HITACHI
Inspire the Next

Modello di Organizzazione, Gestione e Controllo ai sensi del Decreto Legislativo 8 giugno 2001, n. 231 di Hitachi Vantara Italia S.r.l.

Approvato con delibera del Consiglio di Amministrazione di Hitachi Vantara Italia S.r.l. nella seduta del 30/05/2024.

INDICE

PARTE GENERALE 4
1. IL DECRETO LEGISLATIVO N. 231/2001 E LA NORMATIVA RILEVANTE 5
1.1. IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO A CARICO DELLE PERSONE GIURIDICHE ...5
1.2. SANZIONI 6
1.3. DELITTI TENTATI E DELITTI COMMESSI ALL'ESTERO 7
1.4. PROCEDIMENTO DI ACCERTAMENTO DELL'ILLECITO E SINDACATO DI IDONEITÀ DEL GIUDICE 7
1.5. AZIONI ESIMENTI DALLA RESPONSABILITÀ AMMINISTRATIVA 8
2. LINEE GUIDA DI CONFINDUSTRIA 9
3. ADOZIONE DEL MODELLO DA PARTE DI HITACHI VANTARA ITALIA S.R.L. 9
3.1. OBIETTIVI E MISSION AZIENDALE 9
3.2. MODELLO DI GOVERNANCE 10
3.3. ASSETTO ORGANIZZATIVO 10
3.4. MOTIVAZIONI DI HITACHI VANTARA ITALIA NELL'ADOZIONE DEL MODELLO 10
3.4.1. FINALITÀ DEL MODELLO 11
3.4.2. IL PROCESSO DI PREDISPOSIZIONE ED AGGIORNAMENTO DEL MODELLO 11
3.5. STRUTTURA DEL DOCUMENTO 13
3.6. ELEMENTI DEL MODELLO 13
3.7. MODIFICHE ED INTEGRAZIONI DEL MODELLO 14
4. ORGANISMO DI VIGILANZA 15
4.1. IDENTIFICAZIONE DELL'ORGANISMO DI VIGILANZA 15
4.2. FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA 17
4.3. INFORMATIVA DELL'ORGANISMO DI VIGILANZA NEI CONFRONTI DEGLI ORGANI SOCIETARI 18
4.4. FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA 19
4.4.1. SEGNALAZIONI ALL'ODV 19
4.4.2. RACCOLTA, CONSERVAZIONE E ACCESSO ALL'ARCHIVIO DELL'ODV 20
5. FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO NEL CONTESTO AZIENDALE E ALL'ESTERNO 20
5.1. FORMAZIONE DEL PERSONALE 20
5.2. INFORMATIVA AL PERSONALE 21
5.3. INFORMATIVA A COLLABORATORI ESTERNI E PARTNER 21
6. SISTEMA DISCIPLINARE E MISURE IN CASO DI MANCATA OSSERVANZA DELLE PRESCRIZIONI DEL MODELLO 21
6.1. PRINCIPI GENERALI 21
6.2. SANZIONI PER I LAVORATORI DIPENDENTI 22
6.2.1. IMPIEGATI, OPERAI E QUADRI 22
6.2.2. DIRIGENTI 22
6.3. MISURE NEI CONFRONTI DEGLI AMMINISTRATORI E DEL SINDACO UNICO 23
6.4. MISURE NEI CONFRONTI DI COLLABORATORI, CONSULENTI, PARTNER, CONTROPARTI COMMERCIALI ED ALTRI SOGGETTI ESTERNI 23
6.5. PROCEDIMENTO DI APPLICAZIONE DELLE SANZIONI 23

6.5.1. IL PROCEDIMENTO DISCIPLINARE NEI CONFRONTI DEI DIPENDENTI NON DIRIGENTI 24
6.5.2. IL PROCEDIMENTO DISCIPLINARE NEI CONFRONTI DEI DIRIGENTI 24
6.5.3. IL PROCEDIMENTO DISCIPLINARE NEI CONFRONTI DEGLI AMMINISTRATORI E DEL SINDACO UNICO 25
6.5.4. IL PROCEDIMENTO NEI CONFRONTI DEI TERZI DESTINATARI DEL MODELLO 26
7. PRINCIPI GENERALI DI COMPORTAMENTO 26
PARTE SPECIALE 28
1. FUNZIONE DELLA PARTE SPECIALE 29
2. OBBLIGHI DI INFORMATIVA ALL'ODV 30
2.1. OBBLIGHI DI INFORMATIVA AD HOC 30
2.2. OBBLIGHI DI INFORMATIVA PERIODICA 30
3. AREE A RISCHIO REATO DIRETTO E STRUMENTALE 32
3.1. ATTIVITA' COMMERCIALE E DI VENDITA 33
3.2. INSTALLAZIONE DEI BENI/EROGAZIONE DEI SERVIZI 37
3.3. ACQUISIZIONE, PROGRESSIONE E GESTIONE DEL PERSONALE 40
3.4. APPROVVIGIONAMENTO DI BENI E SERVIZI E CONSULENZE 44
3.5. AFFARI SOCIETARI 47
3.6. AMMINISTRAZIONE, FINANZA E CONTROLLO 49
3.7. RISORSE FINANZIARIE 53
3.8. SISTEMI INFORMATIVI 56
3.9. SALUTE E SICUREZZA SUL LAVORO 62
3.10. TEMATICHE AMBIENTALI 67
3.11. GESTIONE PRECONTENZIOSO E CONTENZIOSO 69
3.12. RAPPORTI CON ISTITUZIONI ED ENTI PUBBLICI 71
3.13. DONAZIONI, LIBERALITÀ E OMAGGI 75

PARTE GENERALE

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

1.1. IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA 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 amministrativa, 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 unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche, di fatto, la gestione ed il controllo degli Enti medesimi;
- persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

La responsabilità amministrativa della persona giuridica si aggiunge a quella (penale) della persona fisica che ha commesso il reato e sono entrambe oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale.

Prima dell'entrata in vigore del Decreto, il principio di personalità della responsabilità penale posto dall'art. 27 della Costituzione precludeva la possibilità di giudicare ed eventualmente condannare in sede penale gli Enti in relazione a reati commessi nel loro interesse, potendo sussistere soltanto una responsabilità solidale in sede civile per il danno eventualmente cagionato dal proprio dipendente ovvero per l'obbligazione civile derivante dalla condanna al pagamento della multa o dell'ammenda del dipendente in caso di sua insolvibilità (artt. 196 e 197 c.p.).

La responsabilità amministrativa degli enti può conseguire dalla commissione delle seguenti tipologie di reati:

- reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del Decreto);
- delitti informatici e trattamento illecito di dati (art. 24-*bis* del Decreto);
- delitti di criminalità organizzata (art. 24-*ter* del Decreto);
- reati in tema di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis* del Decreto);
- delitti contro l'industria e il commercio (art. 25-*bis.1* del Decreto);
- reati societari (art. 25-*ter* del Decreto);
- delitti con finalità di terrorismo o di eversione dell'ordine democratico (25-*quater* del Decreto);
- delitti di pratiche di mutilazione degli organi genitali femminili (art. 25-*quater*.1 del Decreto);
- delitti contro la personalità individuale (art. 25-*quinquies* del Decreto);
- reati di abusi di mercato (art. 25-*sexies* del Decreto);
- reati di omicidio colposo o lesioni gravi o gravissime, commesse con violazione delle norme sulla tutela della salute e sicurezza (25-*septies* del Decreto);
- reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-*octies* del Decreto);
- delitti in materia di strumenti di pagamento diversi dai contanti (art. 25 *octies*.1 del Decreto);
- delitti in materia di violazione del diritto d'autore (art. 25-*novies* del Decreto);
- reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25–*decies* del Decreto);
- reati ambientali (art. 25–*undecies* del Decreto);
- reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25–*duodecies* del Decreto);
- reati di razzismo e xenofobia (art. 25-*terdecies* del Decreto);

- reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo apparecchi vietati (art. 25-*quaterdecies* del Decreto);
- reati tributari (art. 25-*quinquiesdecies* del Decreto);
- reati di contrabbando (art. 25-*sexiesdecies* del Decreto);
- delitti contro il patrimonio culturale (art. 25-*septiesdecies* del Decreto);
- riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-*duodevicies* del Decreto);
- reati transnazionali, introdotti dalla Legge 16 marzo 2006 n. 146, "*Legge di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale*"[1].Altre fattispecie di reato potranno in futuro essere inserite dal legislatore nel Decreto Legislativo 231/01, con conseguente possibile necessità di aggiornamento del presente Modello.

