individuare, in forza dei poteri conferiti, come datore di lavoro nell'ambito della Società Ansaldo Green Tech considerata unica Unità Produttiva, l'Amministratore Delegato che esercita i suoi poteri con la collaborazione di dirigenti e preposti ai quali ha provveduto a delegare quanto delegabile e a conferire le funzioni e i poteri necessari in considerazione della loro idoneità tecnica e professionale;
- i **dirigenti**, che esercitano le funzioni ad essi delegate o comunque ad essi attribuite secondo le competenze assegnate in conformità di quanto stabilito dall'art. 16 e dall'art. 18 del D.Lgs. 81/08;
- i **preposti**, che secondo le loro attribuzioni e competenze hanno gli obblighi previsti dall'art. 19 del D.Lgs. 81/08;
- i **lavoratori**, cui spetta adempiere agli obblighi di cui all'art. 20 del D.Lgs. 81/08;
- i **progettisti**, cui spetta l'obbligo di rispettare i principi generali di prevenzione come da art. 22 del D.Lgs. 81/08;
- i **lavoratori distaccati**, nelle ipotesi di distacco di lavoratori la Società adotta adeguate misure di sicurezza in adempimento di quanto previsto al comma 6 dell'art. 3 del D.Lgs. 81/08, prevedendo che gli obblighi di sicurezza siano a carico del distaccatario, fatti salvi gli obblighi a carico del distaccante di informare e formare il lavoratore sui rischi tipici generalmente connessi allo svolgimento delle mansioni per le quali viene distaccato;
- i **fabbricanti** e i **fornitori**, cui spetta adempiere agli obblighi di cui all'art. 23 del D.Lgs. 81/08;

- gli **installatori e montatori** di impianti, attrezzature di lavoro o altri mezzi tecnici, i quali per la parte di loro competenza, devono attenersi alle norme di salute e sicurezza sul lavoro, nonché alle istruzioni fornite dai rispettivi fabbricanti secondo quanto disposto dall'art. 24 del D.Lgs 81/08;
- il **medico competente**, cui spetta adempiere agli obblighi di cui all'art. 25 del D.Lgs. 81/08;
- i **componenti del servizio di prevenzione e protezione**, i quali provvedono ad assolvere i compiti di cui all'art. 33 del D.Lgs. 81/08;
- gli **addetti alle emergenze**, 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.

La linea operativa si avvale del supporto tecnico delle altre competenze aziendali e specificatamente del servizio di prevenzione e protezione, istituito all'interno dell'Azienda con i compiti previsti dalla legge in particolare dall'art. 33 del D.Lgs. 81/08.

Il medico competente, sulla base dell'esito della valutazione dei rischi, ha elaborato un programma di sorveglianza sanitaria che aggiorna in ragione di eventuali modificazioni dei cicli produttivi ed esprime i giudizi di idoneità o meno alla mansione specifica. Il medico competente sulla base dei fattori di rischio per la salute stabilisce la periodicità e la tipologia degli accertamenti clinici, strumentali e di laboratorio che devono essere svolti.

È stato eletto il rappresentante dei lavoratori per la sicurezza che viene consultato nei casi previsti dalla legge e riceve le informazioni previste.

Al sistema di deleghe e subdeleghe è stata data adeguata pubblicità all'interno e all'esterno dell'Azienda. Altrettanta pubblicità all'interno è stata data al Documento redatto a seguito della valutazione dei rischi da parte del datore di lavoro. Il D.V.R. munito di data certa, sottoscritto dal responsabile del servizio di prevenzione e protezione, dal medico competente, dal rappresentante dei lavoratori per la sicurezza, viene conservato, come gli altri documenti rilevanti per salute e sicurezza negli ambienti di lavoro, nel rispetto delle previsioni di cui all'art. 53 del D.lgs. 81/08.

C.2.4 FORMAZIONE

La Società assicura che ciascun lavoratore riceva adeguata formazione, informazione e addestramento secondo quanto disposto dal D.Lgs. 81/08 e dalla normativa tecnica di settore, in particolare:

- al momento dell'assunzione;
- in occasione del trasferimento o di un cambio di mansioni;
- in occasione della massa in esercizio di nuove attrezzature, macchinari o impianti o dell'utilizzo di nuove sostanze.

Poiché la Società ha ritenuto di individuare la lingua italiana come lingua di lavoro per tutti, particolare cura viene adottata per l'informazione e formazione dei lavoratori stranieri ove presenti.

C.3 PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITA' A RISCHIO

C.3.1 PRINCIPI DI COMPORTAMENTO DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Ansaldo Green Tech opera con un sistema interno di gestione della prevenzione e protezione dei lavoratori sui luoghi di lavoro, conforme alle vigenti norme in materia e certificato ISO 45001:2018.

Gli elementi del sistema di gestione della sicurezza tengono conto della specificità della Società che attraverso un'organizzazione complessa ed articolata di dirigenti di vario livello e di preposti, svolge attività:

- nella Sede di Genova;
- nei cantieri esterni di varia complessità e durata.

Poiché il principio ispiratore del D.Lgs. 81/08 si può sintetizzare attraverso la convinzione che la sicurezza sul lavoro si ottiene responsabilizzando tutti coloro (dipendenti e non) che operano all'interno delle aree aziendali e/o delle aree all'interno delle quali prestano la loro opera lavorativa, destinatari della presente Parte Speciale "C" sono tutti i lavoratori della Società, ciascuno in base alle proprie attribuzioni e competenze, nonché tutti i soggetti terzi a vario titolo coinvolti dall'attività aziendale.

La presente Parte Speciale prevede l'espresso divieto a tutti i lavoratori di porre in essere, o anche tollerare che altri pongano in essere, comportamenti:

- tali da integrare le fattispecie di reato considerate dall'art 25-*septies*;
- che possano compromettere i presidi di salute e sicurezza adottati dalla società favorendo potenzialmente la commissione dei reati di omicidio colposo e lesioni personali colpose;
- non conformi alle procedure aziendali o, comunque, non in linea con i principi espressi dal presente Modello e dal Codice Etico in materia di salute, sicurezza e igiene dei luoghi di lavoro
- che siano tesi ad impedire, intralciare, eludere, compromettere gli esiti dell'attività di vigilanza e controllo in materia di salute e sicurezza sul lavoro sia che essa sia svolta per conto della Società sia che sia svolta da autorità di controllo.

Ai collaboratori esterni ed appaltatori sono stati estesi obblighi e divieti, per quanto di loro competenza, attraverso apposite clausole contrattuali.

Nell'ambito del sistema interno di gestione della prevenzione e protezione dei lavoratori sui luoghi di lavoro, come da disposizioni di legge e norma tecnica di settore, spetta al **datore di lavoro**:

- organizzare e gestire la Società secondo principi e criteri conformi alle norme di legge, ai principi del presente documento e del codice etico;
- valutare i rischi per la sicurezza e salute dei lavoratori ed elaborare il "Documento sulla valutazione dei rischi" previsto dal T.U. con le modalità ivi prescritte;
- designare il responsabile del servizio di prevenzione e protezione dai rischi;
- delegare o affidare ai dirigenti i compiti e le responsabilità in relazione alle loro aree di competenza, munendoli di tutti i poteri di organizzazione, gestione e controllo richiesti dalle funzioni delegate o assegnate.

È fatto obbligo al **datore di lavoro,** ai **dirigenti delegati**, nonché ai **dirigenti,** in base alle funzioni conferite, nell'ambito delle loro aree di competenza e avvalendosi dei

soggetti loro subordinati, nonché delle altre strutture o risorse aziendali per loro disponibili, di garantire il rispetto degli obblighi previsti dal D. Lgs 81/08 e dalla normativa tecnica di settore e, in particolare, di:

- nominare il medico competente;
- designare preventivamente i lavoratori 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;
- individuare i preposti per l'effettuazione delle attività di vigilanza;
- nell'affidare i compiti ai lavoratori, tenere conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute ed alla sicurezza;
- fornire ai lavoratori i necessari ed idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione ed il medico competente;
- prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico;
- richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione;
- inviare i lavoratori alla visita medica entro le scadenze previste dal programma di sorveglianza sanitaria e richiedere al medico competente l'osservanza degli obblighi previsti a suo carico dal D.Lgs. 81/08 e s.m.i.;
- nei casi di sorveglianza sanitaria di cui all'articolo 41 del D. Lgs 81/08, comunicare tempestivamente al medico competente la cessazione del rapporto di lavoro;
- adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
- informare prima possibile i lavoratori esposti al rischio di un pericolo grave ed immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
- adempiere agli obblighi di informazione, formazione e addestramento di cui agli articoli 36 e 37 del T.U. e ad altri obblighi specifici di informazione, formazione e addestramento previsti dal D. Lgs 81/08 e s.m.i. e dalla normativa tecnica di settore;
- astenersi dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato;
- consentire ai lavoratori di verificare, mediante il rappresentante dei lavoratori per la sicurezza, l'applicazione delle misure di sicurezza e di protezione della salute;
- consegnare tempestivamente al rappresentante dei lavoratori per la sicurezza, su richiesta di questi e per l'espletamento della sua funzione, copia del documento di cui all'articolo 17, comma 1, lettera a), nonché consentire al medesimo rappresentante di accedere ai dati di cui alla lettera q) del D.Lgs. 81/08 e s.m.i;
- in caso di affidamento di lavori, servizi e forniture all'impresa appaltatrice o a lavoratori autonomi:

- verificare l'idoneità tecnico professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori, ai servizi e alle forniture da affidare in appalto o mediante contratto d'opera o di somministrazione secondo i criteri dettati dalla norma;
- elaborare il documento di cui all'articolo 26, comma 3 del D.Lgs. 81/08 e s.m.i ove ne ricorra l'obbligo e, su richiesta di questi e per l'espletamento della sua funzione, consegnarne tempestivamente copia al rappresentante dei lavoratori per la sicurezza;
- garantire, nell'ambito dei cantieri temporanei o mobili, il rispetto delle prescrizioni applicabili di cui al titolo IV del D.Lgs. 81/08 e s.m.i.;

- prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno verificando periodicamente la perdurante assenza di rischio;
- comunicare in via telematica all'INAIL, nonché per suo tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'articolo 8, entro 48 ore dalla ricezione del certificato medico, a fini statistici e informativi, i dati e le informazioni relativi agli infortuni sul lavoro che comportino l'assenza dal lavoro di almeno un giorno, escluso quello dell'evento e, a fini assicurativi, quelli relativi agli infortuni sul lavoro che comportino un'assenza al lavoro superiore a tre giorni;
- consultare il rappresentante dei lavoratori per la sicurezza nelle ipotesi di cui all'articolo 50 del D.Lgs. 81/08 e s.m.i.;
- adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, adeguate alla natura dell'attività, alle dimensioni dell'azienda o dell'unità produttiva, e al numero delle persone presenti;
- nell'ambito dello svolgimento di attività in regime di appalto e di subappalto, munire i lavoratori di apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore, l'indicazione del datore di lavoro e comunicare il nominativo del o dei preposti individuati per l'attività appaltata;
- convocare la riunione periodica di cui all'articolo 35 del D.Lgs. 81/08 e s.m.i.;
- aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;
- comunicare in via telematica all'INAIL, nonché per suo tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'art. 8 del D.Lgs. 81/08, in caso di nuova elezione o designazione, i nominativi dei rappresentanti dei lavoratori per la sicurezza;
- vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità;
- vigilare in ordine all'adempimento degli obblighi da parte di preposti, lavoratori, progettisti, fabbricanti e fornitori, installatori e medico competente.

Ai **preposti**, nell'ambito delle loro attribuzioni e competenze, è fatto obbligo di:

- sovrintendere e vigilare sulla osservanza da parte dei singoli lavoratori dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione

individuale messa a loro disposizione e, in caso di rilevazione di comportamenti non conformi alle disposizioni e istruzioni impartite dal datore di lavoro e dai dirigenti ai fini della protezione collettiva e individuale, intervenire per modificare il comportamento non conforme, fornendo le necessarie indicazioni di sicurezza. In caso di mancata attuazione delle disposizioni impartite o di persistenza nell'inosservanza interrompere l'attività del lavoratore e informare i superiori diretti;

- verificare affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;
- richiedere l'osservanza delle misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
- informare prima possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
- astenersi dal richiedere ai lavoratori, di proseguire la loro attività in una situazione di lavoro in cui persiste un pericolo grave ed immediato;
- segnalare tempestivamente al datore di lavoro o al dirigente sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro, delle quali venga a conoscenza sulla base della formazione ricevuta;
- in caso di rilevazione di deficienze dei mezzi e delle attrezzature di lavoro e di ogni condizione di pericolo rilevata durante la vigilanza, se necessario, interrompere temporaneamente l'attività e comunque segnalare tempestivamente al datore di lavoro e al dirigente le non conformità;
- frequentare appositi corsi di formazione, secondo quanto previsto dall'articolo 37 del D.Lgs. 81/08 e s.m.i.

Ai singoli **lavoratori** è fatto obbligo di:

- contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;
- osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;
- utilizzare correttamente i macchinari, le apparecchiature, gli utensili, le sostanze ed i preparati pericolosi, i mezzi di trasporto, le altre attrezzature di lavoro, nonché i dispositivi di sicurezza e di protezione (DPI) messi a loro disposizione conformemente all'informazione e formazione ricevute e all'addestramento eventualmente organizzato;
- aver cura delle attrezzature di lavoro e dei DPI messi a loro disposizione, non apportando modifiche di loro iniziativa e segnalando immediatamente al datore, all'RSPP o al preposto qualsiasi difetto od inconveniente rilevato;
- segnalare immediatamente al datore di lavoro, al dirigente, al preposto o al servizio di prevenzione e protezione le deficienze dei mezzi e dei dispositivi citati in precedenza, nonché le altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze e pericoli, dandone notizia al rappresentante dei lavoratori per la sicurezza;

- non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza, ovvero che possono compromettere la sicurezza propria e di altri lavoratori;
- partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro;
- sottoporsi ai controlli sanitari previsti dal D.Lgs. 81/08 e s.m.i. o comunque disposti dal medico competente.

Al **servizio di prevenzione e protezione,** utilizzato dal datore di lavoro, dai dirigenti dai preposti e dai lavoratori è fatto espresso obbligo di attuare i compiti indicati all'art. 33 del T.U. e quindi, con la collaborazione del datore di lavoro dei dirigenti e dei preposti, provvedere:

- all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto delle norme vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
- ad elaborare, per quanto di competenza, le misure preventive e protettive di cui all'articolo 28, comma 2 del T.U., ed i sistemi di controllo di tali misure;
- ad elaborare le procedure di sicurezza per le varie attività aziendali;
- a proporre i programmi di informazione e formazione dei lavoratori;
- a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica di cui all'articolo 35 del T.U.;
- a fornire ai lavoratori le informazioni di cui all'articolo 36 del T.U.

Al **medico competente** è fatto obbligo di:

- collaborare con il datore di lavoro e con il servizio di prevenzione e protezione alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della sorveglianza sanitaria, alla predisposizione della attuazione delle misure per la tutela della salute e della integrità psico-fisica dei lavoratori, all'attività di formazione e informazione nei confronti dei lavoratori, per la parte di competenza, e alla organizzazione del servizio di primo soccorso considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro;
- programmare ed effettuare la sorveglianza sanitaria di cui all'articolo 41 D.Lgs. 81/08, attraverso protocolli sanitari definiti in funzione dei rischi specifici e tenendo in considerazione gli indirizzi scientifici più avanzati;
- in occasione della visita medica preventiva o della visita medica preventiva in fase preassuntiva di cui all'articolo 41 del D.Lgs 81/08 e s.m.i., richiedere al lavoratore di esibire copia della cartella sanitaria e di rischio rilasciata alla risoluzione del precedente rapporto di lavoro e valutarne il contenuto ai fini della formulazione del giudizio di idoneità, salvo che ne sia oggettivamente impossibile il reperimento;
- emettere, sulla base dei risultati della sorveglianza sanitaria, il giudizio di idoneità del lavoratore alla mansione specifica (con o senza prescrizione) stabilendo, laddove necessario e tecnicamente possibile, i limiti di esposizione;
- istituire, aggiornare e custodire, sotto la propria responsabilità, una cartella sanitaria e di rischio per ogni lavoratore sottoposto a sorveglianza sanitaria che

provvederà a consegnare al datore di lavoro in caso di cessazione dall'incarico e al lavoratore alla cessazione del rapporto di lavoro;

- fornire informazioni ai lavoratori sul significato della sorveglianza sanitaria cui sono sottoposti e, nel caso di esposizione ad agenti con effetti a lungo termine, sulla necessità di sottoporsi ad accertamenti sanitari anche dopo la cessazione dell'attività che comporta l'esposizione a tali agenti. A richiesta, ha l'obbligo di fornire informazioni analoghe ai rappresentanti dei lavoratori per la sicurezza;
- informare ogni lavoratore interessato dei risultati della sorveglianza sanitaria e, a richiesta dello stesso, rilasciargli copia della documentazione sanitaria;
- comunicare per iscritto, in occasione delle riunioni periodiche, al datore di lavoro, al responsabile del servizio di prevenzione protezione dai rischi, ai rappresentanti dei lavoratori per la sicurezza, i risultati anonimi collettivi della sorveglianza sanitaria effettuata e fornire indicazioni sul significato di detti risultati ai fini della attuazione delle misure per la tutela della salute e della integrità psico-fisica dei lavoratori;
- visitare gli ambienti di lavoro almeno una volta all'anno o a cadenza diversa che stabilisce in base alla valutazione dei rischi; l'indicazione di una periodicità diversa dall'annuale deve essere comunicata al datore di lavoro ai fini della sua annotazione nel documento di valutazione dei rischi;
- partecipare alla programmazione del controllo dell'esposizione dei lavoratori i cui risultati gli sono forniti con tempestività ai fini della valutazione del rischio e della sorveglianza sanitaria;
- in caso di impedimento per gravi e motivate ragioni, comunicare per iscritto al datore di lavoro il nominativo di un sostituto, in possesso dei requisiti di cui all'articolo 38 del D. Lgs 81/08 e s.m.i., per l'adempimento degli obblighi di legge durante il relativo intervallo temporale specificato.

Ai **progettisti dei luoghi e dei posti di lavoro e degli impianti** è fatto obbligo di:

- rispettare i principi generali di prevenzione in materia di salute e sicurezza sul lavoro al momento delle scelte progettuali e tecniche;
- scegliere attrezzature, componenti e dispositivi di protezione rispondenti alle disposizioni legislative e regolamentari in materia.

Ai **fabbricanti e fornitori** è fatto divieto di vendere, noleggiare, concedere in uso attrezzature di lavoro, dispositivi di protezione individuali ed impianti non rispondenti alle disposizioni legislative e regolamentari vigenti in materia di salute e sicurezza sul lavoro. In caso di locazione finanziaria di beni assoggettati a procedure di attestazione alla conformità, gli stessi dovranno essere accompagnati, a cura del concedente, dalla relativa documentazione.

Agli **installatori e montatori** di impianti, attrezzature di lavoro o altri mezzi tecnici, per la parte di loro competenza, è fatto obbligo di attenersi alle norme di salute e sicurezza sul lavoro, nonché alle istruzioni fornite dai rispettivi fabbricanti.
Gli obblighi relativi a progettisti, fabbricanti, fornitori, installatori e montatori sono applicabili sia qualora il ruolo sia assolto da personale di Ansaldo Green Tech, sia qualora il ruolo sia assolto da soggetti terzi che erogano tale tipo di servizio alla Società o per conto della stessa.

I Destinatari della presente sezione devono esercitare un controllo continuo e puntuale teso ad evidenziare rischi che potrebbero comportare la realizzazione dei reati indicati nell'art. 25-*septies* ed, in generale, qualunque situazione che possa comportare un pericolo

per l'igiene, la salute e la sicurezza dei lavoratori e di tutti i soggetti comunque presenti nelle aree della Società.

Le attività svolte da Ansaldo Green Tech nelle aree potenzialmente a rischio sono regolamentate da procedure interne rispondenti ai criteri imposti dal Decreto.

Il complesso delle procedure scritte è disponibile presso il servizio di prevenzione e protezione e viene diffuso all'interno della Società presso tutti i soggetti interessati. Copia delle indicate procedure è inserita nei siti dedicati dell'Intranet aziendale, accessibile a tutti gli utenti della Società.

Le informazioni e disposizioni verbali vengono trasferite da dirigenti e preposti in modo non formalizzato, direttamente sul posto di lavoro nel corso dello svolgimento dell'attività lavorativa, avendo cura che siano ben comprese da coloro che le ricevono.

Le attività connesse con il presente profilo di rischio devono essere gestite nel rispetto delle norme applicabili e del sistema normativo aziendale che, oltre a inglobare i principi espressi nel Codice Etico e gli obblighi e divieti sopra evidenziati, prevede quanto segue:

- deleghe di responsabilità e nomine/designazioni delle funzioni rilevanti per la sicurezza. In tema di deleghe di responsabilità e nomine/designazioni delle funzioni rilevanti per la sicurezza viene garantito che:
  - le nomine e le designazioni dei soggetti responsabili in materia di salute e sicurezza sul lavoro sono adeguatamente formalizzate, con firma da parte dei soggetti incaricati, e pubblicizzate all'interno della Società e all'esterno ove richiesto;
  - il sistema delle deleghe, nomine e designazioni è coerente con l'evoluzione dell'organizzazione societaria;
  - le Funzioni incaricate di compiti rilevanti per la sicurezza sono dotate dei poteri di organizzazione, gestione e controllo, ed eventualmente di spesa, adeguati alla struttura e alla dimensione dell'organizzazione e alla natura dei compiti assegnati in considerazione anche della possibilità del verificarsi di casi di urgenze non prevedibili né rinviabili;
  - sono definite le responsabilità e le modalità operative atte ad assicurare la verifica del possesso e del mantenimento dei requisiti di competenza e professionalità richiesti per le figure rilevanti per la sicurezza, con particolare riferimento ai requisiti di aggiornamento periodico obbligatori;
- rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici. Sono formalizzati ruoli, responsabilità e modalità operative atte a garantire:
  - idonei flussi informativi tra il servizio SPP e le Funzioni a vario titolo coinvolte nel processo di approvvigionamento di beni e servizi, al fine di assicurare una gestione degli acquisti che tenga conto dell'esigenza di valutare preliminarmente i rischi che possono essere introdotti nella Società in fase di approvvigionamento;
  - il rispetto dei principi generali di prevenzione in materia di salute e sicurezza sul lavoro al momento delle scelte progettuali e tecniche, nella scelta di attrezzature, componenti e dispositivi di protezione e nella gestione di sostanze e preparati pericolosi;
  - il mantenimento nel tempo degli standard tecnico-strutturali di legge, di attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici tramite

adeguanti interventi di manutenzione ordinaria e straordinaria e verifiche periodiche che tengano conto di quanto previsto dalla norma tecnica di settore, nonché delle informazioni contenute nei libretti d'uso e manutenzione delle singole apparecchiature, attrezzature, impianti;

- valutazione dei rischi (DVR) e predisposizione delle misure di prevenzione e protezione;

- gestione dei contratti d'appalto, d'opera o di somministrazione e della sicurezza nei cantieri temporanei o mobili: sono formalizzati ruoli, responsabilità e modalità operative atte ad assicurare:
  - la verifica dell'idoneità tecnica e professionale di fornitori e appaltatori in conformità con quanto previsto dal D.Lgs. 81/08 e s.m.i.;
  - l'informazione, ai suddetti fornitori e appaltatori, sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate;
  - l'elaborazione del Documento Unico di Valutazione dei Rischi per Interferenza (DUVRI), ove ne ricorra l'obbligo ai sensi dell'art. 26 del D.Lgs 81/08 e s.m.i., in cui sono riportate le misure adottate per eliminare o ridurre al minimo i rischi da interferenze. In caso di redazione del documento esso è allegato al contratto di appalto o di opera e ne è garantito l'adeguamento in funzione dell'evoluzione dei lavori, servizi e forniture;
  - l'indicazione, nei singoli contratti di subappalto, di appalto e di somministrazione:
    - dei costi delle misure adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi in materia di salute e sicurezza sul lavoro derivanti dalle interferenze delle lavorazioni;
    - di specifiche clausole contrattuali con riferimento ai requisiti e comportamenti richiesti in relazione alla tipologia di fornitura/servizio reso, ed alle sanzioni previste per il loro mancato rispetto fino alla risoluzione del contratto stesso;
    - di specifiche clausole contrattuali con riferimento all'individuazione del personale che svolge la funzione di preposto;
  - l'assolvimento di tutti gli obblighi di cui al titolo IV° del D.Lgs. 81/08 e s.m.i. (cantieri temporanei o mobili), ove applicabile. In particolare, per il caso in cui Ansaldo Green Tech sia committente di lavori ai quali si applicano le disposizioni sui cantieri temporanei di cui agli artt. 88 e segg. del D.Lgs. 81/08 e s.m.i. viene designato il responsabile dei lavori, nella fase di progettazione e di esecuzione dell'opera, il quale provvede alla nomina del coordinatore cui spetta di predisporre il piano di sicurezza e di coordinamento ed il fascicolo tecnico in conformità a quanto previsto dall'art. 100 del D.Lgs. 81/08 e, nella fase di esecuzione, di controllare l'adeguatezza del piano allo sviluppo dei lavori.