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 (fatti salvi i casi di interdizione definitiva richiamati dall'articolo 16 dal 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 revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- l'esclusione da agevolazioni, finanziamenti, contributi e 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.

[1] I reati presupposto che rilevano come reati transnazionali sono i seguenti: associazione per delinquere (articolo 416 c.p.); associazioni di tipo mafioso anche straniere (articolo 416-bis c.p.); induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (articolo 377-bis c.p.); associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (articolo 291-quater D.P.R. 23 gennaio 1973, n. 43); associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (articolo 74 D.P.R. 9 ottobre 1990, n. 309); traffico di migranti (articolo 12, commi 3, 3-bis, 3-ter e 5 D.Lgs. n. 25 luglio 1998, n. 286); reato di favoreggiamento personale (articolo 378 c.p.).

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 del Decreto). 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 amministrativa dell'Ente (art. 23 del Decreto).

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 tra 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 delle quote è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente, allo scopo di assicurare l'efficacia della sanzione (art. 11 del Decreto).

Oltre alle predette sanzioni, il Decreto prevede che venga sempre disposta (salvo per la parte che può essere restituita al danneggiato) la confisca del prezzo o del profitto del reato, che può avere ad oggetto anche beni o altre utilità dei valori equivalenti, mentre la pubblicazione della sentenza di condanna può essere disposta dal giudice in presenza di una sanzione interdittiva.

1.3. DELITTI TENTATI E DELITTI COMMESSI ALL'ESTERO

L'Ente risponde anche degli illeciti dipendenti da delitti tentati e da reati commessi all'estero.

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. L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra Ente e soggetti che assumono di agire in suo nome e per suo conto. Si tratta di un'ipotesi particolare di c.d. "recesso attivo", previsto dall'art. 56, co. 4, c.p..

In base al disposto dell'art. 4 del Decreto, l'Ente che abbia sede in Italia può essere chiamato a rispondere, in relazione a reati - contemplati dallo stesso Decreto - 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.

1.4. 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.

Altra regola prevista dal Decreto, ispirata a ragioni di effettività, omogeneità ed economia processuale, è quella dell'obbligatoria riunione dei procedimenti: il processo nei confronti dell'Ente dovrà rimanere riunito, per quanto possibile, al processo penale instaurato nei confronti della persona fisica autore del reato presupposto della responsabilità dell'Ente.

L'accertamento della responsabilità dell'Ente, attribuito al giudice penale, avviene mediante:

- la verifica della sussistenza del reato presupposto per la responsabilità dell'Ente;
- 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.

1.5. AZIONI ESIMENTI DALLA RESPONSABILITÀ AMMINISTRATIVA

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

In particolare, 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 (di seguito "Modello");

b) il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di proporne l'aggiornamento sia stato affidato ad un Organismo dell'Ente (di seguito "OdV"), 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'OdV.

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 idoneo a prevenire reati della specie di quello verificatosi.

Il Decreto prevede, inoltre, che il Modello, debba 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 a impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'OdV;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Lo stesso Decreto prevede che i Modelli possano essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria.

2. LINEE GUIDA DI CONFINDUSTRIA

La predisposizione del presente Modello è ispirata alle Linee Guida emanate da Confindustria per la prima volta il 7 marzo 2002 e successivamente nel tempo aggiornate.

Il percorso da queste indicato per l'elaborazione del Modello può essere schematizzato secondo i seguenti punti fondamentali:

- individuazione delle aree a rischio, volta a verificare in quali aree/settori aziendali sia possibile la realizzazione dei reati;
- predisposizione di un sistema di controllo in grado di ridurre i rischi attraverso l'adozione di appositi protocolli. A supporto di ciò concorre l'insieme coordinato di strutture organizzative, attività e regole operative applicate dal management e dal personale aziendale, volto a fornire una ragionevole sicurezza in merito al raggiungimento delle finalità rientranti in un buon sistema di controllo interno. Le componenti più rilevanti del sistema di controllo preventivo proposto da Confindustria sono:
  - codice etico;
  - sistema organizzativo;
  - procedure manuali ed informatiche;
  - poteri autorizzativi e di firma;
  - sistemi di controllo e gestione;
  - comunicazioni al personale e sua formazione.

Il sistema di controllo inoltre deve essere uniformato ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- separazione delle funzioni;
- documentazione dei controlli;
- introduzione di un adeguato sistema sanzionatorio per le violazioni delle norme e delle procedure previste dal Modello;
- individuazione di un OdV i cui principali requisiti siano:
  - autonomia e indipendenza;
  - professionalità;
  - continuità di azione.

Inoltre, le Linee Guida prevedono l'obbligo da parte delle funzioni aziendali, e segnatamente di quelle che svolgono attività individuate come "a rischio", di fornire informazioni all'OdV per segnalare anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili.

Resta inteso che la scelta di non seguire in alcuni punti specifici le Linee Guida non inficia la validità di un Modello. Questo, infatti, essendo redatto con riferimento alla peculiarità di una società particolare, può discostarsi dalle Linee Guida che per loro natura hanno carattere generale.

3. ADOZIONE DEL MODELLO DA PARTE DI HITACHI VANTARA ITALIA S.R.L.

3.1. OBIETTIVI E MISSION AZIENDALE

Hitachi Vantara Italia S.r.l. a s.u. (di seguito "Hitachi Vantara Italia" o "Società"), è interamente posseduta da Hitachi Vantara Nederland B.V. (di seguito "Capogruppo") e fa parte del Gruppo Hitachi Vantara, avente sede centrale a Santa Clara in California, sottogruppo di riferimento del gruppo Hitachi, per quanto riguarda la realizzazione di:

- soluzioni di infrastrutture IT;
- software di data storage management;
- servizi di consulenza per lo storage dati.

La Società, come emerge dalla visura camerale, ha come oggetto sociale *"l'acquisto, la vendita, sia all'ingrosso che al dettaglio, il marketing, in Italia ed all'Estero, anche per mezzo di trasmissione dati, sia in qualità di licenziante che/o mandatario che/o distributore, di computers e prodotti di tecnologia connessi ai computers, compresi software, così come ogni altro tipo di prodotti, materie prime, apparecchiature impianto, strumenti o servizi usati in connessione a ciò; la fornitura, in ogni modo, di servizi e di rete relativi a computers e prodotti di tecnologia riguardanti i computers, inclusi software"*..

3.2. MODELLO DI GOVERNANCE

La *corporate governance* della Società, basata sul modello tradizionale, è così articolata:

- *Assemblea dei Soci*, 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, a esclusione degli atti riservati – dalla Legge e dallo Statuto – all'Assemblea;
- *Sindaco Unico* (di seguito anche "Organo di Controllo"), cui spetta il compito di vigilare:
  - sull'osservanza della legge e dell'atto costitutivo nonché sul rispetto dei principi di corretta amministrazione;
  - sull'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* cui spetta l'attività di revisione legale dei conti.

3.3. ASSETTO ORGANIZZATIVO

Il sistema organizzativo della Società è definito dal Country Leader, tenendo conto delle disposizioni e delle global policies della Capogruppo e quindi anche del fatto che la struttura IT è comune a livello EMEA e che alcuni processi, o parti di processo, sono centralizzati per tutte le società facenti parti del Gruppo Hitachi Vantara (come ad esempio quelle relative al centro di servizi finanziari) di riferimento e che, anche in questa logica, alcune risorse di Hitachi Vantara Italia possono essere chiamate a operare presso altre società del Gruppo Hitachi Vantara di riferimento e viceversa.

Tale sistema è ispirato, nell'ambito di quanto sopra indicato, all'attuazione di una separazione di compiti, ruoli e responsabilità tra le Funzioni in modo tale che nessuna possa in autonomia seguire tutte le fasi di un processo. Il sistema è formalizzato e tenuto aggiornato in documenti che indicano la struttura nel suo complesso, con l'indicazione dei Referenti per ciascuna Funzione, i riporti gerarchici/funzionali ed i compiti e le responsabilità assegnati a ciascuna Funzione. In tale contesto la Società si è dotata di un sistema di norme conforme ai principi di buona gestione identificati dalla norma ISO9001:2015 e ISO 27001:2014.