    Allo stesso coordinatore, nella fase della esecuzione, spetta di promuovere le opportune azioni di cooperazione e di coordinamento, la vigilanza sulla osservanza dei piani da parte delle imprese appaltatrici, nonché di proporre o di adottare le eventuali sanzioni contrattuali verso le imprese inadempienti.

    Per il caso in cui Ansaldo Green Tech sia appaltatrice o affidataria di lavori soggetti alla citata disciplina sui cantieri temporanei, viene garantita l'osservanza degli obblighi previsti dalla legge in materia attraverso la redazione

dei Piani Operativi per la Sicurezza di competenza, verificando la congruenza dei Piani Operativi dei subappaltatori con il Piano Operativo di Ansaldo Green Tech e con il Piano di Sicurezza del Committente.

Prima dell'inizio dei lavori e nel corso di essi, sono previste apposite riunioni di coordinamento e cooperazione condotte con la partecipazione degli appaltatori e fornitori ed, eventualmente, del servizio di prevenzione e protezione.

- Appaltatori, fornitori e lavoratori autonomi hanno l'obbligo, sotto pena di sanzioni disciplinari, di osservare le regole operative afferenti la salute e la sicurezza nei luoghi di lavoro stabilite nel presente Modello, nelle clausole contrattuali, nei documenti di sicurezza, nelle disposizioni relative ai rischi interferenziali. Viene richiesto agli appaltatori di assumere analoghe iniziative volte a trasmettere tutta la documentazione, le informazioni e gli obblighi relativi, verso i subappaltatori;

- riunioni periodiche della sicurezza e consultazione dei RLS: sono formalizzati ruoli, responsabilità e modalità operative atte ad assicurare:
  - la consultazione del RLS in tutti i casi previsti dall'art. 50 del D.Lgs. 81/08 garantendone adeguata tracciabilità;
  - lo svolgimento con periodicità almeno annuale di una riunione cui partecipano il datore di lavoro o un suo rappresentante, il responsabile del servizio di prevenzione e protezione, il medico competente, il rappresentante dei lavoratori per la sicurezza. Nel corso della riunione, di cui si conserva adeguata tracciabilità, vengono trattati almeno i seguenti argomenti:
    - il documento di valutazione dei rischi;
    - l'andamento degli infortuni e delle malattie professionali e della sorveglianza sanitaria;
    - i criteri di scelta, le caratteristiche tecniche e l'efficacia dei dispositivi di protezione individuale;
    - i programmi di informazione, formazione ed addestramento di dirigenti, preposti, lavoratori ai fini della sicurezza e della protezione della loro salute.

    La riunione ha altresì luogo in occasione di eventuali significative variazioni delle condizioni di esposizione al rischio, compresa la programmazione e l'introduzione di nuove tecnologie che hanno riflessi sulla sicurezza e salute dei lavoratori.

- formazione, informazione e addestramento: sono formalizzati ruoli, responsabilità e modalità operative atte ad assicurare:
  - un'adeguata formazione, informazione, addestramento dei lavoratori in conformità a quanto stabilito dagli artt. 36 e 37 del D.lgs. 81/08 e s.m.i. e dagli Accordi in sede di Conferenza permanente per i rapporti tra lo Stato e le Regioni;
  - il possesso dei necessari requisiti da parte dei formatori della sicurezza in accordo a quanto definito dal Decreto interministeriale del 6 marzo 2013 e s.m.i.;
  - la tracciabilità dei processi di formazione, informazione, addestramento e verifica periodica dell'apprendimento;
  - un'adeguata informazione ai fornitori e agli appaltatori riguardo ai rischi specifici presenti, nonché alle regole comportamentali e di controllo adottate

dalla Società, definite nel presente documento e nel sistema normativo aziendale.

Nel pianificare le attività di formazione, informazione, addestramento è fatto obbligo di considerare l'eventuale presenza di lavoratori in distacco o distaccati, personale interinale, personale che effettua prestazioni occasionali di tipo accessorio.

Nello specifico è previsto che ciascun lavoratore riceva una adeguata *informazione*:

- sui rischi per la salute e sicurezza sul lavoro connessi alla attività della impresa in generale;
- sulle procedure che riguardano il primo soccorso, la lotta antincendio, l'evacuazione dei luoghi di lavoro;
- sui nominativi dei lavoratori incaricati di applicare le misure di primo soccorso e antincendio;
- sui nominativi del responsabile e degli addetti del servizio di prevenzione e protezione e del medico competente;
- sui rischi specifici cui è esposto in relazione all'attività svolta, sulle norme di sicurezza e le disposizioni aziendali in materia;
- sui pericoli connessi all'uso delle sostanze e dei preparati pericolosi sulla base delle schede dei dati di sicurezza previste dalle norme vigenti e dalle norme di buona tecnica;
- sulle misure e le attività di protezione e prevenzione adottate.

Nello specifico è previsto che ciascun lavoratore riceva una formazione sufficiente ed adeguata in merito ai rischi specifici di cui al D.lgs. 81/08. La *formazione* e, ove previsto dalla normativa tecnica di settore, *l'addestramento* specifico avviene in occasione:

- della costituzione del rapporto di lavoro o dell'inizio dell'utilizzazione qualora si tratti di somministrazione di lavoro e/o di prestazioni occasionali di tipo accessorio;
- del trasferimento o cambiamento di mansioni;
- dell'evoluzione dei rischi, dell'insorgenza di nuovi rischi o di modifiche legislative.

La norma aziendale definisce ruoli, responsabilità e modalità operative per assicurare adeguata formazione, e i necessari aggiornamenti periodici, nel rispetto degli obblighi previsti dal D.Lgs 81/08 e dalla normativa tecnica di settore, a particolari categorie di lavoratori, quali:

- addetti al servizio di prevenzione e protezione, ove incaricati;
- datore di lavoro, dirigenti e preposti;
- rappresentante dei lavoratori per la sicurezza;
- lavoratori incaricati dell'attività di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave ed immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza.

- sorveglianza sanitaria e gestione degli infortuni: la sorveglianza sanitaria viene garantita attraverso protocolli sanitari definiti dal medico competente sulla base dei rischi specifici. Nel pianificare le attività di sorveglianza sanitaria è fatto obbligo di considerare l'eventuale presenza di lavoratori in distacco o distaccati, personale

interinale, personale che effettua prestazioni occasionali di tipo accessorio. La periodicità dei controlli tiene conto delle norme applicabili nonché del livello dei rischi. Sono formalizzati ruoli, responsabilità e modalità operative atte ad assicurare:

- la visita medica preventiva intesa a constatare l'assenza di controindicazioni al lavoro cui il lavoratore è destinato al fine di valutare la sua idoneità alla mansione specifica;
- la visita medica periodica per controllare lo stato di salute dei lavoratori ed esprimere il giudizio di idoneità alla mansione specifica;
- la visita medica su richiesta del lavoratore, qualora sia ritenuta dal medico competente correlata ai rischi professionali o alle sue condizioni di salute, suscettibili di peggioramento a causa dell'attività lavorativa svolta, al fine di esprimere il giudizio di idoneità alla mansione specifica;
- la visita medica in occasione del cambio della mansione onde verificare l'idoneità alla mansione specifica;
- la visita medica alla cessazione del rapporto di lavoro nei casi previsti dalle norme vigenti;
- la visita medica preventiva in fase pre-assuntiva;
- la visita medica precedente alla ripresa del lavoro, a seguito di assenza per motivi di salute di durata superiore ai sessanta giorni continuativi, al fine di verificare l'idoneità alla mansione;
- l'aggiornamento tempestivo del protocollo sanitario in relazione all'evolversi dell'organizzazione aziendale.

È fatto divieto di effettuare visite mediche per accertare stati di gravidanza e negli altri casi vietati dalle norme vigenti.

La cartella sanitaria e di rischio, istituita e mantenuta aggiornata per ogni lavoratore sottoposto a sorveglianza sanitaria a cura del medico competente è custodita con salvaguardia del segreto professionale e della privacy presso il luogo concordato con il datore di lavoro o suo delegato al momento della nomina.

La norma aziendale definisce, inoltre, ruoli, responsabilità e modalità operative per garantire:

- una tempestiva comunicazione al medico competente in merito alle variazioni relative all'organico aziendale (es. assunzioni, cambio mansioni, cessazioni, rientri dopo malattie con assenze superiori ai 60 gg, ecc.) affinché questi possa assicurare l'aggiornamento del calendario delle visite di idoneità e sorveglianza sanitaria;
- la vigilanza sull'assolvimento degli obblighi previsti per il medico competente compresa la visita degli ambienti di lavoro da parte del medico competente almeno una volta all'anno o con cadenza differente, stabilita in funzione dei risultati della Valutazione dei Rischi;
- l'assolvimento degli obblighi di registrazione e comunicazione in caso di infortuni;
- l'analisi e monitoraggio degli infortuni compresi i *near miss*.

- <u>acquisizione di documentazione e certificazioni obbligatorie di legge</u>: sono definiti ruoli, responsabilità e modalità operative atte ad assicurare l'individuazione,

l'acquisizione, l'aggiornamento e l'adeguata conservazione della documentazione e delle certificazioni obbligatorie di legge (relative ad edifici, impianti, persone, società, ecc.) da parte delle varie Funzioni aziendali, ciascuna nell'ambito delle proprie responsabilità e competenze.

- vigilanza e verifiche periodiche in merito al rispetto delle procedure e delle istruzioni di lavoro in sicurezza e all'efficacia delle procedure adottate: sono definiti ruoli, responsabilità e modalità operative atte ad assicurare:
  - la vigilanza sul rispetto delle procedure e delle istruzioni di sicurezza da parte del personale aziendale e del personale esterno;
  - la segnalazione dei rischi rilevati e dell'eventuale mancato rispetto delle norme di sicurezza da parte del personale aziendale e del personale esterno;
  - l'applicazione del sistema disciplinare in caso di violazioni riscontrate;
  - la pianificazione ed attuazione di verifiche periodiche e sistematiche dell'applicazione e dell'efficacia delle procedure adottate, anche con l'eventuale supporto di professionisti esterni formalmente incaricati nel rispetto delle regole comportamentali e di controllo definite nel presente Modello. Nella pianificazione delle attività di verifica si terrà conto di quanto risultante dalla Valutazione dei Rischi, della casistica relativa ad infortuni, incidenti e *near miss*, dei risultati delle attività di vigilanza e verifica periodica;
  - la definizione e implementazione di adeguati piani di azione per sanare eventuali difformità e/o carenze riscontrate nel corso delle verifiche.

Il personale della Società, a qualsiasi titolo coinvolto nelle attività di gestione degli aspetti in materia antinfortunistica e di tutela dell'igiene e della salute e sicurezza sul lavoro, è tenuto ad osservare le modalità esposte nel presente documento, le previsioni di legge esistenti in materia nonché le norme comportamentali richiamate anche nel Codice Etico. Le violazioni di procedure o altre disposizioni contenute nei documenti di sicurezza che comportino il pericolo per la sicurezza o salute delle persone sono considerate violazioni disciplinari gravi anche quando il pericolo si determina per la persona cui è addebitabile la violazione e anche se nessun danno alla persona si verifica.

C.3.2 PROCEDURE DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Tutte le aree individuate come aree a rischio sono presidiate da procedure la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'O.d.V. affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

In particolare, la presente Parte Speciale è regolamentata dal Documento di Valutazione dei Rischi e dagli altri documenti in esso richiamati, nonché da direttive e procedure di seguito riportate.

Direttiva di riferimento:

- AE GROUP-DI-012 Whistleblowing.

Procedure di riferimento:

- AE-PR-037 Ansaldo Energia Group Travel Management
- AE-PR-072 Vendor Qualification Process;
- AE-PR-102 EHS Requisites for Procurement;

- AE-PR-103 Health and Safety Risk Assessment;
- AE-PR-105 EHS Training;
- AE-PR-106 EHS Communication and consultation;
- AE-PR-107 EHS Surveillance and Performance Measurement;
- AE-PR-108 EHS Non Conformity and corrective actions;
- AE-PR-201 Waste Management;
- AE-PR-206 Hazardous Materials Management;
- AE-PR-208 Industrial Hygiene;
- AE-PR-209 Personal Protective Equipment;
- AE-PR-210 EHS Incident and near miss management;
- AE-PR-211 EHS Project Plan (Sites);
- AE-PR-212 EHS System implementation on sites;
- AE-PR-213 Contractor and Outsourcer Performance Inspection;
- AE-PR-214 Emergency preparedness and management;
- AE-PR-215 Machinery equipment and tool safety;
- AE-PR-218 Working at height;
- AE-PR-219 Lifting Operations and lifting accessories;
- AE-PR-220 Electrical safety;
- AE-PR-222 Sicurezza nelle aree a rischio esplosione;
- AE-PR-223 Hot works;
- AE-PR-225 Safety in professional travelling;
- AE-PR-226 Medical surveillance;
- AE-PR-227 Ergonomics;
- AE-PR-228 Traffic Management in a Site;
- AGT-PR-007 Product Development Design Review process.

PARTE SPECIALE "D"

Reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e delitti in materia di strumenti di pagamento diversi dai contanti

D.1 LA TIPOLOGIA DEI REATI RELATIVI A RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA

D.1.1 PREMESSA

Il decreto legislativo 231/2007, nel dare attuazione alla direttiva 2005/60 CE del Parlamento e del Consiglio d'Europa concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio, ha operato un riordino delle norme antiriciclaggio presenti nell'ordinamento giuridico italiano e ha introdotto nel D.Lgs. 231/2001 l'art. 25-*octies*, che prevede la responsabilità degli enti per i reati di riciclaggio, ricettazione e impiego di denaro, beni o altre utilità di provenienza illecita; il legislatore ha, quindi, disposto l'abrogazione dei commi 5 e 6 dell'art.10 della legge 146/2006 in materia di contrasto del crimine organizzato transnazionale. Di conseguenza, ai sensi dell'art. 25-*octies*, come inserito con il D.Lgs. 231/2007, l'Ente è punibile per i reati previsti dagli articoli 648 c.p., 648-*bis* c.p. e 648-*ter* c.p.

La Legge 186/2014 entrata in vigore il 1° gennaio 2015 ha aggiunto ai reati indicati quello di autoriciclaggio, introdotto nell'ordinamento italiano dalla Legge menzionata con l'art. 648-*ter*.1. Per la trattazione di tale reato si rinvia alla Parte Speciale "L".

Il Decreto Legislativo n. 195 del 8 novembre 2021 ha dato attuazione alla direttiva (UE) 2018/1673 del Parlamento Europeo e del Consiglio, del 23 ottobre 2018, sulla lotta al riciclaggio mediante diritto penale apportando alcune modifiche al Codice Penale. In particolare, sono stati emendati gli artt. 648, 648-bis, 648-ter e 648-ter.1 cp, con l'estensione dei c.d. "reati presupposto" così da ricomprendere sempre tra questi anche i delitti meramente colposi e, più in generale, le contravvenzioni.

D.1.2 RICETTAZIONE (ART. 648 C.P.)

L'art. 648 punisce *"Fuori dei casi di concorso nel reato chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque s'intromette nel farli acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da € 516 a € 10.329. La pena è aumentata quando il fatto riguarda denaro o cose provenienti da delitti di rapina aggravata ai sensi dell'articolo 628, terzo comma, di estorsione aggravata ai sensi dell'articolo 629, secondo comma, ovvero di furto aggravato ai sensi dell'articolo 625, primo comma, n. 7-bis)*

La pena è della reclusione da uno a quattro anni e della multa da euro 300 a euro 6.000 quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi.

La pena è aumentata se il fatto è commesso nell'esercizio di una attività professionale.

Se il fatto è di particolare tenuità, si applica la pena della reclusione sino a sei anni e della multa sino a euro 1.000 nel caso di denaro o cose provenienti da delitto e la pena della reclusione sino a tre anni e della multa sino a euro 800 nel caso di denaro o cose provenienti da contravvenzioni.

Le disposizioni di questo articolo si applicano anche quando l'autore del reato da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale reato".

L'interesse tutelato dall'art. 648 c.p. è inteso sia, in via immediata, ad evitare che una qualsiasi attività delittuosa diventi fonte di successivi profitti sia, in via mediata, a limitare all'origine la spinta all'attività delittuose.

L'elemento oggettivo del reato consiste nella ricezione che è formula comprensiva di qualsiasi conseguimento di possesso della cosa proveniente da reato e, quindi, va inteso come comprensivo di ogni negozio, oneroso o gratuito, idoneo al trasferimento della cosa nella sfera patrimoniale dell'acquirente o, comunque, nel possesso dell'acquirente.

Il termine ricevere indica ogni forma di conseguimento del possesso del bene proveniente da delitto anche se solo temporaneo.

Per occultamento si intende il nascondimento del bene proveniente dal reato dopo averlo ricevuto.

Il profilo richiesto dalla norma comprende ogni forma di utilità o vantaggio anche temporaneo che possa ricavarsi dal possesso della cosa.

La ricettazione è reato istantaneo che si consuma nel momento in cui l'agente consegue il possesso della cosa e, quindi, nell'ipotesi di acquisto si consuma nel momento dell'accordo della cosa e sul prezzo, mentre nell'ipotesi della intromissione si consuma per il solo fatto di essersi intromesso allo scopo di far acquistare – ricevere – occultare il compendio furtivo senza che sia necessario che l'interessamento raggiunga il fine propostosi dall'agente.

Per la fattispecie dolosa, l'elemento soggettivo richiesto dall'art. 648 c.p. è la consapevolezza in capo all'agente circa l'illecita provenienza della cosa.

La conoscenza della provenienza delittuosa può desumersi da qualsiasi elemento, anche indiretto: così dal comportamento dell'imputato che dimostri la certezza dell'origine illecita delle cose ricettate, sulla base dell'omessa o non attendibile indicazione della provenienza della cosa ricevuta, dal comportamento dell'agente successivo all'acquisto, dalle modalità dell'acquisto, dalla natura delle cose, dalla qualità o condizione del venditore.

D.1.3 RICICLAGGIO (ART. 648-*BIS*)

Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da € 5.000 a € 25.000.

La pena è della reclusione da due a sei anni e della multa da euro 2.500 a euro 12.500 quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'articolo 648.

Per riciclaggio si intende ogni attività diretta a far perdere al denaro, oppure a beni o altre utilità economiche di provenienza delittuosa la riconoscibilità della loro origine illecita e/o ad immetterli nel ciclo economico-finanziario, investendoli in iniziative economiche lecite con il pericolo di alterare i meccanismi di mercato.

Il compito di reprimere i fatti di riciclaggio è affidato soprattutto all'art. 648-*bis* e 648- *ter* collocati all'interno del titolo codicistico dedicato ai reati contro il patrimonio.

I proventi riciclabili sono costituiti da "denaro, beni o altra attività" ricomprendendo, pertanto, ogni vantaggio economico derivante da reato.

Le condotte rilevanti per la configurazione del reato sono tutte tipicizzate da un requisito comune perché devono essere realizzate in modo da ostacolare l'identificazione della provenienza delittuosa dell'oggetto.

Per quanto riguarda l'elemento soggettivo l'art. 648-*bis* richiede la consapevolezza della provenienza delittuosa dell'oggetto del riciclaggio e la volontà di ostacolare, con una condotta idonea, l'identificazione della provenienza.

Il secondo comma dell'art. 648-*bis* c.p. prevede una aggravante quando "il fatto è commesso nell'esercizio di una attività professionale".

D.1.4 IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA (ART. 648-*TER* C.P.)

Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da € 5.000 a € 25.000.

La pena è della reclusione da due a sei anni e della multa da euro 2500 a euro 12500 quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita nell'ipotesi di cui al quarto comma dell'articolo 648. Si applica l'ultimo comma dell'articolo 648.

L'art. 648-*ter* tutela l'ordine economico che potrebbe essere turbato dall'immissione nel mercato di beni e soprattutto di capitali di provenienza delittuosa alterando la libera concorrenza.

La condotta richiesta per l'integrazione del reato consiste nell'impiego di proventi delittuosi in attività economiche o finanziarie.

Sono da considerare economiche o finanziarie tutte quelle attività, anche di intermediazione, riguardanti la produzione o la circolazione di beni o di servizi oppure la circolazione di denaro o di valori mobiliari.

Considerato l'utilizzo del termine "impiegare" da parte del legislatore, la norma punisce ogni forma di utilizzazione di capitali illeciti con l'unica specificazione che l'impiego deve avvenire con riguardo ad attività economiche o finanziarie.

Il legislatore ha, quindi, inteso punire il comportamento consistente nell'adoperare i capitali illeciti in un'attività economica o finanziaria, a prescindere da qualsiasi obiettivo o risultato utile per l'agente e sul solo presupposto che lo stesso possa soggettivamente prevedere che l'impiego di capitale in qualche modo gli convenga.

La norma non fa riferimento al soggetto che opera ma al settore nel quale viene fatto l'investimento, pertanto, il reato non ha limitazioni di ordine soggettivo perché risulta punibile sia chi direttamente impiega o propone l'impiego di denaro, sia chi è incaricato dell'impiego di tale capitale, sempre che ci sia la consapevolezza della provenienza dei beni dai delitti espressamente indicati.

D.1.5 INDEBITO UTILIZZO E FALSIFICAZIONE DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART. 493-TER C.P.)

Chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti è punito con la

reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.
In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è ordinata la confisca delle cose che servirono o furono destinate a commettere il reato, nonché del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.
Gli strumenti sequestrati ai fini della confisca di cui al secondo comma, nel corso delle operazioni di polizia giudiziaria, sono affidati dall'autorità giudiziaria agli organi di polizia che ne facciano richiesta.
L'articolo individua tre diverse tipologie di condotte:

- la prima consiste nella indebita utilizzazione, cioè nel concreto uso illegittimo delle carte di credito o delle carte di pagamento – lecita o illecita che sia la loro provenienza – da parte del non titolare al fine di realizzare un profitto per sé o per altri;
- la seconda categoria di condotte include quelle di falsificazione e alterazione dei medesimi strumenti di pagamento;
- infine, viene punito chi possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. Si tratta in questi ultimi casi di un'azione che sotto il profilo logico e temporale è distinta dalla prima perché la precede e ne costituisce il presupposto fattuale.