La diffusione di tali documenti è assicurata attraverso l'invio per posta elettronica, nonché la pubblicazione sull'intranet aziendale.

3.4. MOTIVAZIONI DI HITACHI VANTARA ITALIA NELL'ADOZIONE DEL MODELLO

La Società, per assicurare che il comportamento di coloro che operano per suo conto o nel suo interesse sia sempre conforme ai principi di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, ha ritenuto opportuno procedere all'adozione di un 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.

Il Modello è stato quindi adottato nella convinzione che costituisca un valido strumento di sensibilizzazione nei confronti di coloro che operano nell'interesse o a vantaggio della Società.

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

- i componenti del Consiglio di Amministrazione (di seguito "CdA");
- l'Organo di Controllo;
- i dipendenti e i collaboratori che intrattengono con la Società rapporti contrattuali, a qualsiasi titolo, anche occasionali e/o soltanto temporanei.

Sono, altresì, tenuti al rispetto dei principi indicati nel D.Lgs. 231/01 e nel "Code of Ethics and Business Conduct" del Gruppo Hitachi Vantara coloro che intrattengono con la Società rapporti di qualsiasi natura (clienti, fornitori, partner).

3.4.1. FINALITÀ DEL MODELLO

Il Modello si propone come finalità quelle di:

- migliorare il sistema di corporate governance della Società;
- predisporre un sistema strutturato e organico di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività aziendale, con particolare riguardo a impedire eventuali comportamenti illegali;
- determinare, in coloro che operano in nome e per conto della Società 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 della Società;
- informare coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse della Società che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni fino alla risoluzione del rapporto contrattuale;
- ribadire che la Società non tollera comportamenti illeciti, non rilevando in alcun modo la finalità perseguita ovvero l'erroneo convincimento di agire nel suo interesse o a suo vantaggio, in quanto tali comportamenti sono comunque contrari ai principi etici cui la Società 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.

3.4.2. IL PROCESSO DI PREDISPOSIZIONE ED AGGIORNAMENTO DEL MODELLO

La Società, in considerazione delle esigenze poste dal Decreto, ha avviato un progetto interno finalizzato a garantire l'aggiornamento del presente Modello.

Conseguentemente, tale aggiornamento è stato preceduto da una serie di attività dirette alla costruzione di un sistema di prevenzione e gestione dei rischi, di seguito descritte:

1) *Mappatura delle attività a rischio*. Obiettivo di questa fase è stata l'analisi del contesto aziendale, per mappare le aree di attività della Società e, tra queste, individuare le attività in cui possono - in astratto - essere realizzati i reati previsti dal Decreto. L'identificazione delle attività aziendali e delle aree a rischio è stata attuata attraverso il previo esame della documentazione aziendale (organigramma, processi principali, procure, procedure di gruppo e aziendali, ecc.) e la successiva effettuazione di interviste con i principali Referenti.

2) *Analisi dei rischi potenziali*. Con riferimento alla mappatura delle attività, effettuata sulla base dello specifico contesto in cui opera la Società ed alla relativa rappresentazione dei processi/attività sensibili o a rischio, sono stati identificati i reati potenzialmente realizzabili nell'ambito dell'attività aziendale. Il risultato di tale attività è riepilogato nel documento "*Analisi dei Rischi 231*", in cui sono individuati, per ogni area a rischio rilevata, la descrizione dell'attività e le funzioni coinvolte nella gestione delle stesse nonché i reati e i rischi a cui la Società è esposta.

3) *As-is analysis*. Individuati i reati potenzialmente applicabili, si è proceduto ad analizzare il sistema di controlli preventivi esistente nelle aree di attività a rischio, al fine di esprimere il successivo livello di adeguatezza dello stesso per la prevenzione dei rischi di reato. In tale fase, si è, pertanto, provveduto alla rilevazione degli attuali presidi di controllo interno esistenti (policy di Gruppo, procedure e/o prassi adottate, verificabilità, documentabilità o "tracciabilità" delle operazioni e dei controlli, segregazione delle funzioni, ecc.) attraverso le informazioni fornite dalla Società e l'analisi della documentazione da essa fornita. Il risultato di tali attività è contenuto nel documento "*Analisi dei Rischi 231*".

4) *Individuazione di proposte di miglioramento del sistema di controllo interno*. Sulla base dei risultati ottenuti nella fase precedente e del confronto con un modello teorico di riferimento (coerente con il Decreto, con le Linee Guida di Confindustria e con le migliori pratiche nazionali ed internazionali), la Società ha valutato l'opportunità di effettuare attività di integrazione e/o miglioramento nel sistema dei controlli, indicandole nel documento "*Analisi dei Rischi 231*".

5) *Predisposizione del Modello*. In considerazione degli esiti delle fasi sopra descritte, la Società ha provveduto all'aggiornamento del Modello.

Sulla base del Risk Assessment effettuato, in ragione della specifica operatività della Società, sono state, pertanto, individuate le attività a rischio di commissione di reati previsti dal D.Lgs. 231/01, riportate nella Parte Speciale del presente Modello. Con riferimento alle aree a rischio, sono stati altresì presi in esame gli eventuali rapporti indiretti, ossia quelli che la Società intrattiene, o potrebbe intrattenere, tramite soggetti terzi.

Nel Risk Assessment sono state analizzate le seguenti componenti del sistema di controllo preventivo:

- *Principi etici formalizzati*. La Società ha provveduto a recepire il Codice Etico (Code of Ethics and Compliance) e il Codice di Condotta (Codes of Conduct) del Gruppo Hitachi Vantara (di seguito "Codice Etico e di Condotta"), che esprime i propri valori etici e che definisce, con specifico riferimento alle attività a rischio reato, dei presidi generali di riferimento.
- *Sistema organizzativo*. L'adeguatezza del sistema organizzativo è stata valutata sulla base dei seguenti criteri:
  - formalizzazione del sistema;
  - chiara definizione delle responsabilità attribuite e delle linee di dipendenza gerarchica;
  - esistenza della segregazione e contrapposizione di funzioni;
  - corrispondenza tra le attività effettivamente svolte e quanto previsto dalle missioni e responsabilità descritto dai documenti della Società.
- *Sistema autorizzativo*. L'analisi ha riguardato l'esistenza di poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali assegnate e/o concretamente svolte. L'accertamento è stato condotto sulla base dell'esame delle procure rilasciate e delle deleghe gestionali interne, alla luce dell'organigramma aziendale.
- *Procedure*. L'analisi ha riguardato l'esistenza di procedure formalizzate (anche a livello di Gruppo) per regolamentare le attività svolte dalle Funzioni nelle aree a rischio, tenendo conto non soltanto delle fasi negoziali, ma anche di quelle di istruzione e di formazione delle decisioni aziendali.
- *Sistema di controllo di gestione*. L'analisi ha riguardato il sistema di controllo di gestione vigente nella Società, i soggetti coinvolti nel processo e la capacità del sistema di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità generale e/o particolare.
- *Monitoraggio e gestione della documentazione*. L'analisi ha riguardato l'esistenza di un idoneo sistema di monitoraggio dei processi per la verifica dei risultati e di eventuali non conformità,

nonché l'esistenza di un idoneo sistema di gestione della documentazione tale da consentire la tracciabilità delle operazioni.

- *Sistema disciplinare*. Le analisi svolte sono state finalizzate alla verifica dell'esistenza di un sistema disciplinare che sanzioni l'eventuale violazione dei principi e delle disposizioni volte a prevenire la commissione dei reati.
- *Comunicazione/formazione al personale e informazione dei terzi*. Le verifiche sono state rivolte ad accertare l'esistenza di forme di comunicazione e formazione per i Destinatari e i terzi in materia di D.Lgs. 231/01.

3.5. STRUTTURA DEL DOCUMENTO

Il presente Modello è costituito da una "Parte Generale" e da una "Parte Speciale".

Nella "Parte Generale", dopo un richiamo ai principi del Decreto, alle linee Guida di Confindustria nonché alle motivazioni di adozione del Modello, vengono illustrate:

- le componenti essenziali del Modello, con particolare riferimento all'OdV;
- 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.