Presupposto di queste tipologie di condotta è, infatti, la illecita provenienza della carta o degli altri documenti indicati dalla norma; ciò perché da sole tali condotte non sono caratterizzate da alcuna illiceità a differenza dell'utilizzo indebito o della falsificazione. Nel caso in cui le carte siano contraffatte o alterate l'illecita provenienza deriva direttamente dalla contraffazione o dalla alterazione. Per quanto riguarda le persone giuridiche, tale reato potrebbe astrattamente configurarsi nel caso in cui il dipendente della società cui è affidata la gestione della carta di credito aziendale, ma non ne è il titolare qualificato, la utilizzi indebitamente per un profitto personale arrecando un danno all'ente; laddove invece l'uso indebito fosse ascrivibile al titolare della carta di credito, si potrà configurare il reato di appropriazione indebita ex art. 646 c.p. e non quello di indebito utilizzo di carta di credito.
Pur apparendo effettivamente remoto il caso in cui l'uso indebito – o addirittura la falsificazione – vengano effettuati nell'interesse e a vantaggio dell'ente di appartenenza, l'ipotesi, sebbene in linea teorica, non si può escludere del tutto.

D.1.6 - DETENZIONE E DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A COMMETTERE REATI RIGUARDANTI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART. 493-QUATER C.P.)

Salvo che il fatto costituisca più grave reato, chiunque, alfine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente

per commettere tali reati, o sono specificamente adattati al medesimo scopo, è punito con la reclusione sino a due anni e la multa sino a 1000 euro.
In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è sempre ordinata la confisca delle apparecchiature, dei dispositivi o dei programmi informatici predetti, nonché la confisca del profitto o del prodotto del reato ovvero, quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.
Tale fattispecie richiama in parte alcuni reati informatici che sono già inclusi nel catalogo dei reati presupposto: si pensi ai delitti di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici e di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (artt. 615 quater e 615 quinquies c.p., richiamati nell'art. 24 bis, d.lgs. 231/2001).
Considerato il dettato della norma in esame, pur apparendo effettivamente remota la possibilità che tale reato possa essere commesso nell'interesse e a vantaggio dell'ente di appartenenza, in linea teorica non si può però escludere del tutto.

D.1.7 FRODE INFORMATICA (ART. 640-TER C.P.)

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.
Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o taluna delle circostanze previste dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età, e numero 7.

D.1.8 TRASFERIMENTO FRAUDOLENTO DI VALORI (ART. 512 BIS C.P.)

Salvo che il fatto costituisca più grave reato, chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648 bis e 648 ter, è punito con la reclusione da due a sei anni.
La norma punisce chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione dei delitti di ricettazione, riciclaggio e autoriciclaggio.
SI tratta chiaramente di norma di chiusura, corredata da clausola di sussidiarietà espressa destinata a coprire la condotta di chi non trasferisca effettivamente la titolarità dei beni o del denaro, ma lo faccia fittiziamente, continuando dunque ad avere la disponibilità materiale degli stessi e continuando dunque a goderne.

D.2 AREE A RISCHIO

I reati sopra considerati trovano come presupposto l'instaurazione di rapporti, diretti o indiretti, con clienti, fornitori e partner. Vengono, pertanto, definite aree a rischio tutte quelle aree aziendali che per lo svolgimento della propria attività intrattengono rapporti con gli stessi.

Tenuto conto, pertanto, della molteplicità dei rapporti che Ansaldo Green Tech intrattiene sia in Italia sia all'estero, sono state individuate le seguenti aree di attività ritenute più specificamente a rischio:

1. Attività di vendita.
2. Approvvigionamento ed appalti.
3. Tenuta della contabilità, redazione del bilancio e gestione della fiscalità.
4. Gestione dei contratti di consulenza.
5. Gestione dei flussi finanziari.
6. Promotori commerciali.
7. Gestione delle partnership.
8. Gestione dei rapporti con parti correlate.

Per il dettaglio delle attività a potenziale rischio, si rinvia a quanto indicato nei paragrafi A.3.1, A.3.2, A.3.12, A.3.13, A.3.16 e A.3.17, A.3.19 e A.3.20.

D.3 PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE A RISCHIO

D.3.1 PRINCIPI DI COMPORTAMENTO DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Le procedure aziendali finalizzate alla prevenzione dei reati previsti dall'art. 25-*octies* sono dirette a:

- definire ruoli e responsabilità nella gestione del processo di approvvigionamento;
- definire ruoli e responsabilità nella gestione del processo di vendita di beni e servizi;
- identificare l'attendibilità dei fornitori al fine di verificarne l'affidabilità anche sotto il profilo della tracciabilità delle transazioni economiche con gli stessi;
- monitorare il permanere in capo ai fornitori dei requisiti di affidabilità, correttezza, professionalità ed onorabilità;
- determinare i requisiti minimi in possesso dei soggetti offerenti e fissare i criteri di valutazione delle offerte nei contratti standard;
- verificare la regolarità dei pagamenti con riferimento alla coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- operare controlli sui flussi finanziari aziendali con riferimento ai pagamenti verso terzi, tenendo conto in particolare della sede legale della società, istituti di credito utilizzati ed eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
- disciplinare la registrazione e conservazione dei dati relativi alle transazioni;

- garantire la predisposizione e l'aggiornamento dell'anagrafica dei clienti e dei fornitori;
- stabilire standard contrattuali per l'emissione di ordini/contratti di acquisti nonché il loro rispetto;
- assicurare la corretta gestione della politica fiscale, anche con riguardo alle eventuali transazioni con i Paesi di cui al DM 21 novembre 2001 e 23 gennaio 2002 e s.m.i.;
- attuare un'adeguata formazione ed informazione degli esponenti aziendali in tema di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita;
- dare evidenza delle attività e dei controlli svolti;
- stabilire che il pagamento da parte dei Clienti deve pervenire tramite istituto di credito del Cliente presso il quale sia sempre possibile individuare il soggetto che ha disposto l'operazione verso l'istituto di credito di Ansaldo Green Tech, garantendo pertanto la possibilità di risalire al soggetto che ha disposto l'operazione;
- definire che i pagamenti devono essere effettuati a mezzo bonifico bancario su conti correnti intestati al medesimo soggetto cui è conferito l'ordine/incarico (aperto presso istituti di credito del Paese di residenza/sede legale del soggetto cui è conferito l'incarico);
- vietare pagamenti indirizzati a conti cifrati o a conti per i quali non si è in grado di individuare con precisione le generalità dell'intestatario;
- formalizzare l'iter di attivazione, utilizzo e controllo delle spese effettuate tramite carta di credito/debito con addebito sul conto corrente aziendale;
- vietare l'utilizzo delle carte di credito/debito con addebito sul conto corrente aziendale da parte di soggetto diverso dal legittimo titolare;
- vietare l'effettuazione di operazioni volte ad attribuire fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità della Società.

D.3.2 PROCEDURE DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Tutte le aree individuate come aree a rischio sono presidiate da procedure la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'O.d.V. affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si riportano di seguito le direttive e le procedure da seguire nelle aree di attività a rischio individuate nella presente Parte Speciale.

Direttive di riferimento:

- AE GROUP-DI-002 Export Compliance;
- AE GROUP-DI-004 Appointment of Sales Promoters;
- AE GROUP-DI-007 Managing Intellectual Property Assets;
- AE GROUP-DI-009 Antitrust Directive;
- AE GROUP-DI-012 Whistleblowing.

Procedure di riferimento:

- AE-PR-021 Accounts Receivable Process;
- AE-PR-022 Accounts Payable Process;
- AE-PR-023 Fixed Assets Process;
- AE-PR-024 General Ledger Process;
- AE-PR-025 Tax Management Process;
- AE-PR-026 Consolidation Process;
- AE-PR-027 Treasury and Trade Finance Process;
- AE-PR-037 Ansaldo Energia Group Travel Management;
- AE-PR-043 Professional Services and Consulting Assignments required without RdA;
- AE-PR-044 Supply Chain management;
- AE-PR-046 Intercompany Transfer Pricing Policy;
- AE-PR-050 Intellectual Property Process;AE-PR-051 Intellectual Property Contitution Process;
- AE-PR-064 Project Claims Management Process;
- AE-PR-069 Intellectual Property Transfer process – Manage Non-Disclosure Agreements;
- AE-PR-070 Intellectual Property Transfer process – Manage Collaborative Research;
- AE-PR-071 Vendor Rating Process;
- AE-PR-072 Vendor Qualification Process;
- AE-PR-082 Due Diligence;
- AE-IN-001 Business travel management;
- AE-IN-004 Purchase Request approval flow e rules;
- AE-IN-006 Passive Payments – Operational Checks Against Supplier Data Cyber Frauds;
- AGT-PR-001 Sales process;
- AGT-PR-002 Supply Management.

PARTE SPECIALE "E"

Delitti informatici e trattamento illecito di dati e delitti in materia di violazione del diritto d'autore

E.1 LA TIPOLOGIA DEI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI E DELITTI IN MATERIA DI VIOLAZIONI DEL DIRITTO D'AUTORE

E.1.1 PREMESSA

La legge 18 marzo 2008 n. 48 ha ratificato la Convenzione di Budapest del 23 novembre 2001, promossa dal Consiglio d'Europa in tema di criminalità informatica e riguardante i reati commessi avvalendosi in qualsiasi modo di un sistema informatico o in suo danno.

L'art. 24-*bis* del D.Lgs. 231/2001 contempla la responsabilità degli enti con riguardo a tre distinte categorie:

- reati che comportano un "danneggiamento informatico" art. 24-*bis* comma 1;
- reati derivanti dalla detenzione o diffusione di codici o programmi atti al danneggiamento informatico art. 24-*bis,* comma 2;
- reati relativi al falso in documento informatico e frode informatica.

Con la legge 23 luglio 2009 n. 99 è stato introdotto nel decreto 231/2001 l'art. 25-*novies* che prevede la sanzione per la violazione dei diritti d'autore tutelati dagli artt. 171 (limitatamente all'ipotesi prevista alla lett. A *bis*), *171 bis, ter, septies e octies,* nonché 174-*quinquies* della legge 22 aprile 1941 n. 633.

Quest'ultima legge ha subito diverse modifiche e pur mirando a tutelare prevalentemente le "opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro e alla cinematografia qualunque ne sia il modo e la forma di espressione (definizione delle opere protette come risulta dall'art. 1 della citata legge 633/1941), estende la protezione ai "*programmi per elaboratore in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore*" (art. 2 n. 8) ed alle "*opere del disegno industriale che presentino di per sé carattere creativo e valore artistico*" (art. 2 n. 10).

Le due precisazioni inducono a ritenere meritevole di attenzione anche questa norma che pur inserita in materia per la quale non sono presenti in Ansaldo Green Tech specifiche aree a rischio, potrebbe avere, nella specificità del solo art. 171-*bis*, attività che possono essere considerate a rischio.

Per tali motivi viene preso in considerazione il solo reato previsto dall'art. 171-*bis* la cui rubrica recita "Duplicazione e altre azioni illecite su programmi per elaboratore e su banche dati" e che, richiamato dall'art. 25-*novies* del D.Lgs. 231/2001 contempla la responsabilità per due ipotesi:

- la duplicazione dei programmi informatici e la cessione dei duplicati;
- la duplicazione o cessione di banche di dati.

Prima di passare all'analisi delle singole fattispecie criminose è opportuno fornire alcune definizioni come sono state acquisite nella giurisprudenza.

L'espressione «sistema informatico» esprime il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche. Queste ultime, come si è rilevato in dottrina, sono caratterizzate dalla registrazione (o "memorizzazione"), per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazione elementari di un fatto, effettuate attraverso simboli numerici ("codice") in combinazioni diverse; tali "dati", elaborati automaticamente dalla macchina, generano le "informazioni" costituite "da un insieme più o meno vasto di dati organizzati secondo una logica che consente loro di attribuire un particolare significato per l'utente".

Con l'espressione «sistema telematico» le disposizioni sui crimini informatici rinviano invece ad un insieme combinato di apparecchiature idoneo alla trasmissione a distanza di dati e di informazioni, attraverso l'impiego di tecnologie dedicate alle telecomunicazioni.

La qualifica di operatore del sistema, che può essere rivestita tanto da una persona fisica quanto da una impresa, nella pratica si attribuisce a chiunque può usufruire delle prestazioni e delle risorse di un elaboratore elettronico. Ad esempio:

- il soggetto preposto alle operazioni di «input» e di «output», di avviamento o di arresto dell'elaboratore elettronico;
- il programmatore che scrive, con appositi linguaggi, le istruzioni e le operazioni che il computer è chiamato ad effettuare;
- il sistemista, che studia le possibili evoluzioni di un sistema per ottimizzarlo ed implementarlo;
- l'analista che sviluppa gli algoritmi per soddisfare specifiche esigenze tecniche;
- il singolo utente dei sistemi informatici.

E.1.2 FRODE INFORMATICA (ART. 640-*TER* C.P.)

"Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da € 51 a € 1.032.

La pena è della reclusione da uno a cinque anni e della multa da € 309 a € 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso di qualità di operatore del sistema.

La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza aggravante prevista dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età e numero".

Il reato di frode informatica ha la medesima struttura e, quindi, i medesimi elementi costitutivi della truffa dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona, di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema.

La figura di reato delineata implica un tipo di condotta improntata all'inganno e all'artificio e, quindi, porta a far ritenere penalmente rilevante a tale titolo ogni possibile induzione in errore portata a compimento mediante il ricorso a sistemi informatici. Pertanto, il reato è da considerarsi integrato quando vengano posti in essere quegli interventi consistenti sia nell'adibire il sistema informatico per scopi tutt'affatto diversi da quelli cui esso è stato destinato (alterazione del funzionamento) e sia nel manipolare arbitrariamente i contenuti (intervento sui dati, informazioni e programmi).

In sostanza, il reato implica un tipo di condotta improntata all'inganno e all'artificio e quindi porta a far ritenere penalmente rilevante ogni possibile induzione in errore portata a compimento mediante il ricorso al computer.

In questa particolare fattispecie la norma per la configurazione del reato chiede anche la realizzazione di un profitto con altrui danno.

Come già detto, il D. Lgs. 231/01, perché si configuri la responsabilità dell'ente, richiede che la frode informatica sia commessa in danno dello Stato o di altro ente pubblico.

E.1.3 ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (ART. 615-*TER* C.P.)

"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con l'abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni e dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

Il reato è, quindi, commesso da chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantiene contro la volontà di chi ha diritto di escluderlo. Si considera misura di sicurezza anche la protezione del sistema rappresentata da una semplice chiave di accesso (password).

Non è richiesto che il reato sia commesso a fini di lucro o di danneggiamento; tuttavia, visto che l'accesso abusivo è spesso strumentale alla commissione di altri reati informatici, è possibile un concorso tra il reato di cui all'art. 615-*ter* c.p. ed altri crimini informatici.

Secondo una parte della giurisprudenza, commette il reato anche il soggetto che, pur avendo diritto di accedere al sistema, lo utilizzi per finalità diverse da quelle consentite.

In sostanza, con la previsione di cui all'art. 615-*ter* c.p. il legislatore ha assicurato la protezione del «domicilio informatico» quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto. Tuttavia l'art. 615-*ter* c.p. non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello *jus excludendi alios*, quale che sia il contenuto dei dati racchiusi in esso, purché attinenti alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati sia che titolare dello *jus excludendi* sia persona fisica, sia giuridica, privata o pubblica, o altro ente.

È prevista un'aggravante speciale, comune anche ad altre fattispecie di crimini informatici, nel caso in cui il reato sia commesso con abuso della qualità di operatore del sistema.

E.1.4 INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-*QUATER* C.P.)

"Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno a cinque anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede di ufficio e la pena è della reclusione da tre a otto anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da un altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato".

Per «comunicazioni informatiche o telematiche» si intendono le trasmissioni di dati, suoni, immagini, simboli, programmi ed ogni altra informazione trasportata attraverso sistemi di elaborazione automatizzati.

"Per intercettazione" deve intendersi l'effettiva cognizione del contenuto dell'altrui comunicazione, non importa se sia stata registrata o meno, mentre non è tale la verifica della durata della comunicazione, o la registrazione dei numeri chiamati, a fine di documentazione, controllo e contabilizzazione del traffico telefonico.

L'intercettazione deve essere fraudolenta e, pertanto, deve essere attuata con l'impiego di mezzi ingannevoli o idonei a raggirare il sistema o il gestore.

Oltre all'intercettazione fraudolenta sono sanzionati «l'impedimento» e «l'interruzione» delle comunicazioni che si verificano quando l'agente, con qualunque accorgimento tecnico, utilizzi o inserisca ostacoli fisici o programmi in grado di inibire, arrestare o rendere difficoltoso il normale esercizio del servizio.

Il secondo comma punisce anche chi divulga il contenuto delle comunicazioni fraudolentemente intercettate. Per l'integrazione del reato è necessario che la rivelazione sia rivolta ad un numero indeterminato di persone e che avvenga con un mezzo di informazione al pubblico; non è pertanto punibile la condotta di chi riveli il contenuto delle comunicazioni ad un individuo specifico.

E.1.5 DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE E ALTRI MEZZI ATTI A INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-*QUINQUIES* C.P.)

"Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere

comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater".

Tale norma punisce le varie condotte (procurarsi, detenere, produrre, riprodurre, diffondere, importare, comunicare, consegnare, mettere in altro modo a disposizione di altri o installare apparecchiature, programmi, codici, parole chiave o altri mezzi) idonee ad intercettare, impedire o interrompere comunicazioni; pertanto, perché sia integrato il reato, non è necessario che l'intercettazione, l'interruzione o l'impedimento si verifichino in concreto e quindi il reato si consuma anche se gli apparecchi installati, detenuti, ecc. non abbiano funzionato o non siano stati attivati dall'agente. L'unica ipotesi in cui il reato non può dirsi consumato è quella di inidoneità tecnica assoluta dell'apparecchiatura in questione.

E.1.6 DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (ART. 635-*BIS* C.P.)

"Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".

Le condotte con cui può essere realizzato il reato sono molteplici: distruggere, deteriorare, alterare o sopprimere; «deve ritenersi integrato il delitto di danneggiamento tutte le volte in cui la condotta criminosa apporti alla cosa una modificazione che, diminuendone in modo apprezzabile il valore o impedendone anche parzialmente l'uso, richieda un intervento ripristinatorio dell'essenza e della funzionalità della cosa».

La clausola di riserva ("*salvo che il fatto costituisca più grave reato"*) è prevista perché le condotte di danneggiamento, in alcuni casi, possono essere inquadrate come reati puniti con pene decisamente più alte.

E.1.7 DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI UTILIZZATI DALLO STATO O DA ALTRO ENTE PUBBLICO O COMUNQUE DI PUBBLICA UTILITÀ (ART. 635-*TER* C.P.)

"Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata".

Si tratta di un'ipotesi speculare a quella prevista dall'art. 635-*bis* c.p. in cui tuttavia, trattandosi di beni dello Stato o, comunque, di beni riconducibili ad assolvere ad una funzione di pubblica utilità, la risposta dell'ordinamento è molto più forte.

Il reato si considera commesso anche in assenza di un effettivo deterioramento, distruzione, cancellazione, alterazione o soppressione dei dati.

Se poi gli eventi dovessero verificarsi vi è un ulteriore aumento della sanzione penale.

E.1.8 DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (ART. 635-*QUATER* C.P.)

"Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte inservibili, sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

La distinzione tra il reato di cui all'articolo 635 *bis* e quella descritta all'art. 635-*quater* è legata alle conseguenze della condotta: laddove la soppressione o l'alterazione di dati, informazioni e programmi renda inservibile o quantomeno ostacoli gravemente il funzionamento delle apparecchiature, ricorrerà la più grave ipotesi del danneggiamento di sistemi informatici o telematici.

Il reato può essere commesso sia nelle forme di cui all'art. 635-*bis* (distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui), sia con l'introduzione o con la trasmissione di dati, informazioni o programmi; è evidente che quest'ultima ipotesi attiene al cd. danneggiamento virtuale che si realizza, per lo più, mediante l'invio di file maligni o di virus.

E.1.9 DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ (ART. 635-*QUINQUIES* C.P.)

"Se il fatto di cui all'art. 635 quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

Anche in questo caso, il legislatore offre una tutela rafforzata ai sistemi informatici e telematici di pubblica utilità. Infatti, è previsto un innalzamento delle pene nel caso in cui l'attacco informatico sia rivolto nei confronti di sistemi informatici o telematici di pubblica utilità.

Per integrare il reato è sufficiente porre in essere condotte dirette alla distruzione o al danneggiamento di tali sistemi; quando la distruzione o il danneggiamento si verifichino vi è un ulteriore aggravio della pena.

Il legislatore ha, quindi, deciso di offrire ai sistemi informatici o telematici di pubblica utilità una tutela anticipata e rafforzata.

E.1.10 DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE, CODICI O ALTRI MEZZI ATTI ALL'ACCESSO A SISTEMI INFORMATICI O TELEMATICI (ART. 615-*QUATER* C.P.)

"Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a € 5.164.

La pena è della reclusione da uno a tre anni e della multa da € 5.164 a € 10.329 se ricorra taluna delle circostanze di cui al quarto comma dell'articolo 617-quater".

Le varie condotte (detenere, procurarsi, produrre, riprodurre, diffondere, importare, comunicare, consegnare, mettere in altro modo a disposizione di altri, installare) sono tutte accomunate dall'essere svolte abusivamente e cioè in contrasto con la normale fruizione dei diritti o con l'esercizio di facoltà da parte dell'agente.

Si tratta di un delitto a dolo specifico, nel senso che esso viene a perfezionarsi solo nel caso in cui la condotta dell'agente sia indirizzata a procurare a sé o ad altri un profitto, ovvero ad arrecare un danno a terzi. Il profitto o il danno rappresentano solo il fine cui deve tendere la condotta tenuta dall'agente; per la realizzazione del reato non è quindi necessario che si realizzino.

In alcuni casi l'art. 615-*quater* può concorrere con il reato di cui all'art. 615-*ter* c.p.; per procurarsi abusivamente i codici di accesso può essere, infatti, necessario effettuare anche un accesso abusivo all'interno di un sistema informatico o telematico protetto ovvero l'essersi procurati abusivamente dei codici può essere un atto prodromico ad un accesso abusivo.

Integra il reato la condotta di colui che si procuri abusivamente il numero seriale di un apparecchio telefonico cellulare appartenente ad altro soggetto, poiché attraverso la corrispondente modifica del codice di un ulteriore apparecchio (cd. clonazione) è possibile realizzare una illecita connessione alla rete di telefonia mobile, che costituisce un sistema telematico protetto, anche con riferimento alle banche concernenti i dati esteriori delle comunicazioni, gestite mediante tecnologie informatiche.

E.1.11 DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO (ART. 615-*QUINQUIES* C.P.)

"Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa fino a euro 10.329".

I comportamenti vietati sono molteplici.

Anche questo è un reato a dolo specifico, per cui è necessario che l'agente agisca al fine di danneggiare illecitamente un sistema informatico.