La "Parte Speciale" evidenzia, per ogni area a rischio individuata:

- la descrizione del potenziale profilo di rischio;
- le attività a rischio e le Funzioni coinvolte nell'ambito delle aree a rischio;
- i protocolli di controllo specifici.

Inoltre costituiscono parte integrante del presente Modello i documenti *Hitachi Group Code of Ethics and Compliance* e *Hitachi Group Codes of Conduct* (Allegato 1), che esplicita i valori e comportamenti a cui i Destinatari devono adeguarsi.

3.6. ELEMENTI DEL MODELLO

Di seguito vengono descritti gli elementi su cui si fonda il Modello.

- ***Sistema organizzativo***. Il sistema organizzativo della Società (Funzioni/posizioni organizzative, missioni ed aree di responsabilità) viene definito dal Country Leader e formalizzato in documenti elaborati e diffusi al personale.
- ***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;
  - coloro che agiscono in nome e per conto della Società nei confronti di terzi, ed in particolare della Pubblica Amministrazione, devono essere a ciò delegati.

  Qualora il legale rappresentante della Società venga indagato o imputato per la commissione del reato presupposto da cui dipende la responsabilità amministrativa dell'ente, questi non potrà procedere alla nomina del difensore di fiducia della Società in ragione del generale e assoluto

divieto di rappresentanza posto dall'art. 39 del D.Lgs. 231/01[2]. Per questo motivo, HVI prevede quale regola cautelare per prevenire tale possibile situazione di conflitto di interesse che - nella circostanza prima indicata - sia il soggetto *pro tempore* facente funzione di "legal counsel" della Società a essere specificamente autorizzato a compiere ogni attività necessaria per dotare l'ente di un difensore.

- ***Procedure***. Le procedure aziendali (sviluppate laddove necessarie per attività non demandate ad altre società del Gruppo Hitachi Vantara ovvero non regolamentate da procedure/policy di Gruppo), sono caratterizzate dai seguenti elementi:
  - separazione, per quanto possibile, all'interno di ciascun processo, tra il soggetto che assume la decisione, il soggetto che la autorizza, il soggetto che esegue tale decisione ed il soggetto cui è affidato il controllo del processo;
  - traccia scritta di ciascun passaggio rilevante del processo, incluso il controllo (c.d. "tracciabilità");
  - adeguato formalizzazione.
- ***Controllo di gestione***. Il sistema di controllo di gestione è articolato in base alle indicazioni della Capogruppo e in modo tale da riuscire ad analizzare i consuntivi periodici rispetto al budget e quindi elaborare le riprevisioni. 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***. La documentazione di Hitachi Vantara Italia è 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.
- ***Gestione dei flussi finanziari***. Tale gestione è definita sulla base di principi improntati ad una 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. Tale segregazione è garantita anche per quanto riguarda i flussi finanziari in entrata. Infine la gestione della liquidità è ispirata a criteri di conservazione del patrimonio, con connesso divieto di effettuare operazioni finanziarie a rischio.

Per gli altri elementi su cui si fonda il Modello (Codice Etico e di Condotta, OdV, sistema disciplinare, sistema di informazione e formazione del personale, sistema di informazione a terzi), si rinvia rispettivamente all'allegato 1 e ai successivi capitoli della Parte Generale del Modello specificamente dedicati.

3.7. MODIFICHE ED INTEGRAZIONI DEL MODELLO

Essendo il Modello un "atto di emanazione dell'organo dirigente", in conformità all'art. 6, comma 1, lettera a del Decreto, la sua adozione, così come le successive modifiche e integrazioni sono rimesse alla competenza del CdA della Società.

È riconosciuta al Country Leader la facoltà di apportare direttamente modifiche o integrazioni di carattere formale al Modello, in virtù della necessità di garantire un costante e tempestivo adeguamento dello stesso ai sopravvenuti mutamenti di natura operativa e/o organizzativa all'interno della Società, tra i quali, ad esempio:

- l'integrazione delle macro attività operative, indicate nella Parte Speciale del Modello. In tal caso il Country Leader è tenuto a comunicare i cambiamenti del Modello al CdA nella prima seduta utile successiva all'effettuazione delle modifiche;

[2] Cfr. Sentenza della Corte di Cassazione, sez. III, del 25 luglio 2023, n. 32110.

- il cambiamento di denominazione, l'accorpamento o la separazione di alcune funzioni aziendali;
- l'aggiornamento dell'elenco dei presidi organizzativi.

L'Organismo di Vigilanza è previamente consultato per ogni modifica da apportarsi al Modello.

4. ORGANISMO DI VIGILANZA

4.1. IDENTIFICAZIONE DELL'ORGANISMO DI VIGILANZA

Secondo le indicazioni delle Linee Guida di Confindustria, le caratteristiche dell'OdV – affinché il medesimo possa svolgere le attività sulla base delle indicazioni contenute negli artt. 6 e 7 del Decreto - debbono essere:

a) Autonomia e indipendenza. I requisiti di autonomia e indipendenza sono fondamentali affinché l'OdV non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo. Tali requisiti si possono ottenere escludendo qualsiasi dipendenza gerarchica dell'OdV all'interno della Società e prevedendo un'attività di reporting al CdA.

b) Professionalità. L'OdV deve possedere competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite all'indipendenza, garantiscono l'obiettività di giudizio.

c) Continuità d'azione. L'OdV deve:

- vigilare sul Modello con i necessari poteri d'indagine;
- curare l'attuazione del Modello e assicurarne aggiornamento;
- non svolgere mansioni operative che possano condizionare la visione d'insieme delle attività aziendali che ad esso si richiede.

L'OdV, istituito ai sensi dell'art. 6, lettera b del Decreto, è un organismo plurisoggettivo, composto da tre membri, di cui uno con la qualifica di Presidente. Il CdA determina, all'atto della nomina, la remunerazione spettante all'OdV.

L'avvenuto conferimento dell'incarico è comunicato a tutti i dipendenti e collaboratori della Società.

Tale Organismo potrà avvalersi, nello svolgimento dei propri compiti, del supporto delle Funzioni aziendali che, di volta in volta, saranno ritenute utili allo svolgimento delle attività di propria competenza.

L'OdV è dotato di un proprio Regolamento volto a disciplinare il suo funzionamento e lo svolgimento delle proprie attività, con particolare riferimento alla periodicità delle riunioni e alle modalità di svolgimento e verbalizzazione delle stesse, alle modalità e tempistiche di programmazione delle attività di verifica e alla gestione delle segnalazioni, nonché alla raccolta e archiviazione delle informazioni.

L'OdV dispone, ai sensi dell'art. 6 del Decreto, di "*autonomi poteri di iniziativa e controllo*". In particolare:

- l'**autonomia ed indipendenza** delle quali l'Organismo deve necessariamente disporre sono assicurate dalla presenza di due membri esterni, uno con funzioni di Presidente, privi dunque di mansioni operative all'interno della Società e di interessi che possano confliggere con l'incarico, condizionandone l'autonomia di giudizio e valutazione, nonché dalla circostanza che l'OdV opera in assenza di vincoli gerarchici nel contesto della corporate governance societaria, riportando direttamente al CdA. Inoltre, le attività poste in essere dall'OdV non possono essere sindacate da alcun altro organismo o struttura aziendale, fatto salvo il potere-dovere del CdA di vigilare sull'adeguatezza dell'operato posto in essere dall'OdV. A tal fine è inoltre riconosciuto con cadenza annuale dal CdA all'OdV uno specifico budget di spesa, che dovrà essere impiegato esclusivamente per le spese necessarie all'espletamento delle proprie funzioni e di cui l'Organismo fornirà al CdA apposita rendicontazione del relativo utilizzo;
- la **professionalità** è assicurata dalle specifiche competenze in materia dei suoi componenti e dalla facoltà riconosciuta all'Organismo di avvalersi, per lo svolgimento del suo incarico e con

assoluta autonomia di budget, delle specifiche professionalità sia delle varie Strutture aziendali sia di consulenti esterni. I componenti esterni sono individuati tra professionisti di comprovata competenza ed esperienza nelle tematiche giuridiche, finanziarie e di controllo interno, che hanno maturato un'adeguata e comprovata esperienza nell'ambito di applicazione del Decreto;

- la **continuità di azione** è garantita dalla circostanza che:
  - l'Organismo è libero di operare presso la Società nei tempi e nei modi che ritiene più opportuni per lo svolgimento dell'incarico assegnatogli;
  - fa parte dell'OdV un componente interno che non ha ruoli operativi all'interno della Società;
  - è informato tempestivamente e su base continuativa attraverso i flussi informativi periodici e ad hoc.