E.1.12 FALSITÀ' IN UN DOCUMENTO INFORMATICO PUBBLICO AVENTE EFFICACIA PROBATORIA (ART. 491-*BIS* C.P.)

"Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici".

Le moderne tecnologie hanno messo in crisi l'antica concezione secondo cui la scrittura rappresentava l'unica forma di manifestazione documentabile della volontà dei soggetti; pertanto, il legislatore ha previsto un cd. clausola di equivalenza grazie alla quale alle falsificazioni informatiche di un documento pubblico possono essere applicate le norme concernenti gli atti pubblici, superando definitivamente l'impostazione originaria del codice penale fondata sulla materialità del supporto e sulla forma scritta del documento.

I reati per cui pertanto vale la clausola di equivalenza sono: a) art. 476 «Falsità materiale commessa dal pubblico ufficiale in atti pubblici»; b) art. 477 «Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative»; c) art. 478 «Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti»; d) art. 479 «Falsità ideologica commessa dal pubblico ufficiale in atti pubblici»; e) art. 480 «Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative»; f) art. 481 «Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità»; g) art. 482 «Falsità materiale commessa dal privato»; h) art. 483 «Falsità ideologica commessa dal privato in atto pubblico»; i) art. 484 «Falsità in registri e notificazioni»; l) art. 487 «Falsità in foglio firmato in bianco. Atto pubblico»; m) art. 488 «Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali»; n) art. 489 «Uso di atto falso»; o) art. 490 «Soppressione, distruzione e occultamento di atti veri»; p) art. 491 «Falsità in testamento olografo, cambiale o titoli di credito».

E.1.13 FRODE INFORMATICA DEL SOGGETTO CHE PRESTA SERVIZI DI CERTIFICAZIONE DI FIRMA ELETTRONICA (ART. 640-*QUINQUIES* C.P.)

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

Pur essendo rubricata come frode informatica questa ipotesi di reato prescinde completamente da qualsiasi requisito di fraudolenza e consiste nella violazione degli obblighi stabiliti dall'articolo 32 del Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82).

Si tratta di un reato a dolo specifico e, pertanto, il soggetto che presta servizi di certificazione deve agire al fine di procurare a sé o ad altri un profitto ovvero di arrecare un danno ad un terzo.

E.1.14 DIRITTO D'AUTORE (ART. 171-*BIS* DELLA LEGGE 22 APRILE 1941 N. 633)

1. "Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a trenta milioni. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per

elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.

2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a trenta milioni. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità."

Come si evince dalla lettura della norma due sono le fattispecie prese in considerazione dalla legge, che si distinguono per il bene o interesse tutelato.

Il comma 1 tutela il diritto morale ed economico dell'autore di un programma. Mentre il comma 2 tutela il diritto morale ed economico dell'autore di una banca di dati, equiparata, quindi, a questi fini ad un'opera dell'ingegno.

Denominatore comune delle due ipotesi è il fine di "trarne profitto", formulazione che comporta un alto livello della soglia di punibilità in quanto il "trarne profitto" è stato inteso dalla giurisprudenza non solo come un guadagno ma anche come una "mancata perdita patrimoniale", ossia come un risparmio.

E.2 AREE A RISCHIO

I reati sopra esposti trovano come presupposto l'impiego di sistemi e programmi informatici. Tutti gli esponenti aziendali utilizzano ordinariamente sistemi informatici e hanno, conseguentemente, ampia possibilità di accesso a strumenti e dati informatici e telematici nel contesto svolgimento dell'ordinaria attività lavorativa.

Per quanto concerne i reati informatici, in considerazione della loro natura peculiare, potrebbero essere astrattamente posti in essere in qualsiasi ambito di attività, pertanto si ritiene di valutare il rischio della loro commissione come rischio diffuso.

Le aree aziendali in cui può verificarsi il rischio che siano commessi i reati informatici previsti dal D.Lgs. 231/01 sono, teoricamente, tutte quelle in cui le attività sono supportate da sistemi informatici e/o telematici per l'elaborazione e trasmissione di dati (gestionali, contabili, fiscali, ecc.). Pertanto, con riferimento ai reati informatici sopra esposti, si evidenzia che qualsiasi attività aziendale che contempli la gestione, la manutenzione e l'utilizzo di sistemi informatici, database, piattaforme e strutture ICT in genere, può astrattamente ritenersi a rischio.

Nella Parte Speciale A (vedi paragrafo A.3.21), le attività a rischio sono state raggruppate in tre macro-categorie, nell'ambito delle quali sono previste, tra le altre, le seguenti attività:

- gestione dei profili utente e del processo di autenticazione;
- gestione e protezione della postazione di lavoro;
- gestione degli accessi da e verso l'esterno;
- gestione e protezione delle reti;
- gestione degli output di sistema e dei dispositivi di memorizzazione;
- sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, etc.);
- sviluppo prodotti, ingegneria e produzione.

I principi di comportamento e le modalità di presidio e controllo, nel seguito indicate, costituiscono un presidio di contrasto anche in riferimento ai reati di cui alla Parte Speciale A "Reati contro la Pubblica Amministrazione e delitti di corruzione tra privati e di istigazione alla corruzione tra privati" ed alla Parte Speciale B "Reati societari e di abuso di mercato e relativi illeciti amministrativi di cui al Testo Unico della Finanza".

E.3 PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITA' A RISCHIO

E.3.1 PRINCIPI DI COMPORTAMENTO DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

I destinatari devono adottare regole di condotta conformi a quanto prescritto nella presente Parte Speciale, nonché a quanto previsto dal Codice Etico e dalle procedure aziendali al fine di impedire il verificarsi dei reati trattati.

Le attività devono essere, pertanto, svolte nel rispetto del Modello, del Codice Etico, delle procedure e delle linee guida di comportamento definite. Tali documenti sono stati sviluppati per garantire il rispetto dei seguenti principi:

- Riservatezza: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione / conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- Integrità: garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- Disponibilità: garanzia di reperibilità dei dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

In considerazione della diffusione delle aree a rischio si applicano a tutti i destinatari del Modello principi di comportamento di carattere generale che prevedono:

- il divieto di porre in essere, collaborare o dare causa al verificarsi di comportamenti tali che realizzino direttamente o indirettamente le fattispecie di reato rientranti tra quelle sopra considerate;
- il divieto di violare i principi e le procedure previsti in questa Parte Speciale del Modello.

In particolare, è fatto divieto:

- di alterare documenti informatici aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al sistema informatico o telematico della Società al fine di alterare e/o cancellare dati e/o informazioni;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso dal proprio sistema informatico o telematico al fine di acquisire informazioni riservate;

- svolgere attività abusiva di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico di soggetti pubblici o privati, le informazioni i dati o i programmi in esso contenuti ovvero di favorire l'interruzione o l'alterazione del suo funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti pubblici o privati al fine di acquisire informazioni riservate;
- installare abusivamente, detenere, diffondere apparecchiature e altri mezzi atti all'intercettazione, impedimento o interruzione di comunicazione di soggetti pubblici o privati;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti pubblici o privati;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui o di pubblica utilità;
- distruggere, danneggiare sistemi informatici o telematici altrui o di pubblica utilità.

Ai fini dell'attuazione dei comportamenti di cui sopra, le procedure rivolte a tutti gli esponenti aziendali ed ai collaboratori esterni, prevedono:

- l'utilizzo delle informazioni, applicazioni e apparecchiature esclusivamente per motivi di ufficio ed esclusivamente da parte del soggetto titolare dell'apparecchiatura informatica;
- la tempestiva segnalazione alle funzioni competenti del furto, danneggiamento e/o smarrimento di qualsiasi apparecchiatura informatica;
- il divieto di introdurre e/o conservare in Azienda a qualsiasi titolo e per qualsiasi ragione documentazione e/o materiale informatico di natura riservata e di proprietà di terzi salvo che questi siano stati acquisiti con il loro espresso consenso;
- il divieto di trasferire all'esterno della Società files e qualsiasi documentazione riservata di proprietà della Società;
- il divieto di lasciare incustodito o accessibile a terzi il proprio personal computer;
- il divieto di utilizzo di passwords di altri utenti aziendali;
- il divieto di utilizzo di strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- l'utilizzo della connessione a internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
- la segnalazione all'Unità Organizzativa competente di eventuali utilizzi o funzionamenti anomali delle risorse informatiche;
- l'impiego sulle apparecchiature societarie dei soli prodotti software e/o hardware ufficialmente acquistati dalla società stessa;
- il divieto di effettuare copie non specificatamente autorizzate di dati e software.

Tra le attività di presidio e controllo, sono in particolare previste:

- l'adozione di misure di sicurezza per la protezione ed il controllo del Data Center e delle infrastrutture ICT (server, reti con i relativi apparati) contro i fattori ambientali e per limitare l'accesso alle aree riservate al solo personale formalmente autorizzato;

- l'adozione di misure di sicurezza per l'identificazione/autenticazione degli utenti e per l'autorizzazione agli accessi ai sistemi ed ai dati previsti per la mansione secondo procedure formali per la concessione, la modifica, la revoca delle credenziali di autenticazione (associate univocamente ad ogni utente) e dei privilegi d'accesso;
- il controllo periodico dei privilegi d'accesso degli utenti con modifica e/o rimozione di quelli non più conformi alla situazione aziendale;
- l'adozione di sistemi di autenticazione ed autorizzazione all'accesso ai sistemi che limitano l'accesso a contenuti e funzioni in base al profilo autorizzativo dell'utente;
- il monitoraggio e la tracciatura di tutti gli accessi ai sistemi, con evidenza dei tentativi di intrusione ed attivazione delle azioni per fronteggiare la situazione e ripristinare le condizioni di sicurezza;
- l'adozione di procedure formali per la pianificazione e la gestione del *backup* dei sistemi (programmi, dati, configurazioni), di protezione e conservazione dei supporti;
- l'adozione di misure per rendere sicuri i sistemi in esercizio (applicazioni ed infrastrutture, comprensive della rete di telecomunicazioni con i relativi apparati) e garantire la corretta e sicura circolazione delle informazioni;
- il monitoraggio dei sistemi in esercizio (infrastrutture e applicazioni) per la tempestiva rilevazione di incidenti (e la loro tracciatura) e per la prevenzione di situazioni non conformi all'operatività attesa con l'adozione di procedure formali volte a garantire il ripristino delle condizioni di sicurezza previste;
- il monitoraggio dei sistemi per rilevare la presenza di virus, altro software malevolo, apparati e software non conformi agli standard aziendali e/o non autorizzati;
- l'adozione di procedure formali per rimuovere apparati e software irregolari e/o regolarizzarli e per ripristinare la situazione di sicurezza dei sistemi;
- il monitoraggio degli Asset IT (Hardware e Software) con aggiornamento costante dell'inventario (in seguito ad attività di assegnazione, riconsegna, dismissione, cambio di assegnazione del bene), periodiche riconciliazioni d'inventario e l'adozione di procedure per garantire il ripristino delle condizioni di sicurezza;
- la definizione di norme comportamentali, la formalizzazione delle modalità di utilizzo e la predisposizione degli opportuni meccanismi per lo scambio in sicurezza di informazioni tramite e-mail e internet;
- la predisposizione e la protezione della documentazione di sistema relativa alle configurazioni, personalizzazioni e procedure operative, funzionale ad un corretto e sicuro svolgimento delle attività;
- la separazione fisica degli ambienti sui quali i sistemi sono installati (sviluppo, collaudo, produzione) con diversi privilegi d'accesso;
- la gestione della domanda di asset IT (tra l'altro, PC, apparati Hardware, Software) con l'adozione di procedure formali nelle responsabilità operative/autorizzative e nelle attività (dalla richiesta dell'asset all'autorizzazione all'installazione, modifica, rimozione);
- l'adozione di specifiche procedure formali per il processo di Change Management dei sistemi (infrastrutture, applicazioni, reti) nell'individuazione, selezione, approvazione delle richieste aziendali e nelle varie fasi dallo sviluppo, acquisizione all'installazione delle modifiche, nuovi asset in produzione con gli opportuni controlli di sicurezza nel processo e di validazione, accettazione delle soluzioni;

- il monitoraggio dei servizi delle Terze Parti: in particolare, per i servizi in outsourcing sono predisposte adeguate clausole contrattuali che obbligano il fornitore a comportamenti conformi a quelli stabiliti dall'Azienda e ad accettare i controlli che consentano di verificare il rispetto di quanto concordato.

E.3.2 PROCEDURE DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Tutte le aree individuate come aree a rischio sono presidiate da procedure la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'O.d.V. affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si riportano di seguito le direttive, policy e le procedure da seguire nelle aree di attività a rischio individuate nella presente Parte Speciale.

Direttive di riferimento:

- AE GROUP-DI-001 Code of Conduct for ICT Users;
- AE GROUP-DI-006 Privacy;
- AE GROUP-DI-007 Managing Intellectual Property Assets;
- AE GROUP-DI-008 Information Security;
- AE GROUP-DI-012 Whistleblowing;
- AE GROUP-PL-003 AE Group Information & Cyber Security Policy.

Procedure di riferimento:

- AE-PR-016 Information Technology Management Process;
- AE-PR-017 Information Technology Management Process-IT Demand Management;
- AE-PR-018 Information Technology Management Process-IT Service Execution;
- AE-PR-033 Information & Cyber Security Process - Security Incident Management;
- AE-PR-034 External and Internal Communication;
- AE-PR-048 Information Classification;
- AE-PR-050 Intellectual Property Process;
- AE-PR-051 Intellectual Property Process – IP Constitution;
- AE-PR-057 IT Access Management;
- AE-PR-058 IT Security Operating Handbook;
- AE-IN-006 Passive Payments – Operational Checks Against Supplier Data Cyber Frauds;
- AE-IN-016 Guidelines for the management of company phone.

PARTE SPECIALE "F"

Delitti di criminalità organizzata

F.1 LA TIPOLOGIA DEI DELITTI DI CRIMINALITA' ORGANIZZATA

F.1.1 PREMESSA

Dopo l'emanazione della legge 16 marzo 2006 n. 146 e le innovazioni introdotte dalla L. 15 luglio 2009 n. 94, i delitti di criminalità organizzata sono ritenuti presupposto per l'applicazione delle sanzioni previste dal D.Lgs. 231/01, sia che siano commessi all'interno dello Stato, sia che rientrino fra i delitti transnazionali come definiti dall'art. 3 della L. 146/2006.

Ai sensi del combinato disposto delle leggi n. 146/2006 e 94/2009, i delitti considerati da entrambe le fonti normative e rilevanti ai fini di una responsabilità dell'ente sono: associazione per delinquere (art. 416 c.p.); associazioni di tipo mafioso anche straniere (art. 416-*bis* c.p.); associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del DPR n. 309/1990).

Oltre a quelli sopra menzionati si ricorda che rientrano tra i delitti di criminalità organizzata così come previsti dall'art. 24-*ter* del D.Lgs. 231/01 anche i seguenti reati: scambio elettorale politico-mafioso (art. 416-*ter*); sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.); illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (art. 407, c. 2, lett. a) n. 5 c.p.p.).

Per completezza, si ricorda che rientrano invece tra i reati transnazionali contemplati dal Decreto, oltre a quelli sopra riportati anche i seguenti: associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291 *quater* del DPR n. 43/1973); traffico di migranti (art. 12, commi 3, 3 *bis*, 3 *ter* e 5, D.Lgs. 25 luglio 1998, n. 286); induzione a non rendere o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.); favoreggiamento personale (art. 378 c.p.) (questi ultimi due reati sono trattati nella successiva Parte Speciale).

F 1.2 ASSOCIAZIONE PER DELINQUERE (ART. 416 C.P.)

"Quando tre o più persone si associano allo scopo di commettere più delitti, coloro che promuovono o costituiscono od organizzano l'associazione sono puniti, per ciò solo, con la reclusione da tre a sette anni.
Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni.
I capi soggiacciono alla stessa pena stabilita per i promotori.
Se gli associati scorrono in armi le campagne o le pubbliche vie, si applica la reclusione da cinque a quindici anni.
La pena è aumentata se il numero degli associati è di dieci o più.
Se l'associazione è diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602, nonché all'articolo 12, comma 3-bis, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, si applica la reclusione da cinque a quindici anni nei casi previsti dal primo comma e da quattro a nove anni nei casi previsti dal secondo comma.
Se l'associazione è diretta a commettere taluno dei delitti previsti dagli articoli 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 609-bis, quando il fatto è commesso in danno di un minore di anni diciotto, e 609-undecies, si applica la reclusione da quattro a otto anni nei casi previsti dal primo comma e la reclusione da due a sei anni nei casi previsi dal secondo comma."

Il reato di associazione per delinquere si caratterizza per tre elementi fondamentali, costituiti da:

- un vincolo associativo tendenzialmente permanente, o comunque stabile, destinato a durare anche oltre la realizzazione dei delitti concretamente programmati;
- l'indeterminatezza del programma criminoso, che distingue l'associazione per delinquere dal semplice concorso nel reato;
- l'esistenza, anche minima, di una struttura adeguata alla realizzazione degli obiettivi criminosi.

Il reato si considera commesso per il solo fatto della esistenza di un permanente vincolo associativo rivolto alla commissione di illeciti penali, prescindendo, in concreto, dalla effettiva commissione degli illeciti stessi; infatti, nel caso in cui i reati vengano realizzati, i componenti dell'associazione risponderanno sia del reato di associazione per delinquere sia del reato in concreto posto in essere.
Nell'ambito dell'associazione per delinquere le condotte di partecipazione da una parte e di promozione, costituzione e organizzazione dall'altra, sono previste come distinte ipotesi delittuose.
Promotori, organizzatori e capi si contraddistinguono per avere in seno al sodalizio criminoso un ruolo di supremazia e direzione, mentre quanto alla descrizione della condotta di partecipazione, se ne sottolinea la natura di fattispecie a forma libera che consiste nel contributo apprezzabile e concreto sul piano causale, all'esistenza e al rafforzamento dell'associazione e, quindi, alla realizzazione dell'offesa degli interessi tutelati dalla norma incriminatrice, qualunque sia il ruolo o il compito che il partecipe svolge nell'ambito del sodalizio.
Promuovono l'associazione le persone che, da sole o insieme con altre, se ne fanno iniziatrici.
La costituiscono coloro che con la loro attività ne determinano o concorrono a determinare l'attività.
Organizzatore è chi coordina l'attività dei singoli soci, per assicurare la vita, l'efficienza e lo sviluppo dell'associazione.
I capi sono gli individui che regolano in tutto o in parte l'attività dell'associazione con posizione di superiorità.

F 1.3 ASSOCIAZIONI DI TIPO MAFIOSO ANCHE STRANIERE (ART. 416-*BIS* C.P.)

"Chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone, è punito con la reclusione da dieci a quindici anni.
Coloro che promuovono, dirigono o organizzano l'associazione sono puniti, per ciò solo, con la reclusione da dodici a diciotto anni.
L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.
Se l'associazione è armata si applica la pena della reclusione da dodici a venti anni nei casi previsti dal primo comma e da quindici a ventisei anni nei casi previsti dal secondo comma.
L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito.

Se le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto dei delitti, le pene stabilite nei commi precedenti sono aumentate da un terzo alla metà.
Nei confronti del condannato è sempre obbligatoria la confisca delle cose che servirono o furono destinate a commettere il reato e delle cose che ne sono il prezzo, il prodotto, il profitto o che ne costituiscono l'impiego.
Le disposizioni del presente articolo si applicano anche alla camorra e alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso".

Questa fattispecie di reato si caratterizza per due elementi aggiuntivi rispetto al reato di semplice associazione per delinquere; oltre al vincolo associativo, devono essere, pertanto, presenti: una forza intimidatrice e una condizione di assoggettamento e di omertà.
Forza intimidatrice e condizione di assoggettamento e omertà sono gli strumenti di cui l'associazione mafiosa deve avvalersi al fine di raggiungere i propri scopi associativi.

Il fine a cui deve tendere un'associazione di tipo mafioso è da considerarsi eterogeneo; infatti, le finalità indicate al terzo comma dell'articolo devono essere intese in senso alternativo e non cumulativo.

Sono previste delle aggravanti specifiche nel caso in cui l'associazione mafiosa sia armata, cioè nelle ipotesi in cui abbia la disponibilità di armi, strumentali al conseguimento delle finalità dell'associazione.

L'art. 416 punisce anche il concorso esterno nel reato associativo che è configurabile in rapporto a sporadiche eventuali situazioni in cui sia necessario il contributo temporaneo, limitato anche ad un unico intervento di un soggetto esterno all'associazione stessa.
Tale contributo può manifestarsi nelle forme più varie, anche nel collaborare con l'associazione mafiosa mediante il procacciamento di risorse finanziarie da destinare a lavori pubblici e nell'aggiudicazione "pilotata" dei relativi appalti, attività che offre al sodalizio la possibilità di accrescere le proprie risorse economiche.
Il criterio selettivo tra imprenditori collusi o non, viene provato dalla giurisprudenza nell'acquisizione di un beneficio innaturale a favore dell'impresa.

F.2 AREE A RISCHIO

Tenuto conto della molteplicità dei rapporti che Ansaldo Green Tech intrattiene sia in Italia sia all'estero, sono state individuate le seguenti aree di attività ritenute più specificamente a rischio:

1. Attività di vendita.
2. Approvvigionamenti ed appalti.
3. Gestione dei rapporti con istituzioni ed enti pubblici.
4. Gestione dei contratti di consulenza.
5. Gestione dei flussi finanziari.
6. Promotori commerciali.
7. Gestione delle partnership.

Per il dettaglio delle attività a potenziale rischio, si rinvia a quanto indicato nei paragrafi A.3.1, A.3.2, A.3.3, A.3.13, A.3.16, A.3.17 e A.3.19.

F.3 PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITA' A RISCHIO

F.3.1 PRINCIPI DI COMPORTAMENTO DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Con riferimento alle tipologie di reati richiamate si pone in rilievo come i relativi rischi appaiano già presidiati dalle regole previste nelle procedure, nel Codice Etico e nelle altre Parti del Modello cui si rimanda.

F.3.2 PROCEDURE DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Tutte le aree individuate come aree a rischio sono presidiate da procedure la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'O.d.V. affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si riportano di seguito le direttive e le procedure da seguire nelle aree di attività a rischio individuate nella presente Parte Speciale.

Direttive di riferimento:

- AE GROUP-DI-002 Export Compliance;
- AE GROUP-DI-004 Appointment of Sales Promoters;
- AE GROUP-DI-007 Managing Intellectual Property Assets;
- AE GROUP-DI-009 Antitrust Directive;
- AE GROUP-DI-012 Whistleblowing.

Procedure di riferimento:

- AE-PR-021 Accounts Receivable Process;
- AE-PR-022 Accounts Payable Process;
- AE-PR-027 Treasury and Trade Finance Process;
- AE-PR-037 Ansaldo Energia Group Travel Management;
- AE-PR-043 Professional Services and Consulting Assignments required without RdA;
- AE-PR-044 Supply Chain management
- AE-PR-050 Intellectual Property Process;
- AE-PR-051 Intellectual Property Contitution Process;
- AE-PR-064 Project Claims Management Process
- AE-PR-069 Intellectual Property Transfer process – Manage Non-Disclosure Agreements;
- AE-PR-070 Intellectual Property Transfer process – Manage Collaborative Research;
- AE-PR-071 Vendor Rating Process;
- AE-PR-072 Vendor Qualification Process;
- AE-PR-082 Due Diligence;
- AE-IN-001 Business travel management;

- AE-IN-004 Purchase Request approval flow e rules;
- AE-IN-006 Passive Payments – Operational Checks Against Supplier Data Cyber Frauds;
- AGT-PR-001 Sales process;
- AGT-PR-002 Supply Management;

PARTE SPECIALE "G"

Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

G.1 LA TIPOLOGIA DEI REATI DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA

G.1.1 PREMESSA

La legge n. 116 del 3 agosto 2009 (pubblicata sulla G.U. n. 188 del 14 agosto 2009), "Ratifica ed esecuzione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione, adottata dalla Assemblea generale dell'ONU il 31 ottobre 2003 con risoluzione n. 58/4, firmata dallo Stato italiano il 9 dicembre 2003, nonché norme di adeguamento interno e modifiche al codice penale e al codice di procedura penale", all'art. 4 introduce nel D.Lgs. 231/01 l'art. 25-*decies* "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria".

G.1.2 INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 377-*BIS* C.P.)

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

Tale reato è anche elencato tra quelli transnazionali.

La fattispecie di cui all'art. 377-*bis* c.p. mira a tutelare la genuinità processuale di quanti sono chiamati a riferire fatti di causa davanti all'Autorità Giudiziaria. È un reato di pericolo il cui evento si verifica con la semplice offerta o promessa finalizzata alla falsità giudiziale. La condotta tipica è costituita sia dall'offerta o dalla promessa di denaro o altra utilità che dalla violenza o minaccia.
La condotta dell'agente è punita a dolo specifico: il subornatore non solo deve avere la coscienza e la volontà dell'offerta o della promessa o della violenza o minaccia, ma deve altresì perseguire il fine di indurre il subornato alla falsità.
Il reato si consuma nel momento e nel luogo in cui l'agente esercita la violenza o la minaccia sulla persona offesa oppure offre o promette il denaro o altra utilità.

G.1.3 FAVOREGGIAMENTO PERSONALE (ART. 378 C.P.)

"Chiunque, dopo che fu commesso un delitto per il quale la legge stabilisce la pena di morte o l'ergastolo o la reclusione, e fuori dei casi di concorso nel medesimo, aiuta taluno a eludere le investigazioni dell'Autorità, o a sottrarsi alle ricerche di questa, è punito con la reclusione fino a quattro anni.
Quando il delitto commesso è quello previsto dall'articolo 416 bis, si applica, in ogni caso, la pena della reclusione non inferiore a due anni.
Se si tratta di delitti per i quali la legge stabilisce una pena diversa, ovvero di contravvenzioni, la pena è della multa fino a lire un milione.
Le disposizioni di questo articolo si applicano anche quando la persona aiutata non è imputabile o risulta che non ha commesso il delitto".

Tale reato rientra nel novero di quelli transnazionali trattati dal D.Lgs. 231/01.

L'interesse tutelato dalla norma è assicurare alla giustizia il regolare svolgimento del processo penale.

Nella previsione dell'art. 378 c.p. sono comprese sia le condotte attive sia quelle omissive di per se stesse idonee ad escludere o favorire le investigazioni o ad intralciare o ritardare le ricerche della polizia. La condotta consiste, dunque, nel frapporre un ostacolo, anche se limitato o temporaneo, allo svolgimento delle indagini.
Il reato di favoreggiamento personale di cui all'art. 378 c.p. è a dolo generico e richiede, quale elemento soggettivo, la consapevolezza che la propria condotta si risolva in un aiuto a favore di chi si sa sottoposto alle investigazioni od alle ricerche dell'autorità.
Il reato si perfeziona nel momento in cui il soggetto attivo ha posto in essere la condotta favoreggiatrice.

G.2. AREE A RISCHIO

Il rischio di commissione dei reati si ritiene diffuso in quanto tutti i destinatari del Modello possono astrattamente, essere chiamati a rispondere davanti all'Autorità Giudiziaria.
Si riportano comunque di seguito le principali area a rischio potenzialmente interessate:

1. Approvvigionamenti ed appalti.
2. Gestione dei rapporti con istituzioni ed enti pubblici.
3. Gestione del contenzioso.
4. Gestione degli affari societari.
5. Gestione dei contratti di consulenza.
6. Selezione del personale.
7. Sistemi di gestione, incentivazione e sviluppo del personale.
8. Promotori commerciali.
9. Omaggi, spese di rappresentanza e di ospitalità, organizzazione di eventi e fiere, sponsorizzazioni e pubblicità.
10. Gestione delle partnership.
11. Gestione dei rapporti con parti correlate.

Per il dettaglio delle attività a potenziale rischio, si rinvia a quanto indicato nei paragrafi A.3.2, A.3.3, A.3.4, A.3.7, A.3.13, A.3.14, A.3.15, A.3.17, A.3.18, A.3.19 e A.3.20.

G.3. PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITA' A RISCHIO

G.3.1 PRINCIPI DI COMPORTAMENTO DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

La Società persegue una politica di trasparenza nelle relazioni con l'Autorità Giudiziaria e più in generale con ogni Autorità che abbia compiti di verifica e controllo inerenti le attività svolte dalla Società.

A tal fine le disposizioni della presente norma si intendono valide non solamente nei confronti degli organi riconducibili all'Autorità Giudiziaria in quanto tali, ma anche a coloro che rivestono funzioni di controllo da parte della Pubblica Amministrazione o di altro Ente.

Pertanto le disposizioni contenute nel presente capitolo sono da riferirsi anche al personale ispettivo quale personale ASL/ INAIL, ecc..

Tutti i Destinatari devono:

- attenersi ai principi del Codice Etico;
- di fronte all'Autorità Giudiziaria comportarsi secondo il massimo rispetto delle norme vigenti nonché delle procedure aziendali;
- mantenere una condotta chiara, trasparente, diligente e di collaborazione con l'Autorità Giudiziaria;
- prestare una fattiva collaborazione e rendere all'Autorità Giudiziaria dichiarazioni veritiere, trasparenti ed esaustivamente rappresentative dei fatti.

La Società vieta espressamente a chiunque di coartare od indurre, in qualsiasi forma e con qualsiasi modalità, nel malinteso interesse di Ansaldo Green Tech, la volontà dei Destinatari di rispondere in maniera mendace o non rispondere all'Autorità giudiziaria ed anzi richiede verità, trasparenza e collaborazione.

Tutti i Destinatari devono tempestivamente avvertire l'Organismo di Vigilanza di ogni violenza o minaccia, pressione, offerta o promessa di danaro o altra utilità, ricevuta al fine di alterare le dichiarazioni da rendere all'Autorità giudiziaria.

G.3.2 PROCEDURE DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Tutte le aree individuate come aree a rischio sono presidiate da procedure la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'O.d.V. affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si riportano di seguito le direttive e le procedure da seguire nelle aree di attività a rischio individuate nella presente Parte Speciale.

Direttive di riferimento:

- AE GROUP-DI-002 Export Compliance;
- AE GROUP-DI-003 Litigation Management;
- AE GROUP-DI-004 Appointment of Sales Promoters;
- AE GROUP-DI-005 Anti-Bribery and Corruption;
- AE GROUP-DI-007 Managing Intellectual Property Assets;
- AE GROUP-DI-009 Antitrust Directive;
- AE GROUP-DI-010 Delegation of Authority.
- AE GROUP-DI-012 Whistleblowing.

Procedure di riferimento:

- AE-PR-022 Accounts Payable Process;
- AE-PR-027 Treasury and Trade Finance Process;
- AE-PR-031 Management of powers attorney;
- AE-PR-034 External and Internal Communication;
- AE-PR-035 Management of hospitality and entertainment expenses, corporate gifts, sponsorships and donations;
- AE-PR-043 Professional Services and Consulting Assignments required without RdA;

- AE-PR-044 Supply Chain management;
- AE-PR-046 Intercompany Transfer Pricing Policy;
- AE-PR-050 Intellectual Property Process;
- AE-PR-051 Intellectual Property Process – IP Constitution;
- AE-PR-064 Project Claims Management Process;
- AE-PR-069 Intellectual Property Transfer process – Manage Non-Disclosure Agreements;
- AE-PR-070 Intellectual Property Transfer process – Manage Collaborative Research;
- AE-PR-071 Vendor Rating Process;
- AE-PR-072 Vendor Qualification Process;
- AE-PR-080 Recruitment process;
- AE-PR-081 Privacy;
- AE-PR-082 Due Diligence;
- AE-IN-004 Purchase Request approval flow e rules;
- AE-IN-006 Passive Payments – Operational Checks Against Supplier Data Cyber Frauds;
- AGT-PR-002 Supply Management;

PARTE SPECIALE "H"

Reati ambientali

H.1 LA TIPOLOGIA DEI REATI AMBIENTALI (ART. 25-*UNDECIES* DEL DECRETO) NONCHÉ IL REATO DI "COMBUSTIONE ILLECITA DEI RIFIUTI"

H.1.1 PREMESSA

L'esigenza di una tutela penale dell'ambiente è avvertita sia a livello comunitario che nazionale. A livello comunitario tale esigenza è stata recepita nella Direttiva del Parlamento europeo e del Consiglio n° 99, del 19 novembre 2008, sulla tutela penale dell'ambiente, secondo la quale ciascuno Stato membro deve adottare le misure necessarie affinché siano perseguibili penalmente una serie di attività «illecite e poste in essere intenzionalmente o quanto meno per grave negligenza».

Il 7 Luglio 2011 è stato approvato il Decreto Legislativo 121/11 di attuazione delle Direttive comunitarie in tema di Reati ambientali, denominato "Attuazione della Direttiva 2008/99/C sulla tutela penale dell'ambiente, nonché della direttiva 2009/123/CE che modifica la direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni". In particolare, il D.Lgs. 121/11 prevede l'introduzione nel D.Lgs. 231/2001 del nuovo art. 25-*undecies* che estende la responsabilità dell'ente ai reati ambientali.

Con riferimento ai criteri di imputazione della responsabilità dell'ente trovano applicazione i seguenti criteri:

- criteri oggettivi di imputazione della responsabilità all'ente, definiti all'art. 5 del D.Lgs. 231/01, laddove stabilisce che i reati-presupposto sono riferibili all'ente solo se commessi (da soggetti apicali o da persone a questi sottoposte) nel suo interesse o a suo vantaggio;
- criterio di imputazione soggettiva, per cui l'adozione del Modello di organizzazione, gestione e controllo mantiene una decisiva funzione esimente della responsabilità dell'ente.

Va tuttavia precisato che, nel caso dei reati ambientali, l'art. 25-*undecies* non riconosce efficacia esimente ai modelli organizzativi di gestione definiti conformemente a standard e Regolamenti internazionali, quali il Regolamento EMAS e la norma UNI EN ISO 14001, come è invece avvenuto con l'introduzione della responsabilità dell'ente per i reati commessi in violazione delle norme sulla sicurezza e prevenzione degli infortuni sul lavoro di cui alla L. 123/2007. Inoltre, a differenza delle norme sulla sicurezza, le norme ambientali non individuano preliminarmente l'organizzazione aziendale, ma si limitano a definire, nell'ambito di norme specifiche, le figure responsabili dell'Ente di fronte alle autorità, ad es. la figura del Titolare dell'autorizzazione agli scarichi idrici o alle emissioni in atmosfera.

Nell'introdurre l'art. 25-*undecies* il legislatore ha operato un rimando solo "parziale" alle norme vigenti in materia di tutela dell'ambiente, selezionando solo specifiche ipotesi di reato ed introducendo *ex novo* le fattispecie di cui agli articoli 727-*bis* e 733-*bis* del Codice Penale.

La Legge 22 maggio 2015 n. 68 ha introdotto nuovi delitti ambientali nel codice penale e, quindi, ampliato anche il novero di quelli contemplati dal D.Lgs. 231/01.

Si riporta di seguito una breve descrizione dei reati, tra quelli contemplati nell'art. 25-*undecies* del Decreto, considerati potenzialmente a rischio per la Società.

H.1.2 NORME PREVISTE DAL CODICE PENALE

a) *Inquinamento ambientale*

È punito con la reclusione da due a sei anni e con la multa da euro 10.000 a euro

100.000 chiunque abusivamente cagiona una compromissione o un deterioramento significativi e misurabili:

1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo;

2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna.

Quando l'inquinamento è prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette, la pena è aumentata da un terzo alla metà. Nel caso in cui l'inquinamento causi deterioramento, compromissione o distruzione di un habitat all'interno di un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, la pena è aumentata da un terzo a due terzi." (art. 452-bis c.p.)

b) *Disastro ambientale*

"Fuori dai casi previsti dall'articolo 434, chiunque abusivamente cagiona un disastro ambientale è punito con la reclusione da cinque a quindici anni.

Costituiscono disastro ambientale alternativamente:

1) l'alterazione irreversibile dell'equilibrio di un ecosistema;

2) l'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali;

3) l'offesa alla pubblica incolumità in ragione della rilevanza del fatto per l'estensione della compromissione o dei suoi effetti lesivi ovvero per il numero delle persone offese o esposte a pericolo.

Quando il disastro è prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette, la pena è aumentata da un terzo alla meta". (art. 452-quater c.p.)

c) *Delitti colposi contro l'ambiente*

"Se taluno dei fatti di cui agli articoli 452-bis e 452-quater è commesso per colpa, le pene previste dai medesimi articoli sono diminuite da un terzo a due terzi.

Se dalla commissione dei fatti di cui al comma precedente deriva il pericolo di inquinamento ambientale o di disastro ambientale le pene sono ulteriormente diminuite di un terzo". (art. 452-quinqies c.p.)

d) *Circostanze aggravanti*

"Quando l'associazione di cui all'articolo 416 è diretta, in via esclusiva o concorrente, allo scopo di commettere taluno dei delitti previsti dal presente titolo, le pene previste dal medesimo articolo 416 sono aumentate.

Quando l'associazione di cui all'articolo 416-bis è finalizzata a commettere taluno dei delitti previsti dal presente titolo ovvero all'acquisizione della gestione o comunque del controllo di attività economiche, di concessioni, di autorizzazioni, di appalti o di servizi pubblici in materia ambientale, le pene previste dal medesimo articolo 416-bis sono aumentate.

Le pene di cui ai commi primo e secondo sono aumentate da un terzo alla metà se dell'associazione fanno parte pubblici ufficiali o incaricati di un pubblico servizio che esercitano funzioni o svolgono servizi in materia ambientale." (art.452 octies c.p.).

H.1.3 NORME PREVISTE DAL TESTO UNICO AMBIENTALE (D.LGS. N. 152/2006)

Gestione di rifiuti non autorizzata (art. 256) e Combustione illecita di rifiuti (art. 256 *bis*)

a) Raccolta, trasporto, recupero, smaltimento, commercio e intermediazione di rifiuti, non pericolosi e pericolosi, in mancanza della prescritta autorizzazione, iscrizione o comunicazione:

Fuori dai casi sanzionati ai sensi dell'articolo 29-quattuordecies, comma 1,chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214, 215 e 216 è punito: a) con la pena di […] se si tratta di rifiuti non pericolosi; b) con la pena di […] e con l'ammenda da […] se si tratta di rifiuti pericolosi (art. 256, comma 1, D.Lgs. n. 152/2006).

"Le pene di cui ai commi 1, 2 e 3 sono ridotte della metà nelle ipotesi di inosservanza delle prescrizioni contenute o richiamate nelle autorizzazioni, nonché nelle ipotesi di carenza dei requisiti e delle condizioni richiesti per le iscrizioni o comunicazioni" (256, comma 4, D.Lgs 152/2006).

b) Realizzazione o gestione di una discarica non autorizzata:

"Fuori dai casi sanzionati ai sensi dell'articolo 29-quattuordecies, comma 1, chiunque realizza o gestisce una discarica non autorizzata è punito con la pena di […] e con l'ammenda da […]. Si applica la pena di […] e dell'ammenda da […] se la discarica è destinata, anche in parte, allo smaltimento di rifiuti pericolosi. Alla sentenza di condanna o alla sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale, consegue la confisca dell'area sulla quale è realizzata la discarica abusiva se di proprietà dell'autore o del compartecipe al reato, fatti salvi gli obblighi di bonifica o di ripristino dello stato dei luoghi" (art. 256, comma 3, D.Lgs. n. 152/2006).

c) Attività non consentite di miscelazione di rifiuti:

"Chiunque, in violazione del divieto di cui all'articolo 187, effettua attività non consentite di miscelazione di rifiuti, è punito […]" (art. 256, comma 5, D.Lgs. n. 152/2006).

d) Combustione illecita di rifiuti:

"Chiunque appicca il fuoco a rifiuti abbandonati ovvero depositati in maniera incontrollata è punito con la reclusione da due a cinque anni. Nel caso in cui sia appiccato il fuoco a rifiuti pericolosi, si applica la pena della reclusione da tre a sei anni. Il responsabile è tenuto al ripristino dello stato dei luoghi, al risarcimento del danno ambientale e al pagamento, anche in via di regresso, delle spese per la bonifica.

Le stesse pene si applicano a colui che tiene le condotte di cui all'articolo 255, comma 1, e le condotte di reato di cui agli articoli 256 e 259 in funzione della successiva combustione illecita di rifiuti.

La pena è aumentata di un terzo se il delitto di cui al comma 1 è commesso nell'ambito dell'attività di un'impresa o comunque di un'attività organizzata. Il titolare dell'impresa

o il responsabile dell'attività comunque organizzata è responsabile anche sotto l'autonomo profilo dell'omessa vigilanza sull'operato degli autori materiali del delitto comunque riconducibili all'impresa o all'attività stessa; ai predetti titolari d'impresa o responsabili dell'attività si applicano altresì le sanzioni previste dall'articolo 9, comma 2, del decreto legislativo 8 giugno 2001, n. 231.

La pena è aumentata di un terzo se il fatto di cui al comma 1 è commesso in territori che, al momento della condotta e comunque nei cinque anni precedenti, siano o siano stati interessati da dichiarazioni di stato di emergenza nel settore dei rifiuti ai sensi della legge 24 febbraio 1992, n. 225.

I mezzi utilizzati per il trasporto di rifiuti oggetto del reato di cui al comma 1 del presente articolo, inceneriti in aree o in impianti non autorizzati, sono confiscati ai sensi dell'articolo 259, comma 2, salvo che il mezzo appartenga a persona estranea alle condotte di cui al citato comma 1 del presente articolo e che non si configuri concorso di persona nella commissione del reato. Alla sentenza di condanna o alla sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale consegue la confisca dell'area sulla quale è commesso il reato, se di proprietà dell'autore o del concorrente nel reato, fatti salvi gli obblighi di bonifica e ripristino dello stato dei luoghi.

Si applicano le sanzioni di cui all'articolo 255 se le condotte di cui al comma 1 hanno a oggetto i rifiuti di cui all'articolo 184, comma 2, lettera e). Fermo restando quanto previsto dall'articolo 182, comma 6-bis, le disposizioni del presente articolo non si applicano all'abbruciamento di materiale agricolo o forestale naturale, anche derivato da verde pubblico o privato" (art. 256 bis D.Lgs. n. 152/2006).

Siti contaminati (art. 257)

e) Inquinamento del suolo, del sottosuolo, delle acque superficiali e delle acque sotterranee con il superamento delle concentrazioni soglia di rischio (sempre che non si provveda a bonifica, in conformità al progetto approvato dall'autorità competente) e omissione della relativa comunicazione agli enti competenti. La condotta di inquinamento è aggravata dall'utilizzo di sostanze pericolose:

"Salvo che il fatto costituisca più grave reato, chiunque cagiona l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio è punito […] se non provvede alla bonifica in conformità al progetto approvato dall'autorità competente nell'ambito del procedimento di cui agli articoli 242 e seguenti. In caso di mancata effettuazione della comunicazione di cui all'articolo 242[2], il trasgressore è punito [...].

Si applica la pena di […] se l'inquinamento è provocato da sostanze pericolose". (art. 257, comma 1 e 2, D.Lgs. n. 152/2006).

Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258)

f) *"Salvo che il fatto costituisca reato, chiunque effettua il trasporto di rifiuti senza il formulario di cui all'articolo 193 o senza i documenti sostitutivi ivi previsti, ovvero riporta nel formulario stesso dati incompleti o inesatti é punito con la sanzione*

[2] Art. 242 Procedure operative ed amministrative
"Al verificarsi di un evento che sia potenzialmente in grado di contaminare il sito, il responsabile dell'inquinamento mette in opera entro ventiquattro ore le misure necessarie di prevenzione e ne dà immediata comunicazione ai sensi e con le modalità di cui all'articolo 304, comma 2. La medesima procedura si applica all'atto di individuazione di contaminazioni storiche che possano ancora comportare rischi di aggravamento della situazione di contaminazione. […]"

amministrativa pecuniaria da milleseicento euro a diecimila euro. Si applica la pena dell'articolo 483 del codice penale nel caso di trasporto di rifiuti pericolosi. Tale ultima pena si applica anche a chi nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto." (art. 258 comma 4 D.Lgs. n. 152/2006).

Traffico illecito di rifiuti (art. 259 e art. 260 abrogato dall'art. 7 D.Lgs. 21/18 ed inserito all'art. 452-*quaterdecies* del c.p.)

g) Spedizione di rifiuti costituente traffico illecito. La condotta è aggravata se riguarda rifiuti pericolosi:

"Chiunque effettua una spedizione di rifiuti costituente traffico illecito ai sensi dell'articolo 26 del regolamento (CEE) 1° febbraio 1993, n. 259[3], o effettua una spedizione di rifiuti elencati nell'Allegato II del citato regolamento in violazione dell'articolo 1, comma 3, lettere a), b), c) e d), del regolamento stesso è punito […]. La pena è aumentata in caso di spedizione di rifiuti pericolosi". (art. 259, comma 1, D.Lgs. n. 152/2006).

h) Attività organizzate per il traffico illecito di rifiuti:

"Chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti è punito […]. (art. 260, c. 1 , D.Lgs. n. 152/2006, abrogato dall'art. 7 D.Lgs. 21/18 ed inserito all'art. 452-quaterdecies del c.p.).

Inquinamento atmosferico (art. 279)

i) Violazione, nell'esercizio di uno stabilimento, dei valori limite di emissione o delle prescrizioni stabiliti dall'autorizzazione, dai piani e programmi o dalla normativa, ovvero dall'autorità competente, che determini anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa:

"Nei casi previsti dal comma 2[4] si applica sempre la pena di […] se il superamento dei valori limite di emissione determina anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa" (art. 279, comma 5, D.Lgs. n. 152/2006).

H.2 AREE A RISCHIO

Tenuto conto dell'attività svolta da Ansaldo Green Tech sono state individuate le seguenti aree di attività ritenute più specificamente a rischio:

1. gestione dei rifiuti;
2. gestione materie prime e tutela delle acque, del suolo e sottosuolo;
3. gestione emissioni in atmosfera;

---

[3] *Si specifica che il citato regolamento è stato abrogato dall'articolo 61 del regolamento (CE) n. 1013/2006, con decorrenza dal 12/07/2007 e che i riferimenti al regolamento abrogato (CEE) n. 259/93 s'intendono fatti al quello del 2006.*

[4] *"Chi, nell'esercizio di uno stabilimento, viola i valori limite di emissione o le prescrizioni stabiliti dall'autorizzazione, dagli Allegati I, II, III o V alla parte quinta del presente decreto, dai piani e dai programmi o dalla normativa di cui all'articolo 271 o le prescrizioni altrimenti imposte dall'autorità competente ai sensi del presente titolo è punito […]. Se i valori limite o le prescrizioni violati sono contenuti nell'autorizzazione integrata ambientale si applicano le sanzioni previste dalla normativa che disciplina tale autorizzazione" (art. 279, comma 2, D. Lgs. n. 152/2006).*

4. gestione delle emergenze.