L'OdV riferisce al CdA della Società.

La nomina quale componente dell'OdV è condizionata alla presenza dei requisiti professionali e di onorabilità, nonché all'assenza di cause di incompatibilità con la nomina stessa, quali – a titolo esemplificativo – relazioni di parentela con gli esponenti degli organi e vertici della Società e potenziali conflitti di interesse con il ruolo ed i compiti che andrebbe a svolgere. In tale contesto, costituiscono motivi di ineleggibilità dell'OdV:

- avere rapporti di coniugio, parentela o di affinità entro il quarto grado con gli Amministratori della Società;
- intrattenere, direttamente o indirettamente, relazioni economiche e/o rapporti contrattuali, a titolo oneroso o gratuito, con la Società, di rilevanza tale da condizionarne l'autonomia di giudizio;
- essere titolare, direttamente o indirettamente, di quote del capitale sociale di Hitachi Vantara Italia o essere legato da altri rapporti patrimoniali, tali da permettere di esercitare il controllo o un'influenza notevole sulla Società, ovvero comunque da comprometterne l'indipendenza;
- essere titolare di deleghe che possano minarne l'indipendenza del giudizio;
- 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 stati sottoposti 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, per il Presidente, da cause di ineleggibilità ai sensi degli artt. 2399 lett. c e 2409-septiesdecies c.c..

I componenti esterni dell'OdV restano in carica per tre anni e rimangono, in ogni caso, in carica fino alla nomina dei loro successori.

La cessazione dalla carica di componente dell'Organismo potrà essere, altresì, determinata da rinuncia, decadenza o revoca ed in ogni caso sarà compito del CdA provvedere senza indugio alla sostituzione.

La rinuncia di un componente dell'Organismo può essere esercitata in qualsiasi momento e deve essere comunicata al CdA formalmente, unitamente alle motivazioni che l'hanno determinata.

La decadenza di un componente dell'Organismo 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.

Ove sopraggiungano cause di incompatibilità, l'OdV è tenuto a darne comunicazione formale al CdA; quest'ultimo, esperiti gli opportuni accertamenti per il tramite del Legal Business Partner, stabilisce un termine non inferiore a 30 giorni entro il quale deve cessare la situazione di incompatibilità. Trascorso tale termine senza che la predetta situazione sia cessata, il CdA deve dichiarare l'avvenuta decadenza dell'Organismo ed assumere le opportune deliberazioni.

Il sopraggiungere di cause di incompatibilità potrebbe essere rilevato anche da persona diversa dall'interessato, che provvede a darne comunicazione formale al CdA che procederà come sopra descritto.

Parimenti, l'interdizione o l'inabilitazione, ovvero una grave infermità che renda l'OdV inidoneo a svolgere le proprie funzioni di vigilanza per un periodo superiore a sei mesi, comporterà la dichiarazione di decadenza dell'Organismo, da attuarsi con le modalità sopra definite.

Per garantire la necessaria stabilità dell'OdV e tutelare il legittimo svolgimento delle funzioni e della posizione ricoperta da una rimozione ingiustificata, un componente dell'OdV può essere revocato solo per giusta causa. A tale proposito, per "giusta causa" di revoca possono intendersi, a titolo esemplificativo:

- un grave inadempimento dei propri doveri così come definiti nel Modello;
- una sentenza di condanna della Società ai sensi del Decreto o una sentenza di patteggiamento, passata in giudicato, ove risulti l'"omessa o insufficiente vigilanza" da parte dell'Organismo, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;
- una sentenza di condanna o di patteggiamento emessa nei confronti dell'Organismo per aver commesso uno dei reati previsti dal Decreto o reati della stessa natura;
- il venire meno di uno dei requisiti morali o professionali che costituiscono *condicio sine qua non* per la nomina dell'OdV;
- la violazione degli obblighi di riservatezza cui è tenuto l'OdV in ordine alle notizie ed informazioni acquisite nell'esercizio delle sue funzioni. In particolare l'OdV deve assicurare la riservatezza delle informazioni di cui viene 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 dell'OdV deve essere trattata in conformità con la legislazione vigente in materia e, in particolare, in conformità con le norme sulla privacy;
- la commissione di condotte in violazione del Modello e/o del Codice Etico e di Condotta.

Ove sussistano gravi ragioni di convenienza (ad esempio applicazione di misure cautelari), il CdA potrà disporre – sentito il parere del Sindaco Unico, se non è lui stesso il componente dell'OdV interessato – la sospensione dalle funzioni di componente dell'OdV, provvedendo tempestivamente alla nomina di un nuovo componente dell'Organismo.

4.2. FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA

La mission dell'OdV della Società 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'OdV:

- monitorare la validità nel tempo del Modello, promuovendo, anche previa consultazione delle Funzioni interessate, le azioni necessarie al fine di assicurarne l'efficacia. Tale compito comprende la formulazione di proposte di adeguamento da inoltrare alle Funzioni competenti e la successiva verifica dell'attuazione e della funzionalità delle soluzioni proposte;
- effettuare la verifica del corretto svolgimento, presso le Funzioni aziendali ritenute a rischio di reato, delle attività aziendali, in conformità al Modello adottato e proporre l'aggiornamento e l'integrazione delle stesse, ove se ne evidenzi la necessità;

- effettuare una verifica dei poteri autorizzativi e di firma esistenti, per accertare la loro coerenza con le responsabilità organizzative e gestionali definite e proporre il loro aggiornamento e/o modifica ove necessario, nonché allo scopo di verificare l'esercizio degli stessi nell'ambito delle attribuzioni assegnate;
- proporre, sulla base dei risultati ottenuti, alle Funzioni aziendali competenti/Country Leader, l'opportunità di elaborare, integrare e modificare procedure, che regolamentino adeguatamente lo svolgimento delle attività, al fine di implementare un idoneo Modello;
- definire e monitorare i flussi informativi per essere periodicamente aggiornato dai soggetti interessati sulle attività valutate a rischio di reato;
- accertarsi che siano portate a conoscenza dei Destinatari del Modello le modalità con cui è possibile inviare all'OdV segnalazioni in merito a comportamenti o eventi che possano determinare una violazione del Modello o che siano rilevanti ai sensi della normativa di cui al D.lgs. n. 231/01;
- attuare, in conformità al Modello, un efficace flusso informativo nei confronti del CdA che consenta all'Organismo di riferire allo stesso in merito all'attività di vigilanza svolta;
- promuovere un adeguato processo formativo del personale attraverso idonee iniziative per la diffusione della conoscenza e della comprensione del Modello, nonché l'adeguata informativa di coloro che operano per conto della Società con riferimento al Codice Etico e di Condotta adottato.

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

- accedere a ogni documento e/o informazione aziendale rilevante per lo svolgimento delle funzioni attribuitegli ai sensi del Decreto;
- assicurarsi che i Responsabili delle Funzioni aziendali forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste;
- avvalersi delle Funzioni aziendali che si potranno rendere utili all'espletamento delle attività di propria competenza;
- 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;
- procedere, qualora si renda necessario, alla richiesta di informazioni, nonché all'audizione diretta di Amministratori, Dipendenti, terzi.

4.3. INFORMATIVA DELL'ORGANISMO DI VIGILANZA NEI CONFRONTI DEGLI ORGANI SOCIETARI

In merito all'attività di reporting, l'OdV della Società provvede a fornire un'informativa scritta annuale nei confronti del CdA e dell'Organo di Controllo. In particolare, il reporting avrà a 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 di infrazioni del Modello ricevute nel corso del periodo e le azioni intraprese dall'OdV stesso e dagli altri soggetti interessati a fronte di tali segnalazioni;
- le attività cui non si è potuto procedere per giustificate ragioni di tempo e/o risorse e/o altro impedimento motivato;
- lo stato dell'attuazione del Modello con indicazione dei necessari e/o opportuni interventi correttivi e migliorativi dello stesso ed il loro livello di implementazione;
- il Piano di attività per il periodo successivo.