H.3 IL SISTEMA DI GESTIONE AMBIENTALE DI ANSALDO GREEN TECH

Ansaldo Green Tech ha implementato e mantiene attivo un Sistema di Gestione Ambientale (SGA) secondo la Norma internazionale ISO 14001:2015.

Il SGA di Ansaldo Green Tech è sottoposto a verifiche periodiche e certificato da un Ente accreditato da ACCREDIA che ne attesta la conformità ai requisiti della Norma, con particolare riferimento alla conformità legislativa ambientale applicabile.

La certificazione secondo la ISO 14001:2015 è frutto della scelta volontaria dell'Azienda che ha così deciso di stabilire, attuare, mantenere attivo e migliorare costantemente nel tempo un proprio sistema di gestione ambientale, allineandolo alle *best practice*. Pertanto, la scelta di Ansaldo Green Tech va nella direzione di porre la massima attenzione nello sviluppare e mantenere un sistema di gestione adeguato a tenere sotto controllo gli impatti ambientali delle proprie attività, ricercandone sistematicamente il miglioramento.

I requisiti a cui si è ispirata Ansaldo Green Tech nello sviluppo del proprio SGA sono quelli previsti nella Norma ISO 14001:2015 che, tra l'altro, sono del tutto generali, ovvero applicabili a qualsiasi tipo di organizzazione, e schematizzabili secondo il modello del miglioramento continuo definito dalla metodologia PDCA (Plan-Do-Check-Act, ovvero Pianificare-Attuare-Verificare-Agire).

In considerazione di ciò, Ansaldo Green Tech ha sviluppato un proprio sistema di procedure che definisce, tra l'altro, compiti, responsabilità e flussi di attuazione nelle diverse Fasi sopra citate. Più in particolare il sistema, costruito, tra l'altro, per garantire una sana segregazione delle funzioni, regolamenta:

- per la fase di *pianificazione*, le attività relative a:
    - identificazione e valutazione degli aspetti ambientali;
    - individuazione delle Prescrizioni *ex lege* e delle altre prescrizioni applicabili;
    - definizione di politiche ambientali, di obiettivi con riferimento agli aspetti ambientali e di programmi di miglioramento, di prevenzione e protezione ambientale;
- per la fase di *attuazione*, le attività relative a:
    - definizione di «risorse, ruoli, responsabilità ed autorità» relative al sistema di gestione ambientale;
    - formazione/informazione, ovvero quelle attività volte a fare si che la «competenza, formazione e consapevolezza» delle persone (sia di quelle che lavorano per l'organizzazione sia di quelle che lavorano per conto di essa) le cui attività hanno impatti ambientali, siano sempre adeguate alle esigenze e congrue rispetto al perseguimento della politica ambientale;
    - definizione di un efficace sistema di «comunicazione» all'interno dell'organizzazione e verso l'esterno;
    - l'emissione, il riesame, la modifica, l'aggiornamento, la disponibilità, l'accessibilità, il controllo della «Documentazione» del sistema di gestione ambientale;

- «Controllo operativo» del sistema di gestione ambientale, delle attività e delle operazioni relative agli aspetti ambientali risultati significativi;
- l'individuazione e la gestione delle potenziali emergenze ambientali;

- per la fase di *verifica*, le attività relative a:
  - continuo monitoraggio, sorveglianza e misurazione (i) delle operazioni che possono avere impatti ambientali significativi, (ii) del raggiungimento degli obiettivi prefissati e (iii) della corretta taratura della strumentazione di monitoraggio ambientale;
  - verifica periodica e sistematica del rispetto delle prescrizioni previste dalla legge e delle altre eventuali prescrizioni (es. procedure ed istruzioni operative aziendali) sottoscritte dall'organizzazione;
  - gestione delle «non conformità, azioni correttive ed azioni preventive» rilevate a seguito di un mancato soddisfacimento di un requisito;
  - controllo sistematico delle registrazioni rilevanti;
  - conduzione di Audit interni;
- per la fase di *reazione*, le attività relative al periodico (ovvero in caso di incidenti/problematiche rilevanti) Riesame del SGA da parte della Direzione e alla gestione delle decisioni conseguenti al Riesame.

Il complesso delle procedure è disponibile presso l'Unità di Ansaldo Energia che si occupa del sistema documentale e/o dei sistemi di gestione certificati e viene diffuso a tutti i soggetti interessati. Le procedure sono, inoltre, disponibili nella Intranet aziendale.

H.3.1 L'ORGANIZZAZIONE PER LA GESTIONE AMBIENTALE

La Società utilizza per la formalizzazione delle funzioni, dei compiti e della responsabilità dei diversi Enti e Unità aziendali, specifici documenti organizzativi (vedi paragrafo 2.7 della Parte Generale del presente Modello).

Anche in tema di tutela dell'ambiente vengono utilizzati gli indicati documenti organizzativi che evidenziano compiti e responsabilità per i diversi soggetti secondo il principio della responsabilità connessa alle attività da ciascuno dirette, controllate o eseguite e per l'area di lavoro di competenza.

L''Amministratore Delegato quale legale rappresentante in forza dei poteri conferiti, è il titolare della posizione di garanzia in materia ambientale nell'ambito della Società Ansaldo Green Tech.
L'Amministratore Delegato per l'espletamento dei compiti in materia ambientale si avvale della collaborazione di delegati e sub - delegati ai quali sono stati conferite le funzioni e i poteri necessarie in considerazione della loro idoneità tecnica, esperienza e capacità professionale.

La Società si avvale, inoltre, del supporto delle Strutture di Ansaldo Energia competenti in materia di ambiente e di salute e sicurezza su lavoro.

H.4 PRINCIPI DI COMPORTAMENTO8 E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITA' A RISCHIO

H.4.1 PRINCIPI DI COMPORTAMENTO DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

La presente Parte Speciale prevede l'espresso divieto – a carico degli Esponenti Aziendali in via diretta, ed a carico dei Collaboratori esterni e Partner tramite apposite clausole contrattuali -, di porre in essere collaborare o dare causa alla realizzazione di comportamenti tali che considerati individualmente o collettivamente:

- integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-*undecies* del D.Lgs. 231/2001);
- possano compromettere i presidi di tutela ambientale adottati dalla Società favorendo potenzialmente la commissione dei reati ambientali di cui all'art. 25-*undecies* del D. Lgs. 231/2001;
- costituiscano violazione alle procedure aziendali o, comunque, siano da ritenersi non in linea con i principi espressi dal presente Modello e del Codice Etico;
- siano tesi ad impedire, intralciare, eludere, compromettere gli esiti dell'attività di vigilanza e controllo ambientali sia che essa sia svolta per conto della Società sia che sia svolta da autorità di controllo.

È fatto, inoltre, obbligo di:

- osservare tutti i dettami previsti dal D.lgs. 152/06 e s.m.i. o da altre leggi e regolamenti in materia ambientale applicabili;
- osservare le procedure che disciplinano l'attività aziendale, con particolare riferimento al Modello di Governance aziendale di Ansaldo Green Tech ed alle procedure del SGA
- osservare le prescrizioni contenute nelle autorizzazioni ambientali ove presenti.

In tema di deleghe di responsabilità e nomine/designazioni delle funzioni rilevanti per la tutela dell'ambiente viene garantito che:

- le deleghe in materia ambientale sono adeguatamente formalizzate, con la specifica indicazione dei poteri delegati, la firma da parte dei soggetti incaricati, e pubblicizzate all'interno della Società e all'esterno ove richiesto;
- il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
- il sistema delle deleghe, nomine e designazioni è coerente con l'evoluzione dell'organizzazione societaria;
- le Unità organizzative incaricate di compiti rilevanti per la tutela ambientale sono dotate dei poteri di organizzazione, gestione e controllo, ed eventualmente di spesa, adeguati alla struttura e alla dimensione dell'organizzazione e alla natura dei compiti assegnati in considerazione anche della possibilità del verificarsi di casi di urgenze non prevedibili né rinviabili.

I Destinatari devono esercitare un controllo continuo e puntuale teso ad evidenziare i rischi che potrebbero comportare la realizzazione dei reati indicati nell'art. 25-*undecies* ed, in generale, qualunque situazione che possa comportare un pericolo per la tutela ambientale.

Le attività connesse con il presente profilo di rischio devono essere gestite nel rispetto delle norme applicabili e del sistema normativo aziendale che, oltre a inglobare i principi espressi

nel Codice Etico e gli obblighi e divieti sopra evidenziati, prevede che i destinatari garantiscano, nell'ambito delle proprie responsabilità e competenze:

- la definizione e l'aggiornamento, in base ai cambiamenti nella struttura organizzativa ed operativa della Società, di procedure specifiche per la prevenzione dei potenziali impatti ambientali connessi con l'attività, in cui siano disciplinate le modalità di gestione delle attività sensibili identificate;
- l'acquisizione di documentazioni e certificazioni obbligatorie di legge e la loro conservazione;
- il controllo sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate in materia ambientale e della conformità alla legislazione vigente;
- un adeguato livello di informazione/formazione dei dipendenti e informazione dei fornitori/appaltatori, sul sistema procedurale ambientale definito dalla Società e sulle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole di comportamento e controllo definite dalla Società stessa;
- l'attuazione di attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni in materia ambientale anche nei confronti degli appaltatori;
- l'attuazione di periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate;
- un efficace sistema di coordinamento e adeguati flussi informativi tra le Unità coinvolte.

I principi di controllo specifici, definiti per disciplinare le attività di **gestione dei rifiuti** prodotti dall'organizzazione affinché le stesse siano svolte in conformità ai requisiti normativi e autorizzativi vigenti, prevedono la definizione di ruoli, responsabilità e modalità operative per garantire:

- il rispetto di tutti gli adempimenti previsti dalle norme in capo al produttore del rifiuto;
- il rispetto dei termini temporali per le annotazioni sul registro di carico e scarico dei rifiuti e per la presentazione della dichiarazione annuale (MUD);
- l'adeguatezza delle aree di deposito, anche con riferimento a particolari tipologie di rifiuti speciali pericolosi, ed il rispetto dei requisiti previsti dalla normativa applicabile per il deposito temporaneo (limiti quantitativi, qualitativi e temporali);
- l'identificazione dei rifiuti e l'attribuzione del codice CER e delle eventuali caratteristiche di pericolosità nel rispetto di quanto previsto dalle norme di settore;
- il ricorso, ove necessario, ad analisi di caratterizzazione dei rifiuti effettuate da laboratori qualificati previa individuazione della frequenza di caratterizzazione, delle modalità di campionamento e di adeguati flussi informativi verso i laboratori di analisi in merito alla provenienza e composizione dei campioni da analizzare;
- la vigilanza sulla correttezza/esaustività delle informazioni contenute nei certificati di analisi sui rifiuti forniti dai laboratori terzi;
- la corretta compilazione delle schede di omologa ove richieste;
- la qualifica iniziale e la verifica periodica del possesso e della validità delle iscrizioni/comunicazioni/autorizzazioni previste dalle norme per la gestione dei rifiuti da parte dei soggetti terzi (intermediari, trasportatori, smaltitori) a cui vengono attribuite responsabilità in merito alla gestione dei rifiuti prodotti (inclusa

la permanenza della validità delle fidejussioni prestate, ove previste, ed eventuali altre prescrizioni contenute nelle specifiche autorizzazioni);

- la verifica della correttezza e completezza della documentazione di trasporto (formulari di identificazione dei rifiuti), inclusa la verifica delle targhe dei mezzi utilizzati ed il possesso dei requisiti previsti dalla norma ADR, ove applicabile (cartellonistica, equipaggiamenti, documenti di trasporto);
- la verifica della presenza della documentazione attestante il corretto smaltimento dei rifiuti (es. IV copia del formulario) da ricevere entro i tempi previsti dalla norma applicabile e l'adozione dei provvedimenti di legge, ove previsti;
- la tracciabilità di tutte le attività relative alla gestione dei rifiuti;

Le norme aziendali prevedono, inoltre, il divieto di:

- trasporto in conto proprio di rifiuti prodotti in assenza dei requisiti previsti dalle norme;
- spedizione transfrontaliera di rifiuti, ove necessario, in assenza dei requisiti previsti dalle norme;
- combustione dei rifiuti;
- miscelazione dei rifiuti pericolosi con i rifiuti non pericolosi e di rifiuti pericolosi che abbiano caratteristiche di pericolosità differenti.

I principi di controllo specifici, definiti per disciplinare le attività di **gestione materie prime e tutela delle acque, del suolo e sottosuolo** da parte dell'organizzazione al fine di prevenire fenomeni di contaminazione, prevedono:

- che tutte le attività siano svolte su aree pavimentate e tutti i contenitori siano posizionati su bacini di contenimento grigliati e mobili;
- il divieto di scaricare prodotti liquidi pericolosi all'interno dei lavabi, dei tombini e delle griglie per la raccolta delle acque meteoriche presenti nei piazzali;
- l'obbligo di gestire e smaltire i residui liquidi come rifiuti;
- un adeguato e tempestivo intervento in caso di eventi accidentali che possano comportare fenomeni di inquinamento delle acque, del suolo e/o sottosuolo anche mediante l'utilizzo di presidi (es: materiali assorbenti, scope, pale, ecc.) opportunamente resi disponibili in reparto;
- esercitazioni periodiche per la messa in pratica delle procedure di intervento in emergenza;
- la comunicazione ex art. 242 del D.Lgs 152/06 e s.m.i. al verificarsi di un evento che sia potenzialmente in grado di contaminare il sito;
- ove necessario, la bonifica dei siti inquinati in conformità a progetti approvati dall'Autorità competente nell'ambito del procedimento di cui agli articoli 242 e seguenti del D.Lgs 152/06 e s.m.i..

I principi di controllo specifici, definiti per disciplinare le attività di **gestione delle emissioni in atmosfera** dell'organizzazione affinché gli stessi siano conformi ai requisiti normativi ed autorizzativi vigenti, prevedono la definizione di ruoli, responsabilità e modalità operative per garantire:

- l'identificazione di tutte le attività che generano emissioni e di tutti i punti di emissione;
- l'identificazione della necessità di richiesta di una nuova autorizzazione o di rinnovo, modifica, aggiornamento di autorizzazioni preesistenti e la predisposizione della relativa istruttoria nonché le necessarie verifiche di completezza ed accuratezza sulla documentazione prevista dall'iter autorizzativo;
- il monitoraggio delle tempistiche per l'ottenimento del rinnovo/modifica delle autorizzazioni esistenti e la comunicazione dell'avvenuto ottenimento dell'autorizzazione, sua modifica e/o rinnovo alle figure interessate;
- l'individuazione e il monitoraggio puntuale di tutte le prescrizioni (anche quelle una tantum) previste dai provvedimenti autorizzativi e la conduzione delle attività e degli impianti, compresa la relativa manutenzione, in modo da garantire il rispetto di tutte le prescrizioni;
- la segregazione delle funzioni coinvolte nel processo di ottenimento e gestione dei provvedimenti autorizzativi.

I principi di controllo specifici, definiti per disciplinare le attività di **gestione delle emergenze** prevedono:

- l'individuazione delle attività critiche e delle situazioni di emergenza che possono avere un impatto sull'ambiente;
- l'individuazione dei ruoli, responsabilità e modalità di prevenzione, mitigazione e risposta alle situazioni di emergenza con possibile impatto sull'ambiente e organizzazione dei necessari rapporti con i servizi pubblici competenti in materia;
- l'aggiornamento delle norme aziendali di preparazione e risposta alle emergenze, in particolare dopo che si sono verificati incidenti o situazioni di emergenza;
- la definizione e attuazione di programmi di formazione e addestramento del personale riguardo ai possibili incidenti con conseguenze per l'ambiente;

Poiché, inoltre, nell'ambito delle aree a rischio assumono rilevanza i comportamenti di terzi cui l'organizzazione può affidare lo svolgimento di parte delle attività, i principi di controllo specifico prevedono l'esistenza di una norma aziendale che disciplini le attività di selezione dei fornitori, successivo affidamento dei contratti e monitoraggio delle prestazioni, tesa a garantire che i fornitori a cui vengono affidate attività rilevanti da un punto di vista ambientale siano idonei da un punto di vista tecnico, professionale e autorizzativo e siano vincolati contrattualmente al rispetto delle norme ambientali vigenti e ai requisiti specifici stabiliti dall'organizzazione. In particolare, tale norma aziendale definisce ruoli, responsabilità e modalità operative per garantire:

- l'identificazione delle tipologie di fornitori rilevanti da un punto di vista ambientale;
- la qualifica iniziale dei fornitori attraverso la verifica del rispetto di requisiti normativi ad essi applicabili e delle loro prestazioni ambientali;
- la verifica periodica della permanenza della validità di requisiti specifici necessari per la qualifica iniziale e lo svolgimento delle attività da parte dei fornitori;
- la definizione delle informazioni che devono essere date ai fornitori riguardo le norme e prescrizioni da rispettarsi nell'ambito dello svolgimento della loro attività in partnership e/o per conto della Società;

- la vigilanza sull'operatività dei fornitori anche con particolare riferimento alla combustione illecita dei rifiuti;
- la segnalazione di scostamenti rispetto a quanto previsto dalle norme ambientali vigenti e ai requisiti specifici stabiliti dall'organizzazione e la definizione di azioni correttive atte a evitare il ripetersi degli scostamenti individuati;
- la tracciabilità di tutte le attività relative al processo di selezione e affidamento a terzi di attività rilevanti da un punto di vista ambientale e di tutte le attività relative al processo di monitoraggio delle prestazioni dei fornitori.

Il personale della società, a qualsiasi titolo coinvolto in attività che comportino impatti ambientali, è tenuto ad osservare le modalità esposte nel presente documento, le previsioni di legge esistenti in materia nonché le norme comportamentali richiamate anche nel Codice Etico.

H.4.2 PROCEDURE DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Tutte le aree individuate come aree a rischio sono presidiate da procedure la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'O.d.V. affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si riportano di seguito le direttive e le procedure da seguire nelle aree di attività a rischio individuate nella presente Parte Speciale.

Direttiva di riferimento:

- AE GROUP-DI-012 Whistleblowing.

Procedure di riferimento:

- AE-PR-001 Ansaldo Energia Group Management System Documents;
- AE-PR-101 Compliance with EHS legislative regulations and other requirements;
- AE-PR-102 EHS Requisites for Procurement;
- AE-PR-104 Environmental aspects identification and management;
- AE-PR-105 EHS Training;
- AE-PR-107 EHS Surveillance and Performance Measurement;
- AE-PR-108 EHS Non Conformity and corrective actions;
- AE-PR-201 Waste Management;
- AE-PR-202 Air Emission Control;
- AE-PR-205 Soil and groundwater protection and management of possible spillage;
- AE-PR-206 Hazardous Materials Management;
- AE-PR-210 EHS Incident and near miss management;
- AE-PR-211 EHS Project Plan (SITES);
- AE-PR-212 EHS System implementation on sites;
- AE-PR-213 Contractor and Outsourcer Performance Inspection;
- AE-PR-214 Emergency preparedness and management;
- AE-PR-229 Housekeeping;

- AGT-ENV-001 Servizio di raccolta e smaltimento dei rifiuti speciali di Ansaldo Green Tech S.p.A. stabilimento di C.so Perrone 118.

PARTE SPECIALE "I"

Delitti contro l'industria e il commercio

I.1 LA TIPOLOGIA DEI DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

I.1.1 PREMESSA

Come evidenziato nella Parte Generale, la legge 99 del 23 luglio 2009 ha esteso la disciplina del Decreto ad alcune fattispecie di reato inerenti i ***delitti contro l'industria e il commercio***, introducendo l'art. 25-*bis*.1.
Di questi in seguito all'attività di analisi alcuni sono ritenuti in via astratta realizzabili a vantaggio della Società. Nel seguito di questo paragrafo sono evidenziati i reati contemplati nell'art. 25-*bis*.1 astrattamente applicabili.

I. 1.2 VENDITA DI PRODOTTI INDUSTRIALI CON SEGNI MENDACI (ART. 517 C.P.)

"Chiunque pone in vendita o mette altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa fino a ventimila euro."

Il delitto di cui all'art. 517 c.p., modificato dalla legge n. 99 del 2009 solo per inasprirne l'apparato sanzionatorio, portando la reclusione fino ai due anni, funge da chiusura del sistema codicistico di tutela penale dei marchi, anche se l'interesse tutelato non è il sistema *extra*-penale di tutela dei marchi e dei segni distintivi, ma piuttosto l'ordine economico e la generalità dei consumatori, che potrebbero essere ingannati nelle proprie scelte di acquisto. Il delitto ha carattere sussidiario, in quanto le condotte ivi previste sono punite solo allorché non siano considerate come reato da altre disposizioni di legge.
La sfera giuridica tutelata dal delitto di vendita di prodotti industriali con segni mendaci mira a colpire condotte tipiche di falso ideologico, cioè punisce l'utilizzazione di marchi mendaci, vale a dire quei marchi che, senza costituire copia o imitazione di un marchio registrato, per il contenuto o per il rapporto in cui si trovano con il prodotto, sono idonei ad indurre in errore i consumatori.
Inoltre, per la configurabilità della fattispecie, non occorre che il marchio imitato sia registrato o riconosciuto a norma della legge interna o internazionale.
Sul fronte dei potenziali soggetti attivi, occorre evidenziare come il reato rientri nella categoria dei reati comuni. Pertanto, non sono solo gli amministratori a poter porre in essere tali condotte, ma anche i loro collaboratori, che potranno rispondere sia a titolo di concorso, quando abbiano cooperato consapevolmente con gli amministratori, sia a titolo autonomo, quando abbiano agito su loro esclusiva iniziativa.
L'art. 517 prevede due condotte alternative consistenti nel "porre in vendita", ovvero nel "mettere altrimenti in circolazione" prodotti con attitudine ingannatoria. La prima condotta consiste nell'offerta di un determinato bene a titolo oneroso, mentre la seconda ricomprende qualsiasi forma di messa in contatto della merce con il pubblico, anche e titolo oneroso.
Anche la mera presentazione di prodotti industriali con segni mendaci alla dogana per lo sdoganamento può integrare il delitto in esame (Cass. Sez. III n. 232469/05).
Di vitale importanza per l'integrazione degli estremi del delitto è l'attitudine ingannatoria che deve avere il prodotto imitato; in altri termini, il prodotto deve poter trarre in inganno il consumatore di media diligenza, anche se poi non si concretizza il reale danno al consumatore, poiché la fattispecie è di pericolo concreto.
Il mendacio ingannevole può cadere anche sulle modalità di presentazione del prodotto, cioè in quel complesso di colori, immagini, fregi, che possono indurre l'acquirente a falsare il giudizio sulla qualità o la provenienza della merce offerta.
Il reato, infine, richiede il dolo generico, occorre, quindi, la mera consapevolezza dell'attitudine decettiva della veste di presentazione del prodotto.

I. 1.3 FABBRICAZIONE E COMMERCIO DI BENI REALIZZATI USURPANDO TITOLI DI PROPRIETÀ INDUSTRIALE (ART. 517-*TER* C.P.)

"Salva l'applicazione degli articoli 473 e 474 chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, fabbrica o adopera industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso è punito, a querela della persona offesa, con la reclusione fino a due anni e con la multa fino a euro 20.000.
Alla stessa pena soggiace chi, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i beni di cui al primo comma.
Si applicano le disposizioni di cui agli articoli 474-bis, 474-ter, secondo comma, e 517-bis, secondo comma.
I delitti previsti dai commi primo e secondo sono punibili sempre che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale".