L'Organismo dovrà riferire tempestivamente al CdA (o al solo Presidente qualora ritenuto opportuno per maggiore rapidità di intervento) in merito a qualsiasi informazione ritenuta utile per l'assunzione di determinazioni urgenti da parte del CdA/Presidente.

4.4. FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

L'art. 6, comma 2, lett d) del Decreto impone la previsione nel Modello 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.

E' possibile contattare l'OdV indirizzando la comunicazione ad "Organismo di Vigilanza di Hitachi Vantara Italia S.r.l.", presso la sede della Società in Via del Bosco Rinnovato, 9, 20090 Assago (MI) oppure tramite la casella email dedicata "*OdV.Italia@hitachivantara.com*".

Per le specifiche informazioni che devono essere obbligatoriamente trasmesse dalle Funzioni all'Organismo con cadenza ad hoc o periodica, si rinvia al capitolo 2 della Parte Speciale del Modello.

4.5. SEGNALAZIONI ALL'ODV (WHISTLEBOLWING)

Nell'ambito del sistema di whistleblowing sviluppato dal Gruppo Hitachi Vantara, la Società mette a disposizione di chiunque volesse effettuare una segnalazione all'OdV un canale informatico indipendente, disponibile all'indirizzo https://www.hitachivantara.com/hotline, che permette di effettuare segnalazioni:

- scritte;
- orali tramite hotline (telefono).

Il componente interno dell'OdV monitora le eventuali segnalazioni ricevute, coinvolgendo l'OdV qualora la segnalazione afferisca ad ambiti riguardanti il Modello o condotte rilevanti ai sensi del D.Lgs. 231/01.

Nel caso in cui il segnalante volesse presentare la segnalazione in un incontro, lo può richiedere per email all'indirizzo "*OdV.Italia@hitachivantara.com*".

Tali canali garantiscono la riservatezza dell'identità del segnalante, della persona coinvolta, della persona comunque menzionata nella segnalazione, del contenuto della segnalazione e della relativa documentazione nonché di qualsiasi altra informazione o elemento della segnalazione dal cui disvelamento si possa dedurre direttamente o indirettamente l'identità del segnalante.

I Destinatari del Modello sono, pertanto, tenuti a segnalare all'OdV ogni informazione, di qualsiasi tipo, proveniente anche da terzi, di cui siano venuti a diretta conoscenza e attinente alla violazione del Modello nelle aree di attività a rischio o a eventuali altre irregolarità rilevanti ai sensi del Decreto. Segnatamente:

- la commissione di reati richiamati dal Decreto o il compimento di atti idonei diretti alla realizzazione degli stessi;
- comportamenti non in linea con le regole di condotta previste dal presente Modello;
- operazioni di particolare rilievo o che presentino profili di rischio tali da indurre a ravvisare il ragionevole pericolo di commissione di reati.

Le segnalazioni di condotte illecite dovranno essere circostanziate e fondate su elementi di fatto precisi e concordanti, e potranno essere effettuate utilizzando gli appositi canali indicati nel paragrafo precedente.

L'OdV prenderà in considerazione tutte le segnalazioni ricevute, comprese quelle pervenute in forma anonima, purché adeguatamente circostanziate; valuterà le eventuali conseguenti iniziative a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto ogni relativa decisione assunta.

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/di Gruppo interessate, 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.

Quando è accertata anche con sentenza di primo grado la responsabilità penale della persona segnalante per i reati di diffamazione o calunnia ovvero la sua responsabilità civile per lo stesso titolo, nei casi di dolo o colpa grave, a questi è irrogata una sanzione disciplinare.

La Società:

- tutela coloro che effettuano segnalazioni in buona fede, da ritorsioni, discriminazioni o penalizzazioni, dirette o indirette, per motivi collegati alla segnalazione;
- vieta atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- garantisce la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede;
- garantisce che il personale sia a conoscenza delle procedure di segnalazione e sia in grado di usarle, essendo consapevole dei propri diritti e delle tutele nel quadro delle procedure adottate, attraverso idonea comunicazione secondo le modalità previste nel capitolo 5;
- provvede, in caso di riscontrata violazione delle misure di tutela del segnalante, nonché di segnalazioni infondate rivelate con dolo o colpa grave, a identificare e applicare la sanzione ritenuta più adeguata alla circostanza, in accordo con quanto definito successivo capitolo 6.

4.6. RACCOLTA, CONSERVAZIONE E ACCESSO ALL'ARCHIVIO DELL'ODV

Ogni informazione, segnalazione, report previsti nel Modello sono conservati dall'OdV in un apposito archivio, il cui accesso è consentito nei termini riportati nel Regolamento dell'Organismo.

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

5.1. FORMAZIONE DEL PERSONALE

La Società promuove la conoscenza del Modello e del Codice Etico e di Condotta tra i dipendenti che sono pertanto tenuti a conoscerne il contenuto, ad osservarli e a contribuire alla loro attuazione.

Human Resources, in cooperazione con l'OdV, gestisce la formazione del personale sui contenuti del D.Lgs. 231/01 e sull'attuazione del Modello.

Il percorso di formazione prevede seminari formativi in aula / modalità e-learning al personale direttivo e a quello titolare di procure. Per il resto del personale le modalità di formazione prevedono anche la possibilità di utilizzo di modalità "e-learning". La partecipazione alle sessioni di formazione è obbligatoria.

La tracciabilità della partecipazione all'attività di formazione è attuata attraverso la predisposizione dell'elenco dei partecipanti e la relativa sottoscrizione da parte degli stessi ovvero attraverso modalità informatiche nel caso di formazione tramite piattaforma e-learning.

Eventuali sessioni formative di aggiornamento saranno effettuate in caso di rilevanti modifiche apportate al Modello, al Codice Etico e di Condotta o relative a sopravvenute novità normative rilevanti per l'attività della Società, ove l'OdV non ritenga sufficiente la semplice diffusione della modifica con le modalità descritte nel successivo paragrafo 5.2.

5.2. INFORMATIVA AL PERSONALE

La Società, oltre alla sopra evidenziata attività di formazione, provvede a dare al personale un'adeguata informativa in merito a:

- novità normative in tema di responsabilità amministrativa degli Enti;
- modifiche procedurali ed organizzative.

E' responsabilità di EMEA Regional Compliance, in cooperazione con l'OdV curare:

- l'inserimento del Modello e del Codice Etico e di Condotta nell'intranet aziendale;
- l'invio di comunicazioni sulle modifiche apportate al Modello, al Codice Etico e di Condotta, nonché relativamente a modifiche normative rilevanti per il Decreto.

E' responsabilità di Human Resources curare la distribuzione del Modello e del Codice Etico e del Codice di Condotta ai nuovi assunti al momento dell'assunzione.

5.3. INFORMATIVA A COLLABORATORI ESTERNI E PARTNER

La Società promuove la conoscenza e l'osservanza del D.Lgs. 231/01 e del Codice Etico e di Condotta anche tra i partner commerciali e finanziari, i consulenti, gli agenti, i collaboratori a vario titolo ed i fornitori della Società.

L'informativa avviene, per i soggetti prima elencati, attraverso la comunicazione dell'esistenza del Modello e del Codice Etico e di Condotta e la pubblicazione nel sito internet della Società della Parte Generale del Modello e del Codice Etico e di Condotta.

La Società inoltre provvede a inserire nei contratti con le controparti sopra menzionate apposite clausole contrattuali che prevedono, in caso di comportamenti non in linea con il D.Lgs. 231/01, opportune sanzioni sino alla risoluzione degli obblighi negoziali. Anche in questo caso eventuali eccezioni devono essere motivate e portate all'attenzione dell'OdV.

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

6.1. 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 devono *"introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello"*.

Per il 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.

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 dalla Società in piena autonomia ed indipendentemente dalla tipologia di illecito che le violazioni del Modello stesso possano determinare.

L'individuazione e l'applicazione delle sanzioni 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.

E' responsabilità:

- dell'OdV monitorare costantemente l'adeguatezza del sistema disciplinare;
- di Human Resources aggiornare il sistema disciplinare.

6.2. SANZIONI PER I LAVORATORI DIPENDENTI

6.2.1. IMPIEGATI, OPERAI E QUADRI

I comportamenti tenuti dai lavoratori dipendenti in violazione delle regole comportamentali del presente Modello, ivi compreso il mancato rispetto delle procedure aziendali costituiscono illeciti disciplinari.

Con riferimento alle sanzioni irrogabili nei riguardi dei lavoratori dipendenti esse rientrano tra quelle previste dal Contratto Collettivo Nazionale applicato, nel rispetto delle procedure previste dall'articolo 7 dello Statuto dei lavoratori ed eventuali normative speciali applicabili.

In particolare, in conformità al vigente Contratto Collettivo Nazionale dei Lavoratori Metalmeccanici, si prevede che:

- incorre nel provvedimento di *richiamo verbale* il dipendente che adotti un comportamento non conforme alle prescrizioni del presente Modello o del Codice Etico e di Condotta laddove si tratti di comportamento di non grave entità e non produttivo di effetti rilevanti per il funzionamento del Modello e prontamente rilevato dallo stesso dipendente;
- incorre nel provvedimento di *ammonizione scritta* il dipendente che adotti un comportamento non conforme alle prescrizioni del presente Modello o del Codice Etico e di Condotta laddove si tratti di comportamento di non grave entità e non produttivo di effetti rilevanti per il funzionamento del Modello ed emerso in virtù di controlli effettuati da soggetti interni diversi da chi ha commesso la violazione;
- incorre nel provvedimento della *multa non superiore a tre ore di retribuzione* il dipendente che incorra per più di due volte nel corso dell'anno in comportamenti non conformi alle prescrizioni del presente Modello o del Codice Etico e di Condotta, laddove si tratti di comportamenti non produttivi di effetti rilevanti per il funzionamento del Modello;
- incorre nel provvedimento della *sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni* il dipendente che violi in modo non lieve le procedure aziendali interne adottando un comportamento non conforme alle prescrizioni del presente Modello o del Codice Etico e di Condotta ed esponendo la Società a rischio di danno o a lieve danno, o le procuri vantaggio in violazione delle disposizioni contenute nel Codice Etico e di Condotta;
- incorre nel *licenziamento con preavviso* il dipendente che adotti un comportamento gravemente non conforme alle prescrizioni del presente Modello o del Codice Etico e di Condotta;
- incorre nel *licenziamento senza preavviso* il dipendente che, comunque, per inosservanza di disposizioni del presente Modello e/o del Codice Etico e di Condotta, provochi alla Società grave nocumento morale o materiale o compia azioni che costituiscono delitto a termini di legge, determinando una grave lesione del vincolo fiduciario tale per cui il rapporto non possa essere proseguito.

6.2.2. DIRIGENTI

In caso di violazione da parte di dirigenti del presente Modello o di adozione di un comportamento non conforme alle prescrizioni del Modello stesso, si provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal vigente Contratto Collettivo Nazionale di Lavoro.

In particolare:

- in caso di violazione non grave di una o più regole procedurali o comportamentali previste nel Modello o nel Codice Etico e di Condotta, il dirigente incorre nel *richiamo scritto* all'osservanza degli stessi, che costituisce condizione necessaria per il mantenimento del rapporto fiduciario con la Società;
- in caso di grave violazione di una o più prescrizioni del Modello o del Codice Etico e di Condotta 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 o del Codice Etico e di Condotta 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*.

6.3. MISURE NEI CONFRONTI DEGLI AMMINISTRATORI E DEL SINDACO UNICO

Nel caso di violazione del Modello da parte degli Amministratori o del Sindaco Unico della Società, l'OdV ne informerà il CdA o il Sindaco Unico, 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.

6.4. MISURE NEI CONFRONTI DI COLLABORATORI, CONSULENTI, PARTNER, CONTROPARTI COMMERCIALI ED ALTRI SOGGETTI ESTERNI

Ogni comportamento posto in essere nell'ambito di un rapporto contrattuale dai collaboratori, consulenti, partner, agenti, controparti commerciali e altri soggetti esterni, in contrasto con quanto indicato dal D.Lgs. 231/01 o dal Code of Ethics and Business Conduct, potrà determinare, grazie all'attivazione di opportune clausole, l'irrogazione delle seguenti sanzioni: diffida, applicazione di una penale (risarcimento dei danni) o risoluzione del rapporto contrattuale.

E' responsabilità della Società:

- curare l'elaborazione e l'aggiornamento di tali clausole contrattuali;
- curare l'inserimento negli accordi negoziali con i terzi tali clausole contrattuali.

6.5. PROCEDIMENTO DI APPLICAZIONE DELLE SANZIONI

Il procedimento di irrogazione delle sanzioni conseguenti alla violazione del Modello e delle procedure 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 della sanzione 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'OdV segnala la possibile rilevanza ex D.Lgs. 231/01 dell'episodio.

Più precisamente, nei casi in cui l'Organismo riceva una segnalazione ovvero acquisisca, nel corso della propria attività di vigilanza, gli elementi idonei a configurare il pericolo di una violazione del Modello, ha l'obbligo di attivarsi per espletare gli accertamenti rientranti nei propri compiti. Nel caso tale attività riguardasse il Sindaco Unico, gli altri componenti provvederanno a curare tali accertamenti.

Esaurita l'attività di verifica, l'OdV valuta, sulla base degli elementi in proprio possesso, la sussistenza delle condizioni per l'attivazione del procedimento disciplinare, procedendo così come indicato nei successivi capitoli 6.5.1 – 6.5.4.

6.5.1. IL PROCEDIMENTO DISCIPLINARE NEI CONFRONTI DEI DIPENDENTI NON DIRIGENTI

Il procedimento di applicazione della sanzione nei confronti di Dipendenti non dirigenti avviene nel rispetto dell'iter di seguito descritto nonché delle normative vigenti e del contratto collettivo applicabile.

In particolare, l'OdV trasmette al Responsabile di Human Resources una relazione contenente:

- le generalità del soggetto 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 Società, tramite il Responsabile di Human Resources, entro dieci giorni dall'acquisizione della relazione, trasmette al Dipendente una comunicazione di contestazione scritta contenente:

- l'indicazione puntuale della condotta constatata;
- le previsioni del Modello oggetto di violazione;
- l'avviso della facoltà di formulare eventuali deduzioni e/o giustificazioni scritte entro cinque giorni dalla ricezione della comunicazione, nonché di richiedere l'intervento del rappresentante dell'associazione sindacale cui il dipendente aderisce o conferisce mandato.

A seguito delle eventuali controdeduzioni dell'interessato, il Responsabile Human Resources decide se applicare o meno una sanzione, determinandone l'entità, e motiva il provvedimento.

Le sanzioni non possono comunque essere applicate prima che siano decorsi cinque giorni dalla ricezione della contestazione e devono essere comminate, a cura del Responsabile Human Resources, entro dieci giorni dall'invio della contestazione, o comunque entro il termine eventualmente inferiore che dovesse essere previsto dalla contrattazione collettiva applicabile nel caso concreto.. Se il provvedimento non viene comminato entro tale termine le giustificazioni si riterranno accolte.

Il relativo provvedimento è comunicato altresì all'OdV, che verifica inoltre l'effettiva applicazione della sanzione irrogata.

Il Dipendente, ferma restando la possibilità di adire l'Autorità Giudiziaria, può, nei venti giorni successivi la ricezione del provvedimento, promuovere la costituzione di un Collegio di conciliazione ed arbitrato, restando in tal caso la sanzione sospesa fino alla relativa pronuncia.

Nell'ambito dell'iter sopra descritto, è previsto che il CdA della Società sia informato in merito agli esiti delle verifiche interne ed al profilo sanzionatorio applicato nei confronti dei dipendenti.

6.5.2. IL PROCEDIMENTO DISCIPLINARE NEI CONFRONTI DEI DIRIGENTI

La procedura di accertamento dell'illecito con riguardo ai Dirigenti è espletata nel rispetto delle disposizioni normative vigenti nonché del vigente Contratto Collettivo Nazionale di Lavoro.