L'art. 517-*ter* c.p., inserito dall'art. 15 comma 1 della L. n. 99 del 23 luglio 2009, sostituisce, con talune modifiche ed aggiunte, la fattispecie di cui al primo comma dell'art.127 D. Lgs. 10 febbraio 2005 n. 30, c.d. codice della proprietà industriale.
L'art. 517-*ter* scatta, quindi, sicuramente nei casi di usurpazione illegittima di brevetto, ma anche nei casi di concorrenza sleale per imitazione servile, cioè quella che pur non potendo essere ascritta alla contraffazione *tout court*, è in grado di generare confusione nel pubblico circa la "provenienza imprenditoriale" dei prodotti imitati. L'imitazione deve cadere sulla forma del prodotto o della sua confezione (contorni, colori, superfici, layout/caratterizzazione grafica), in maniera tale da "comunicare" la provenienza da un'impresa del prodotto stesso (c.d. forma distintiva o individualizzante, come il marchio di forma).
Si tratta di un delitto a tutela sicuramente del patrimonio e differisce (sostituendolo) dall'art. 127 D. Lgs. 10 febbraio 2005 n. 30 per una certa rilevanza dell'elemento soggettivo, e lo conferma la misura maggiore della pena edittale.

I.2. AREE A RISCHIO

Sono state individuate le seguenti aree di attività ritenute più specificamente a rischio dei reati in analisi:

1. Attività di vendita.
2. Approvvigionamenti ed appalti.
3. Gestione delle commesse.
4. Gestione dei contratti di consulenza.
5. Promotori commerciali.
6. Gestione delle partnership.

Per il dettaglio delle attività a potenziale rischio, si rinvia a quanto indicato nei paragrafi A.3.1, A.3.2, A.3.6, A.3.13, A.3.17 e A.3.19.

I.3. PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITA' A RISCHIO

I.3.1 PRINCIPI DI COMPORTAMENTO DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

A tutti i Destinatari del Modello (in considerazione dei diversi obblighi e posizioni che ciascuno assume nei confronti della Società) è fatto divieto di porre in essere comportamenti che possano rientrare nelle fattispecie di reato richiamate nel paragrafo I.1 della presente Parte Speciale.

In particolare, nell'espletamento delle attività considerate sensibili, i Destinatari dovranno attenersi ai seguenti principi generali di condotta:

- astenersi dal porre in essere qualsiasi situazione il cui scopo si risolva nel compiere attività finalizzate a turbare la libertà dell'industria e del commercio;
- verificare, nel caso di acquisto di beni/componenti da terzi, che questi non siano stati prodotti impiegando elementi soggetti a diritti di privativa;
- verificare, nel caso di realizzazione di componenti/progettazione di componenti, che non siano utilizzati componenti e/o disegni soggetti a diritti di privativa.

I.3.2 PROCEDURE DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Tutte le aree individuate come aree a rischio sono presidiate da procedure la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'O.d.V. affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si riportano di seguito le direttive e le procedure da seguire nelle aree di attività a rischio individuate nella presente Parte Speciale.

Direttive di riferimento:

- AE GROUP-DI-002 Export Compliance;
- AE GROUP-DI-004 Appointment of Sales Promoters;
- AE GROUP-DI-007 Managing Intellectual Property Assets;
- AE GROUP-DI-009 Antitrust Directive;
- AE GROUP-DI-012 Whistleblowing.

Procedure di riferimento:

- AE-PR-021 Accounts Receivable Process;
- AE-PR-022 Accounts Payable Process;
- AE-PR-027 Treasury and Trade Finance Process;
- AE-PR-043 Professional Services and Consulting Assignments required without RdA;
- AE-PR-044 Supply Chain management;
- AE-PR-050 Intellectual Property Process;
- AE-PR-051 Intellectual Property Contitution Process;
- AE-PR-064 Project Claims Management Process;
- AE-PR-069 Intellectual Property Transfer process – Manage Non-Disclosure Agreements;

- AE-PR-070 Intellectual Property Transfer process – Manage Collaborative Research;
- AE-PR-071 Vendor Rating Process;
- AE-PR-072 Vendor Qualification Process;
- AE-PR-082 Due Diligence;
- AE-IN-004 Purchase Request approval flow e rules;
- AE-IN-006 Passive Payments – Operational Checks Against Supplier Data Cyber Frauds;
- AGT-PR-001 Sales process;
- AGT-PR-002 Supply Management;
- AGT-PR-005 Project Management;
- AGT-PR-006 Phase Review Management.

PARTE SPECIALE "L"

Reato di autoriciclaggio

L.1 IL REATO DI AUTORICICLAGGIO (ART. 648-*TER.1*)

Come evidenziato nella premessa della Parte Speciale D, la Legge 15 dicembre 2014, n. 186, ha introdotto nell'ordinamento giuridico italiano l'art. 648-*ter.1* del Codice Penale prevedendo una nuova fattispecie di reato, il ***reato di autoriciclaggio.*** Tale norma ha modificato l'art. 25-*octies* del Decreto, collocando la nuova fattispecie accanto ai reati di *"ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita"*.

Il reato è stato emendato dal Dlgs n. 195 del 2021 che ha dato attuazione alla direttiva (UE) 2018/1673 del Parlamento Europeo e del Consiglio, del 23 ottobre 2018, sulla lotta al riciclaggio mediante il diritto penale.

A seguito della riforma, l'articolo 648*.ter.1* del Codice Penale così recita: *"si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo 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.*

La pena è della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi.

La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni.

Si applicano comunque le pene previste dal primo comma se il denaro, i beni o le altre utilità provengono da un delitto commesso con le condizioni o le finalità di cui all'articolo 416 bis.1.

Fuori dei casi di cui ai commi precedenti, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale. La pena è aumentata quando i fatti sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale.

La pena è diminuita fino alla metà per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto. Si applica l'ultimo comma dell'articolo 648".

Fino alla introduzione della L. 186/14, il legislatore aveva configurato le condotte di ricettazione, riciclaggio e impiego di denaro, beni o altre utilità di provenienza illecita come reati contestabili solo a soggetti diversi dall'autore del reato presupposto. La novità della L. 186/14 sta nel punire colui che, dopo aver commesso o concorso a commettere un reato, impiega, sostituisce o trasferisce in attività economiche, finanziarie, imprenditoriali o speculative, denaro, beni o altre utilità provenienti dalla commissione di tale reato, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

La responsabilità degli Enti, con riguardo al reato di autoriciclaggio si configura in tutti i casi in cui, a seguito di un reato, l'Ente impieghi le utilità che ne derivano per lo svolgimento della propria attività. In generale, quindi, tutti i reati commessi nell'interesse o a vantaggio dell'Ente che generano un'utilità possono essere considerati astrattamente presupposto del reato di autoriciclaggio.

Ancorché, come sopra evidenziato, qualsiasi reato che generi un'utilità per l'Ente possa in astratto costituire presupposto per il compimento del reato di autoriciclaggio per la Società, Ansaldo Green Tech ha, comunque, provveduto ad effettuare un'analisi volta ad individuare più specificatamente quali delitti possano configurarsi, in via astratta, nello svolgimento

delle proprie attività, tali da comportare il rischio di commissione del reato di autoriciclaggio.

La Società ha, quindi, innanzitutto considerato come reati presupposto dell'autoriciclaggio, i reati, tra quelli rientranti nel novero del Decreto 231/01, già ritenuti potenzialmente a rischio e quindi già trattati nelle Parti Speciali precedenti o a fronte dei quali sono stati comunque individuati dei principi di comportamento nella Parte Generale, nonché dei principi nel Codice Etico.

Tenuto conto però del fatto che delitto presupposto del reato di autoriciclaggio può essere anche un reato non contemplato dal Decreto 231/01, l'analisi è stata condotta, come si accennava in precedenza, anche sugli altri reati previsti dalle fonti principali dell'ordinamento italiano. Dall'esito di tale analisi è emerso che la Società ritiene astrattamente commissibili e, quindi, potenziale fonte di autoriciclaggio i reati di seguito riportati e suddivisi in macro-categorie:

- **REATI DI FALSO:**
  - Falso giuramento della parte (art. 371 c.p.);
  - False informazioni al pubblico ministero o al procuratore della Corte penale internazionale (art. 371-*bis* c.p.);
  - False dichiarazioni al difensore (art. 371-*ter* c.p);
  - Falsa testimonianza (art. 372 c.p.);
  - False dichiarazioni o attestazioni in atti destinati all'autorità giudiziaria o alla Corte penale internazionale (art. 374-*bis* c.p.);
  - Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.);
  - Falsità materiale commessa d pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.);
  - Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.);
  - Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative (art. 480 c.p.);
  - Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.);
  - Falsità materiale commessa dal privato (art. 482 c.p.);
  - Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.);
  - Falsità in registri e notificazioni (art. 484 c.p.);
  - Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.);
  - Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.);
  - Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.);
  - Uso di atto falso (art. 489 c.p.);
  - Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.);
  - Documenti equiparati agli atti pubblici agli effetti della pena (art. 491. c.p.);
  - Falsa attestazione o dichiarazione a un pubblico ufficiale sulla identità o su qualità personali proprie o di altri (art. 495 c.p.);
  - Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri (art. 495-*bis* c.p.);
  - False dichiarazioni sull'identità o su qualità personali proprie o di altri (art. 496 c.p.);
- **REATI TRIBUTARI COSÌ COME MODIFICATI DAL D.LGS 158/2015:**
  - Omesso versamento di ritenute certificate (art. 10-*bis* D.Lgs. 74/2000);
  - Omesso versamento di IVA (art. 10-*ter* D.Lgs. 74/2000);
- **REATI CONTRO L'AMMINISTRAZIONE DELLA GIUSTIZIA:**
  - Frode processuale (art. 374 c.p.);

  - Intralcio alla giustizia (art. 377 c.p.);
  - Rivelazione di segreti inerenti a un procedimento penale (art. 379-*bis* c.p.);
- **REATI CONTRO LA PUBBLICA AMMINISTRAZIONE:**
  - Abuso di ufficio (art. 323 c.p.);
  - Rivelazione ed utilizzazione di segreti di ufficio (art. 326 c.p.);
  - Millantato credito (art. 346 c.p.);
  - Violazione di sigilli (art. 349 c.p.);
  - Astensione dagli incanti (art. 354 c.p.);
- **REATI CONTRO L'ECONOMIA PUBBLICA:**
  - Rialzo e ribasso fraudolento di prezzi sul pubblico mercato o nelle borse di commercio (art. 501 c.p.);
  - Manovre speculative su merci (art. 501-*bis* c.p.);
- **DELITTI CONTRO L'INCOLUMITÀ PUBBLICA:**
  - Crollo di costruzioni o altri disastri dolosi (art. 434 c.p.);
  - Rimozione od omissione dolosa di cautele contro infortuni sul lavoro (art.437 c.p.);
- **REATI CONTRO IL PATRIMONIO:**
  - Furto (art. 624 c.p.);
  - Estorsione (art. 629 c.p.);
  - Danneggiamento (art. 635 c.p.);
  - Truffa (art. 640 c.p.);
  - Fraudolento danneggiamento dei beni assicurati (art. 642 c.p.);
  - Appropriazione indebita (art. 646 c.p);
- **ALTRI REATI:**
  - Associazioni sovversive (art. 270 c.p.);
  - Infedeltà patrimoniale (art. 2634 c.c.);
  - Combustione illecita dei rifiuti (art. 256-*bis* D.Lgs. 152/06).

L.2. AREE A RISCHIO

Per quanto concerne il reato di autoriciclaggio, in considerazione del fatto che qualsiasi reato che arrechi un'utilità per la Società possa comportare la commissione di tale reato, si ritiene di valutare il rischio della commissione del reato in analisi come rischio diffuso. Pertanto, tutte le aree aziendali sono in astratto a rischio di commettere un reato presupposto per la commissione del reato di autoriciclcaggio, nel caso in cui la Società impieghi, sostituisca o trasferisca il denaro, i beni o le altre utilità, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

L.3. PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITA' A RISCHIO

L.3.1 PRINCIPI DI COMPORTAMENTO DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Nel presente paragrafo si riportano i principi da rispettare al fine di prevenire la commissione dei reati elencati al paragrafo L.1, non colposi e non annoverati dal Decreto 231/01, ma considerati a rischio per la Società in quanto presupposto del reato di autoriciclaggio.

In merito ai reati contemplati dal Decreto, che la Società ha già considerato a rischio e che costituiscono potenzialmente anche presupposto del reato di autoriciclaggio, per la trattazione dei principi volti a prevenire la loro commissione, e quindi l'autoriciclaggio, si rinvia alle altre Parti Speciali, nonché alla Parte Generale e al Codice Etico.

La presente Parte Speciale prevede:

- l'espresso divieto a tutti i Destinatari di porre in essere, o anche tollerare che altri pongano in essere, comportamenti:
    - tali da integrare le fattispecie dei delitti presupposto del reato di autoriciclaggio sopra considerate;
    - che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
    - non conformi alle procedure o, comunque, non in linea con i principi espressi dal presente Modello e dal Codice Etico;
    - volti ad impiegare in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto;
- l'obbligo ai Destinatari di:
    - tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme nazionali ed internazionali vigenti, del Codice Etico, dei principi contenuti nel presente Modello e delle procedure aziendali;
    - evitare di porre in essere azioni - o dare causa alla realizzazione di comportamenti - tali che integrino direttamente o indirettamente le fattispecie di reato rientranti in quelle sopra illustrate;
    - osservare una condotta tesa a garantire il regolare funzionamento di Ansaldo Green Tech, assicurando ed agevolando ogni forma di controllo sulle attività aziendali da parte dell'O.d.V.;
    - curare che nessun rapporto venga iniziato con persone o enti che non abbiano intenzione di adeguarsi ai principi etici della Società.

Con specifico riferimento alla classe di reati di falso, è fatto obbligo ai Destinatari di:

- non giurare il falso;
- non dare false informazioni/dichiarazioni a rappresentanti della PA ed al proprio difensore;
- non richiedere a rappresentanti della PA di produrre falsi documenti, autorizzazioni, certificati;
- non firmare/richiedere di firmare a collaboratori o terzi documenti in bianco;
- non usare per qualsiasi fine un atto/documento falso;
- non distruggere o occultare atti che possano avere fine probatorio;
- non dare/dichiarare generalità false proprie o di altri.

Con specifico riferimento alla classe di reati tributari:

- è fatto obbligo ai Destinatari di:
    - non simulare operazioni (per es. emissioni fatture o altri documenti per operazioni inesistenti) per ottenere un beneficio fiscale;
    - non omettere di effettuare dichiarazioni fiscali;
    - non occultare o distruggere documenti contabili propri o di terzi;
    - provvedere in maniera tempestiva all'effettuazione dei pagamenti fiscali;

- ai Destinatari è fatto espresso divieto di predisporre e inviare dichiarazioni fiscali alle Autorità competenti, contenenti dati falsi, artefatti, incompleti o comunque non rispondenti al vero, ovvero omettere dichiarazioni al fine di evadere le imposte sui redditi o sul valore aggiunto;
- Ansaldo Green Tech prevede, inoltre:
    - la puntuale verifica in ordine all'effettività e congruità delle prestazioni in relazione alle quali viene rilasciata fattura alla Società, con coinvolgimento delle Unità che hanno usufruito della prestazione per acquisire attestazione dell'effettivo svolgimento della stessa e della sua rispondenza all'oggetto del contratto;
    - la tracciabilità del processo relativo alla trasmissione delle dichiarazioni fiscali alle Autorità competenti, da effettuarsi nel rispetto delle norme di legge e regolamenti, in vista degli obiettivi di trasparenza e corretta informazione.

Con specifico riferimento alla classe di reati contro l'amministrazione della giustizia, oltre a quanto indicato nella parte speciale G, è fatto obbligo ai Destinatari di:

- non simulare operazioni ovvero predisporre documenti per trarre beneficio nel corso di un procedimento;
- non intralciare l'attività di coloro che si occupano dell'amministrazione della giustizia;
- non rivelare segreti/informazioni riservate inerenti ad un procedimento penale;
- non mutare artificiosamente lo stato dei luoghi o delle cose o delle persone in occasione di ispezioni o di esperimento giudiziale.

Con specifico riferimento alla classe di reati contro la pubblica amministrazione indicati nel paragrafo L.1, oltre a quanto indicato nella parte speciale A, è fatto obbligo ai Destinatari di:

- non richiedere ad un pubblico ufficiale o incaricato di pubblico servizio di compiere delle attività che possano comportare un vantaggio alla Società ovvero arrecare ad altri un danno ingiusto;
- non richiedere ad un pubblico ufficiale o incaricato di pubblico servizio di rivelare notizie di ufficio che devono rimanere riservate;
- non millantare credito presso un pubblico ufficiale ovvero presso un pubblico impiegato;
- non richiedere favori/somme di denaro o altra utilità per intercedere per conto di altri presso un pubblico ufficiale ovvero presso un pubblico impiegato;
- non violare i sigilli apposti per disposizione della legge o per ordine dell'autorità al fine di assicurare la conservazione o l'identità di una cosa.

Con specifico riferimento alla classe di reati contro l'economia pubblica, è fatto obbligo ai Destinatari di:

- non divulgare notizie false, esagerate o tendenziose;
- non compiere manovre speculative, ovvero occultare, accaparrare o fare incetta di materie prime.

Con specifico riferimento alla classe di reati contro l'incolumità pubblica, è fatto obbligo ai Destinatari di:

- svolgere tutte le attività di manutenzione ordinaria e straordinaria agli edifici necessari ad evitare qualsiasi tipo di crollo degli stessi;
- monitorare diligentemente l'attività svolta da ditte terza volte a garantire la manutenzione degli edifici;
- porre la massima attenzione nel non rimuovere, ovvero nel sostituire tempestivamente laddove dovuto, quanto necessario per evitare infortuni sul lavoro;
- provvedere ad apporre apparecchi e segnali, laddove necessari, atti ad impedire infortuni sul lavoro.

Con specifico riferimento alla classe di reati contro il patrimonio, è fatto obbligo ai Destinatari di:

- non sottrarre documentazione, dati o beni mobili/immobili a terzi;
- non richiedere prestazioni non contrattualizzate o che non si intende contrattualizzare;
- non promettere altre utilità a fornitori in caso di svolgimento di attività non prevista in apposito ordine/contratto;
- non distruggere, disperdere, deteriorare o rendere, in tutto o in parte, inservibili cose mobili o immobili altrui;
- non danneggiare appositamente beni assicurati al fine di ottenere un rimborso assicurativo non dovuto.

Con specifico riferimento alla classe di reati indicati come altri reati nel paragrafo L.1, è fatto obbligo ai Destinatari di seguire i principi di comportamento evidenziati nel paragrafo 6 della Parte Generale, nella Parte Speciale B e nella Parte Speciale H.

L.3.2 PROCEDURE DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Tutte le aree individuate come aree a rischio sono presidiate da procedure la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'O.d.V. affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si riportano di seguito le direttive, policy e procedure da seguire nelle aree di attività a rischio individuate nella presente Parte Speciale.

Direttive e policy di riferimento:

- AE GRUOP-DI-001 Code of Conduct for ICT Users;
- AE GROUP-DI-002 Export Compliance;
- AE GROUP-DI-003 Litigation Management;
- AE GROUP-DI-004 Appointment of Sales Promoters;
- AE GROUP-DI-005 Anti-Bribery and Corruption;
- AE GROUP-DI-006 Privacy;
- AE GROUP-DI-007 Managing Intellectual Property Assets;
- AE GROUP-DI-008 Information Security;

- AE GROUP-DI-009 Antitrust Directive;
- AE GROUP-DI-010 Delegation of Authority;
- AE GROUP-DI-012 Whistleblowing
- AE GROUP-PL-003 AE Group Information & Cyber Security Policy;
- AE GROUP-PL-005 Anti-Bribery and Corruption policy.

Procedure di riferimento:

- AE-PR-001 Ansaldo Energia Group Management System Documents;
- AE-PR-016 Information Technology Management Process;
- AE-PR-017 Information Technology Management Process-IT Demand Management;
- AE-PR-018 Information Technology Management Process-IT Service Execution;
- AE-PR-021 Accounts Receivable Process;
- AE-PR-022 Accounts Payable Process;
- AE-PR-023 Fixed Assets Process;
- AE-PR-024 General Ledger Process;
- AE-PR-025 Tax Management Process;
- AE-PR-026 Consolidation Process;
- AE-PR-027 Treasury and Trade Finance Process;
- AE-PR-031 Management of powers attorney;
- AE-PR-033 Information & Cyber Security Process - Security Incident Management;
- AE-PR-034 External and Internal Communication;
- AE-PR-035 Management of hospitality and entertainment expenses, corporate gifts, sponsorships and donations;
- AE-PR-037 Ansaldo Energia Group Travel Management;
- AE-PR-043 Professional Services and Consulting Assignments required without RdA;
- AE-PR-044 Supply Chain management;
- AE-PR-046 Intercompany Transfer Pricing Policy;
- AE-PR-047 Management of Inside Information;
- AE-PR-048 Information Classification;
- AE-PR-050 Intellectual Property Process;
- AE-PR-051 Intellectual Property Process – IP Constitution;
- AE-PR-057 IT Access Management;
- AE-PR-058 IT Security Operating Handbook;
- AE-PR-064 Project Claims Management Process;
- AE-PR-069 Intellectual Property Transfer process – Manage Non-Disclosure Agreements;
- AE-PR-070 Intellectual Property Transfer process – Manage Collaborative Research;

- AE-PR-071 Vendor Rating Process;
- AE-PR-072 Vendor Qualification Process;
- AE-PR-075 Indipendent Auditors management;
- AE-PR-080 Recruitment Process;
- AE-PR-081 Privacy;
- AE-PR-082 Due Diligence;
- AE-PR-101 Compliance with EHS legislative regulations and other requirements;
- AE-PR-102 EHS Requisites for Procurement;
- AE-PR-103 Health and Safety Risk Assessment;
- AE-PR-104 Environmental aspects identification and management;
- AE-PR-105 EHS Training;
- AE-PR-106 EHS Communication and consultation;
- AE-PR-107 EHS Surveillance and Performance Measurement;
- AE-PR-108 EHS Non Conformity and corrective actions;
- AE-PR-201 Waste Management;
- AE-PR-202 Air Emission Control;
- AE-PR-205 Soil and groundwater protection and management of possible spillage;
- AE-PR-206 Hazardous Materials Management;
- AE-PR-208 Industrial Hygiene;
- AE-PR-209 Personal Protective Equipment;
- AE-PR-210 EHS Incident and near miss management;
- AE-PR-211 EHS Project Plan (SITES);
- AE-PR-212 EHS System implementation on sites;
- AE-PR-213 Contractor and Outsourcer Performance Inspection;
- AE-PR-214 Emergency preparedness and management;
- AE-PR-215 Machinery equipment and tool safety;
- AE-PR-218 Working at height;
- AE-PR-219 Lifting Operations and lifting accessories;
- AE-PR-220 Electrical safety;
- AE-PR-222 Sicurezza nelle aree a rischio esplosione;
- AE-PR-223 Hot works;
- AE-PR-225 Safety in professional travelling;
- AE-PR-226 Medical surveillance;
- AE-PR-227 Ergonomics;
- AE-PR-228 Traffic Management in a Site;
- AE-PR-229 Housekeeping;

- AE-IN-001 Business travel management;
- AE-IN-004 Purchase Request approval flow e rules;
- AE-IN-006 Passive Payments – Operational Checks Against Supplier Data Cyber Frauds;
- AE-IN-016 Guidelines for the management of company phone;
- AGT-PR-001 Sales process;
- AGT-PR-002 Supply Management;
- AGT-PR-005 Project Management;
- AGT-PR-006 Phase Review Management;
- AGT-PR-007 Product Development Design Review process;
- AGT-ENV-001 Servizio di raccolta e smaltimento dei rifiuti speciali di Ansaldo Green tech S.p.A. stabilimento di C.so Perrone 118.

PARTE SPECIALE "M"

Reati tributari

M.1 LA TIPOLOGIA DEI REATI TRIBUTARI

M.1.1 PREMESSA

I reati tributari sono stati introdotti dalla Legge 19 dicembre 2019 n. 157 *"Conversione in legge, con modificazioni, del decreto-legge 26 ottobre 2019, n. 124, recante disposizioni urgenti in materia fiscale e per esigenze indifferibili"*.

In particolare, il richiamato D.L. 124/2019, con l'art. 39, è intervenuto in materia penale-tributaria modificando molte delle fattispecie penali previste dal D.Lgs. 74 del 2000 ed inserendo, nel novero dei reati presupposto della responsabilità degli enti, anche alcuni reati fiscali, aggiungendo al D.Lgs. 231/2001 l'art. *25-quinquiesdecies* (reati tributari).

Quest'ultimo è stato successivamente modificato dal D.lgs. 75/2020 che è andato ad estendere i reati tributari applicabili ai sensi del D.lgs. 231/01.

M.1.2 DICHIARAZIONE FRAUDOLENTA MEDIANTE USO DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 2 CO. 1 E 2-*BIS* 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."

L'art. 2 individua un reato commissivo, che si consuma nel momento della presentazione o della trasmissione in via telematica della dichiarazione nella quale sono indicati gli elementi passivi fittizi. L'interesse protetto dalla fattispecie è quello dell'Erario alla percezione dei tributi dovuti, prescindendo dalla realizzazione dell'evasione stessa, di qui l'illiceità penale della dichiarazione fraudolenta, avendo il legislatore inteso rafforzare in via di anticipazione la tutela del bene giuridico protetto. Il profitto del reato si identifica, dove non necessariamente l'operazione posta in essere realizza un incremento patrimoniale del reo, in un risparmio di imposta e dunque di spesa.

M.1.3 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."

La fattispecie delineata dall'art. 3 è un reato proprio, potendo essere realizzato solo da coloro che sono obbligati alla presentazione della dichiarazione dei redditi. La condotta rilevante si articola nella presentazione di una dichiarazione mendace e nella esecuzione di una attività ingannatoria a sostegno del mendacio materializzato nella dichiarazione. Tale attività può consistere nel compimento di operazioni simulate oggettivamente o soggettivamente ovvero nel ricorso a documenti falsi o ancora nel ricorso a mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria.

M.1.4 DICHIARAZIONE INFEDELE (ART. 4 D.LGS. 74/2000)

"1. Fuori dei casi previsti dagli articoli 2 e 3, è punito con la reclusione da due anni a quattro anni e sei mesi chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:

a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a € 100.000,00;

b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a € 2.000.000,00.

1-bis. Ai fini dell'applicazione della disposizione del comma 1, non si tiene conto della non corretta classificazione, della valutazione di elementi attivi o passivi oggettivamente esistenti, rispetto ai quali i criteri concretamente applicati sono stati comunque indicati nel bilancio ovvero in altra documentazione rilevante ai fini fiscali, della violazione dei criteri di determinazione dell'esercizio di competenza, della non inerenza, della non deducibilità di elementi passivi reali.

1-ter. Fuori dei casi di cui al comma 1-bis, non danno luogo a fatti punibili le valutazioni che complessivamente considerate, differiscono in misura inferiore al 10 per cento da quelle corrette. Degli importi compresi in tale percentuale non si tiene conto nella verifica del superamento delle soglie di punibilità previste dal comma 1, lettere a) e b)."

Al fine di considerare applicabile tale reato ai sensi del D.lgs. 231/01 è necessario che la condotta sia realizzata congiuntamente:

- nell'ambito di sistemi fraudolenti di tipo transfrontaliero connessi al territorio di almeno un altro Stato membro dell'Unione europea;
- al fine di evadere l'imposta sul valore aggiunto;
- per un importo complessivo pari o superiore a euro 10 milioni.

M.1.5 OMESSA DICHIARAZIONE (ART. 5 D.LGS. 74/2000)

"1. È punito con la reclusione da due a cinque anni chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad € 50.000,00.

1-bis. È punito con la reclusione da due a cinque anni chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad € 50.000,00

2. Ai fini della disposizione prevista dai commi 1 e 1-bis non si considera omessa la dichiarazione presentata entro novanta giorni dalla scadenza del termine o non sottoscritta o non redatta su uno stampato conforme al modello prescritto."

Al fine di considerare applicabile tale reato ai sensi del D.lgs. 231/01 è necessario che la condotta sia realizzata congiuntamente:

- nell'ambito di sistemi fraudolenti di tipo transfrontaliero connessi al territorio di almeno un altro Stato membro dell'Unione europea;
- al fine di evadere l'imposta sul valore aggiunto;
- per un importo complessivo pari o superiore a euro 10 milioni.

M.1.6 EMISSIONE DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 8 CO. 1 E 2-*BIS* D.LGS. 74/2000)

"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."

L'emissione di fatture per operazioni inesistenti è reato istantaneo, che si consuma nel momento in cui l'emittente perde la disponibilità della fattura, non essendo richiesto che il documento pervenga al destinatario, né che quest'ultimo lo utilizzi ed infatti il significato dei termini "emissione" e "rilascio" si ricava direttamente dal DPR 633/1973, il cui art. 21 dispone che "la fattura si ha per emessa all'atto della consegna o spedizione all'altra parte" dell'operazione commerciale.

M.1.7 OCCULTAMENTO O DISTRUZIONE DI DOCUMENTI CONTABILI (ART. 10 D.LGS. 74/2000)

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

La condotta del reato previsto dall'art. 10 può consistere sia nella distruzione che nell'occultamento delle scritture contabili o dei documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari, con conseguenze diverse rispetto al momento consumativo, giacché la distruzione realizza un'ipotesi di reato istantaneo, che si consuma con la soppressione della documentazione, mentre l'occultamento - consistente nella temporanea o definitiva indisponibilità della documentazione da parte degli organi verificatori - costituisce un reato permanente, che si protrae sino al momento dell'accertamento fiscale, dal quale soltanto inizia a decorre il termine di prescrizione.

M.1.8 INDEBITA COMPENSAZIONE (ART. 10-QUATER D.LGS. 74/2000)

1. È punito con la reclusione da sei mesi a due anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a € 50.000,00.

2. È punito con la reclusione da un anno e sei mesi a sei anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai € 50.000,00."

Al fine di considerare applicabile tale reato ai sensi del D.lgs. 231/01 è necessario che la condotta sia realizzata congiuntamente:

- nell'ambito di sistemi fraudolenti di tipo transfrontaliero connessi al territorio di almeno un altro Stato membro dell'Unione europea;
- al fine di evadere l'imposta sul valore aggiunto;
- per un importo complessivo pari o superiore a euro 10 milioni.

M.1.9 SOTTRAZIONE FRAUDOLENTA AL PAGAMENTO DI IMPOSTE (ART. 11 D.LGS. 74/2000)

"1. È 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. È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per se' 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."

La fattispecie prevista dall'art. 11 costituisce reato di pericolo, integrato dal compimento di atti simulati o fraudolenti volti a occultare i propri o altrui beni, idonei - secondo un giudizio "ex ante" che valuti la sufficienza della consistenza patrimoniale del contribuente rispetto alla pretesa dell'Erario - a pregiudicare l'attività recuperatoria dell'amministrazione finanziaria, a prescindere dalla sussistenza di un'esecuzione esattoriale in atto. La fraudolenza o la simulazione richieste dall'art. 11 possono essere realizzate anche mediante il trasferimento di soldi all'estero.

M.2 AREE A RISCHIO

Le aree di attività considerate a rischio in relazione ai reati tributari sono ritenute le seguenti:

1. Approvvigionamenti ed appalti.
2. Gestione delle commesse.
3. Tenuta della contabilità, redazione del bilancio e gestione della fiscalità.
4. Gestione dei contratti di consulenza.
5. Gestione dei rapporti con parti correlate.

Per il dettaglio delle attività a potenziale rischio, si rinvia a quanto indicato nei paragrafi A.3.2, A.3.6, A.3.12, A.3.13 e A.3.20.

M.3 PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE A RISCHIO

M.3.1 PRINCIPI DI COMPORTAMENTO DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

I Destinatari devono adottare regole di condotta conformi a quanto prescritto nella presente Parte Speciale ed in quelle che la precedono per quanto qui applicabili, nonché a quanto previsto dal Codice Etico e dalle procedure aziendali al fine di impedire il verificarsi dei reati trattati.

Ai Destinatari è fatto espresso obbligo di:

- osservare una condotta improntata a principi di integrità, correttezza e trasparenza nelle attività che determinano impatti di natura fiscale, nel rispetto delle normative vigenti;
- improntare i rapporti con l'Amministrazione Finanziaria a criteri di integrità, correttezza, trasparenza e collaborazione, evitando comportamenti che possano in qualsiasi modo considerarsi di ostacolo alle attività che l'Amministrazione Finanziaria è chiamate a svolgere. In tale prospettiva, gli Esponenti aziendali devono:
  - inviare le dichiarazioni previste dalla legge in modo tempestivo, completo ed accurato;
  - indicare nelle predette dichiarazioni dati rispondenti al vero, completi e corretti;
  - evitare ogni comportamento che possa ostacolare l'accertamento dell'Amministrazione Finanziaria ovvero indurre la stessa in errore, ovvero comportamenti volti a occultare o distruggere documenti contabili la cui conservazione è obbligatoria, ossia atti fraudolenti sui propri e altrui beni al fine di non pagare o pagare meno imposte;
- effettuare una puntale verifica in ordine all'effettività e congruità delle prestazioni in relazioni alle quali viene rilasciata fattura alla Società, con coinvolgimento delle Unità che hanno usufruito della prestazione al fine di acquisire attestazione dell'effettivo svolgimento della stessa e della sua rispondenza all'oggetto del contratto;
- effettuare una puntuale verifica in ordine all'effettività e congruità delle prestazioni in relazione alle quali viene emessa fattura da parte della Società, con

coinvolgimento delle Unità che attestano l'effettivo avanzamento/svolgimento delle attività inerenti la relativa commessa;

- porre particolare attenzione alle compensazioni, al fine di evitare che ne possano essere realizzate di indebite;
- monitorare il corretto assolvimento dei compiti trasferiti ad eventuali Studi esterni/Capogruppo;
- garantire la segregazione nel processo di determinazione e versamento delle imposte con riferimento alle fasi di:
  a. determinazione delle imposte dirette e indirette rispetto alle evidenze contabili e alla normativa fiscale;
  b. verifica dei Modelli F24 rispetto alle imposte determinate e/o delle richieste di pagamento;
  c. autorizzazione dei Modelli F24 e/o delle richieste di pagamento;
  d. esecuzione dei pagamenti/versamenti delle imposte;
- garantire la segregazione nel processo di inoltro delle dichiarazioni/comunicazioni fiscali periodiche con riferimento alle fasi di:
  a. verifica delle dichiarazioni/comunicazioni fiscali rispetto alle fonti dei dati ed ai requisiti di legge;
  b. sottoscrizione delle dichiarazioni/comunicazioni fiscali;
  c. inoltro telematico all'Amministrazione Finanziaria (diretto o tramite intermediario);
- effettuare un monitoraggio costante dell'evoluzione del quadro normativo di riferimento;
- verificare la completezza e correttezza dei dati contabili e gestionali necessari al calcolo delle imposte dirette e indirette;
- verificare accuratamente il processo di determinazione delle imposte dirette e indirette rispetto alle evidenze e alla normativa contabile e fiscale;
- garantire la formale approvazione, nel rispetto delle deleghe e delle procure in essere, dei modelli dichiarativi e di versamento delle imposte dirette e indirette;
- garantire un'adeguata profilazione delle utenze all'interno dei sistemi informativi aziendali dedicati alla rilevazione dei fatti contabili connessi alle imposte dirette e indirette;
- disciplinare la registrazione e conservazione dei dati relativi alle transazioni, garantendo la tracciabilità delle stesse di modo tale che sia sempre possibile ripercorrere le movimentazioni dalla loro origine con il supporto di tutta la documentazione necessaria;
- archiviare, nel rispetto dei termini di legge:
  a. le evidenze contabili e tutta la documentazione a supporto della determinazione delle imposte dirette e indirette;
  b. le evidenze degli avvenuti pagamenti/ versamenti;
  c. le dichiarazioni/comunicazioni fiscali periodiche inviate all'Amministrazione Finanziaria.

M.3.2 PROCEDURE DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Tutte le aree individuate come aree a rischio sono presidiate da procedure la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'OdV affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si riportano di seguito le direttive e le procedure da seguire nelle aree di attività a rischio individuate nella presente Parte Speciale.

Direttive di riferimento:

- AE GROUP-DI-002 Export Compliance;
- AE GROUP-DI-007 Managing Intellectual Property Assets;
- AE GROUP-DI-009 Antitrust Directive.
- AE GROUP-DI-012 Whistleblowing.

Procedure di riferimento:

- AE-PR-021 Accounts Receivable Process;
- AE-PR-022 Accounts Payable Process;
- AE-PR-023 Fixed Assets Process;
- AE-PR-024 General Ledger Process;
- AE-PR-025 Tax Management Process;
- AE-PR-026 Consolidation Process;
- AE-PR-027 Treasury and Trade Finance Process;
- AE-PR-043 Professional Services and Consulting Assignments required without RdA;
- AE-PR-044 Supply Chain management;
- AE-PR-046 Intercompany Transfer Pricing Policy;
- AE-PR-050 Intellectual Property Process;
- AE-PR-051 Intellectual Property Process – IP Constitution;
- AE-PR-064 Project Claims Management Process
- AE-PR-069 Intellectual Property Transfer process – Manage Non-Disclosure Agreements;
- AE-PR-070 Intellectual Property Transfer process – Manage Collaborative Research;
- AE-PR-071 Vendor Rating Process;
- AE-PR-072 Vendor Qualification Process;
- AE-PR-082 Due Diligence;
- AE-IN-004 Purchase Request approval flow e rules;
- AE-IN-006 Passive Payments – Operational Checks Against Supplier Data Cyber Frauds;
- AGT-PR-002 Supply Management;
- AGT-PR-005 Project Management;

- AGT-PR-006 Phase Review Management.

PARTE SPECIALE "N"

Reati di contrabbando

N.1 LA TIPOLOGIA DEI REATI DI CONTRABBANDO

I reati di contrabbando sono stati inseriti nel novero dei reati presupposto per l'applicazione delle sanzioni previste dal D.Lgs. 231/2001 con il D.Lgs. 14 luglio 2020 n. 75 il quale, all'art. 5 comma 1 lett d), aggiunge l'art. 25-*sexiesdecies* che testualmente recita:

"*1. In relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica 23 gennaio 1973 n. 43 si applica all'ente la sanzione pecuniaria fino a duecento quote.*

2. Quando i diritti di confine dovuti superano i centomila euro si applica all'ente la sanzione pecuniaria fino a quattrocento quote.

3. Nei casi previsti dai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'art. 9, comma 2 lettere c), d) ed e)."

La descrizione dei reati di cui all'art. 25-*sexiesdecies* va quindi ricercata nel D.P.R. 23 gennaio 1973 n. 43 denominato "*Testo Unico delle disposizioni legislative in materia doganale*", il quale al Capo I (contrabbando) del Titolo VII (violazioni doganali) enumera nel dettaglio le varie ipotesi di contrabbando descritte negli articoli da 282 a 292.

Trascurando le ipotesi di contrabbando di tabacchi lavorati in quanto fatti che non possono essere commesse in ambito Ansaldo Green Tech nell'interesse della Società, le ipotesi di astratto interesse sono:

- art. 282 - contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali;
- art. 283 - contrabbando nel movimento delle merci nei laghi di confine;
- art. 284 - contrabbando nel movimento marittimo delle merci;
- art. 285 - contrabbando nel movimento delle merci per via aerea;
- art. 286 - contrabbando nelle zone extra-doganali;
- art. 287 - contrabbando per indebito uso di merci importate con agevolazioni doganali;
- art. 288 - contrabbando nei depositi doganali;
- art. 289 - contrabbando nel cabotaggio e nella circolazione;
- art. 290 - contrabbando nell'esportazione di merci ammesse a restituzione di diritti;
- art. 291 - contrabbando nell'importazione od esportazione temporanea.

A tutte le ipotesi si affianca l'art. 292 che sotto la rubrica "*Altri casi di contrabbando*" sanziona "*chiunque, fuori dei casi preveduti dagli articoli precedenti, sottrae merci al pagamento dei diritti di confine dovuti*", norma che possiamo considerare di chiusura e che ci consente, per una miglior comprensione, di ricondurre tutte le fattispecie, al di là della analitica descrizione del legislatore, all'ipotesi di una sottrazione delle merci al pagamento dei diritti di confine, realizzata o presunta o anche tentata, perché in materia di contrabbando il tentativo (art. 294) è equiparato al reato consumato.

Vale invece la pena di rimarcare che, pur essendo prevista per tutte le ipotesi di contrabbando una sanzione amministrativa, che, come tale, sarebbe esclusa dall'applicazione delle sanzioni del D.Lgs. 231/2001, tuttavia per effetto delle aggravanti previste dall'art. 295 tutte le ipotesi rientrano fra i reati, e quindi incorrono nel D.Lgs. 231/2001:

- Lett c) quando il fatto sia connesso con altro delitto contro la fede pubblica o contro la pubblica amministrazione (il contrabbando commesso con l'uso di atti falsi o contraffatti rappresenta un'ipotesi facilmente ricorrente nel panorama criminale);
- Lett d) quando il colpevole sia un associato per commettere delitti di contrabbando e il delitto commesso sia fra quelli per cui l'associazione è stata costituita;
- Lett d bis) quando l'ammontare dei diritti di confine dovuti è superiore a cinquantamila (o ipotesi ulteriormente aggravata a centomila) euro.

Sono previste attenuanti che in questa sede non meritano di essere trattate.

N.2 AREE A RISCHIO

Le aree di attività considerate a rischio in relazione ai reati di contrabbando sono ritenute le seguenti:

1. Approvvigionamenti ed appalti.
2. Gestione delle commesse.
3. Tenuta della contabilità, redazione del bilancio e gestione della fiscalità.

Per il dettaglio delle attività a potenziale rischio, si rinvia a quanto indicato nei paragrafi A.3.2, A.3.6. e A.3.12.

N.3 PRINCIPI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE A RISCHIO

N.3.1 PRINCIPI DI COMPORTAMENTO DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

I Destinatari devono adottare regole di condotta conformi a quanto prescritto nella presente Parte Speciale ed in quelle che la precedono per quanto qui applicabili, nonché a quanto previsto dal Codice Etico e dalle procedure aziendali al fine di impedire il verificarsi dei reati trattati.

Ai Destinatari è fatto espresso obbligo di:

- osservare una condotta improntata a principi di integrità, correttezza e trasparenza nelle attività di importazione ed esportazione di beni, nel rispetto delle normative doganali italiane ed estere vigenti;
- improntare i rapporti con l'Agenzia Dogane e Monopoli e con gli uffici doganali a criteri di integrità, correttezza, trasparenza e collaborazione, evitando comportamenti che possano in qualsiasi modo considerarsi di ostacolo alle attività che Agenzia/uffici doganali sono chiamati a svolgere. In tale prospettiva, gli Esponenti aziendali devono:
  - predisporre/inviare/consegnare i documenti previsti dalla normativa vigente in modo tempestivo, completo ed accurato;
  - indicare nei predetti documenti dati rispondenti al vero, completi e corretti;
  - evitare ogni comportamento che possa ostacolare l'accertamento del soggetto pubblico ovvero indurre lo stessa in errore, ovvero comportamenti volti a occultare trasferimenti di beni al di fuori del territorio dell'Unione Europea, ossia atti fraudolenti sui propri e altrui beni al fine di non pagare/non far pagare o pagare/far pagare meno dazi;

- monitorare il corretto assolvimento dei compiti trasferiti all'operatore doganale della Società, ove costituito da un soggetto terzo;
- garantire la segregazione nel processo di importazione di beni, con riferimento alle fasi di:
  a. predisposizione del Documento Amministrativo Unico (DAU);
  b. sottoscrizione del DAU a cura di chi ne ha i poteri;
  c. consegna del DAU all'ufficio doganale e ricezione della bolletta doganale;
  d. pagamento dei dazi doganali;
  e. registrazione della bolletta doganale;
- garantire la segregazione nel processo di esportazione di beni, con riferimento alle fasi di:
  a. predisposizione della dichiarazione di esportazione;
  b. sottoscrizione della dichiarazione di esportazione da parte di chi ne ha i poteri;
  c. inoltro della dichiarazione di esportazione all'ufficio doganale e ricezione del Documento di Accompagnamento Esportazione (DAE);
  d. consegna del DAE all'ufficio doganale di uscita;
- effettuare un monitoraggio costante dell'evoluzione del quadro normativo di riferimento;
- garantire un'adeguata profilazione delle utenze con riferimento a coloro che accedono ai sistemi informativi pubblici dedicati alle attività doganali;
- disciplinare la registrazione e conservazione dei dati relativi alle transazioni di carattere doganale, garantendo la tracciabilità delle stesse di modo tale che sia sempre possibile ripercorrere le movimentazioni dalla loro origine con il supporto di tutta la documentazione necessaria;
- archiviare, nel rispetto dei termini di legge, tutta la documentazione inerente alle attività doganali.

N.3.2 PROCEDURE DA SEGUIRE NELLE AREE DI ATTIVITÀ A RISCHIO

Tutte le aree individuate come aree a rischio sono presidiate da procedure la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'OdV affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si riportano di seguito le direttive e le procedure da seguire nelle aree di attività a rischio individuate nella presente Parte Speciale.

Direttive di riferimento:

- AE GROUP-DI-002 Export Compliance;
- AE GROUP-DI-007 Managing Intellectual Property Assets;
- AE GROUP-DI-009 Antitrust Directive;
- AE GROUP-DI-012 Whistleblowing.

Procedure di riferimento:

- AE-PR-021 Accounts Receivable Process;
- AE-PR-022 Accounts Payable Process;
- AE-PR-023 Fixed Assets Process;
- AE-PR-024 General Ledger Process;
- AE-PR-025 Tax Management Process;
- AE-PR-026 Consolidation Process;
- AE-PR-027 Treasury and Trade Finance Process;
- AE-PR-043 Professional Services and Consulting Assignments required without RdA;
- AE-PR-044 Supply Chain management
- AE-PR-050 Intellectual Property Process;
- AE-PR-051 Intellectual Property Process – IP Constitution;
- AE-PR-064 Project Claims Management Process;
- AE-PR-069 Intellectual Property Transfer process – Manage Non-Disclosure Agreements;
- AE-PR-070 Intellectual Property Transfer process – Manage Collaborative Research;
- AE-PR-071 Vendor Rating Process;
- AE-PR-072 Vendor Qualification Process;
- AE-PR-082 Due Diligence;
- AE-IN-004 Purchase Request approval flow e rules;
- AE-IN-006 Passive Payments – Operational Checks Against Supplier Data Cyber Frauds;
- AGT-PR-002 Supply Management;
- AGT-PR-005 Project Management;
- AGT-PR-006 Phase Review Management.