In particolare, l'OdV trasmette al Country Leader (nel caso in cui sia coinvolto il Country Leader, al Presidente del CdA) una relazione contenente:

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

Entro cinque giorni dall'acquisizione della relazione dell'OdV, il Country Leader convoca il Dirigente interessato mediante una comunicazione di contestazione contenente:

- l'indicazione della condotta constatata e l'oggetto di violazione ai sensi del Modello;
- l'avviso della data della audizione e la facoltà dell'interessato di formulare, anche in quella sede, eventuali considerazioni, sia scritte che verbali, sui fatti.

A seguire il Country Leader definirà la posizione dell'interessato, prendendo una decisione motivata in merito all'applicazione o meno di una sanzione.

Se il soggetto per cui è stata attivata la procedura di contestazione ricopre una posizione apicale con attribuzione di deleghe da parte del CdA, e nel caso in cui l'attività di indagine ne comprovi il coinvolgimento ai sensi del Modello, il Country Leader informa tempestivamente il CdA che deciderà sulla revoca delle deleghe attribuite in base alla natura dell'incarico e dell'eventuale sanzione da applicare. Il Country Leader provvederà a implementare il relativo procedimento sanzionatorio.

Il provvedimento di comminazione della sanzione è comunicato per iscritto all'interessato, entro dieci giorni dall'invio della contestazione, o comunque entro il termine eventualmente inferiore che dovesse essere previsto dalla contrattazione collettiva applicabile nel caso concreto, a cura del Country Leader.

Nell'ambito dell'iter sopra descritto, è previsto che il CdA sia informato in tutti i casi suddetti in merito agli esiti delle verifiche interne e al profilo sanzionatorio applicato.

L'OdV, cui è inviato per conoscenza il provvedimento di irrogazione della sanzione, verifica la sua applicazione.

Ferma restando la facoltà di adire l'Autorità giudiziaria, chi è interessato al procedimento può promuovere, nei venti giorni successivi alla ricezione del provvedimento disciplinare, la costituzione di un Collegio di conciliazione ed arbitrato, secondo quanto previsto dalla contrattazione collettiva applicabile al caso concreto.

In caso di nomina di tale Collegio, la sanzione disciplinare resta sospesa fino alla pronuncia di tale organo.

6.5.3. IL PROCEDIMENTO DISCIPLINARE NEI CONFRONTI DEGLI AMMINISTRATORI E DEL SINDACO UNICO

Qualora l'OdV riscontri la violazione del Modello da parte di un soggetto che rivesta la carica di Amministratore, il quale non sia legato alla Società da un rapporto di lavoro subordinato, trasmette al CdA una relazione contenente:

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

Entro dieci giorni dall'acquisizione della relazione dell'OdV, il CdA convoca il membro indicato dall'OdV 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;
- contenere l'indicazione della condotta contestata e delle previsioni del Modello oggetto di violazione;
- comunicare all'interessato la data della adunanza, con l'avviso della facoltà di formulare eventuali rilievi e/o deduzioni, sia scritte e sia verbali. La convocazione deve essere sottoscritta dal Presidente o da almeno due membri del Cda.

In occasione dell'adunanza del CdA, a cui è invitato a partecipare anche l'OdV, 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 CdA, sulla scorta degli elementi acquisiti, determina l'eventuale sanzione ritenuta applicabile.

Nel caso in cui è coinvolto l'intero (o più della metà) CdA, l'OdV, trasmette la relazione di cui sopra al Sindaco Unico che provvede a convocare l'Assemblea dei Soci, invitando a tale Assemblea anche i componenti del CdA

interessati. Una volta ascoltati i membri del CdA, l'Assemblea provvede a irrogare (o meno) la sanzione che ritiene più opportuna.

La delibera del CdA e/o quella dell'Assemblea, a seconda dei casi, viene comunicata per iscritto, a cura del CdA, all'interessato nonché all'OdV

Il procedimento sopra descritto trova applicazione anche qualora sia riscontrata la violazione del Modello da parte del Sindaco Unico, nei limiti consentiti dalle norme di legge applicabili. In questo caso è il CdA che provvede a convocare l'Assemblea dei Soci.

Nei 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 il procedimento previsto di seguito con riguardo ai Dirigenti/Dipendenti. Qualora all'esito di tale procedimento sia comminata una sanzione, il CdA convocherà senza indugio l'Assemblea dei Soci per deliberare i provvedimenti conseguenti.

6.5.4. IL PROCEDIMENTO NEI CONFRONTI DEI TERZI

Per consentire l'assunzione delle iniziative previste dalle clausole contrattuali indicate al par. 6.4, l'OdV trasmette al Responsabile della Funzione che gestisce il rapporto contrattuale e, per conoscenza al Country Leader (al Presidente del CdA nel caso in cui sia il Country Leader a gestire il rapporto contrattuale), una relazione contenente:

- gli estremi del soggetto 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 CdA della Società, dovrà essere trasmessa anche all'attenzione del medesimo.

Il Responsabile della Funzione che gestisce il rapporto contrattuale, d'intesa con la Funzione Legal Business Partner, sulla base delle eventuali determinazioni nel frattempo assunte dal Country Leader/CdA, invia all'interessato una comunicazione scritta contenente l'indicazione della condotta constatata nonché l'indicazione della clausola contrattuale di cui si chiede l'applicazione.

Il relativo provvedimento è comunicato all'OdV, che verifica l'effettiva applicazione della sanzione.

7. PRINCIPI GENERALI DI COMPORTAMENTO

Il presente Modello prevede l'espresso divieto a carico dei Destinatari di porre in essere comportamenti:

- tali da integrare qualsiasi fattispecie di reato (anche solo nella forma del tentativo), incluse pertanto anche quelle previste dal D.Lgs. 231/01 ed elencate nel capitolo 1.1 della presente Parte Generale;
- 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 con i principi espressi dal presente Modello o dal Codice Etico e di Condotta.

Pertanto, è fatto obbligo ai Destinatari del Modello di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge, del Codice Etico e di Condotta, dei principi contenuti nel presente Modello e delle procedure aziendali;
- svolgere le attività sociali nel rispetto assoluto delle leggi e delle normative nazionali ed internazionali vigenti;

- osservare una condotta tesa a garantire il regolare funzionamento della Società, assicurando ed agevolando ogni forma di controllo sulla gestione da parte degli Organi Sociali, dell'OdV e dell'Organo di Controllo;
- applicare costantemente le regole del presente Modello, del Codice Etico e di Condotta e delle norme interne aziendali, mantenendosi aggiornati sull'evoluzione normativa;
- curare che nessun rapporto venga iniziato con persone o enti che non abbiano intenzione di adeguarsi ai principi etici della Società;
- assicurare la veridicità, la completezza e la correttezza delle informazioni comunicate alla Pubblica Amministrazione, alle autorità di vigilanza o controllo nel rispetto della normativa vigente.

PARTE SPECIALE

1. FUNZIONE DELLA PARTE SPECIALE

La Parte Speciale del Modello ha l'obiettivo, coerentemente con i principi delineati nella Parte Generale, di definire e formalizzare per *ogni area di attività a rischio ex D.Lgs. 231/01 individuata*:

- il *potenziale profilo di rischio*, ovvero i reati che possono essere in astratto realizzati nell'area a rischio e le modalità di commissione degli stessi;
- le *attività a rischio e gli Enti coinvolti* ovvero le diverse attività aziendali a rischio e le Funzioni aziendali coinvolte nella loro gestione;
- i *protocolli di controllo specifici* che i Destinatari, così come individuati nella Parte Generale, sono tenuti a rispettare, intendendosi per tali i documenti aziendali che regolamentano l'operatività della Società, gli specifici strumenti e attività di controllo ritenuti rilevanti ai sensi della prevenzione dei reati di cui al D.Lgs. 231/01, applicabili alle attività ed ai processi a rischio-reato.

La presente Parte Speciale si applica ai Destinatari del Modello così come identificati nella Parte Generale dello stesso.

La Società si adopera, in linea con quanto descritto nel capitolo 5 della Parte Generale, affinché venga data ai Destinatari adeguata formazione in ordine ai contenuti della Parte Speciale.

Come già anticipato nella Parte Generale, per consentire all'OdV di essere periodicamente aggiornato dalle Funzioni aziendali interessate sulle attività a rischio di reato sono previsti obblighi informativi verso l'OdV, riepilogati nel successivo capitolo 2.

2. OBBLIGHI DI INFORMATIVA ALL'ODV

2.1. OBBLIGHI DI INFORMATIVA AD HOC

Di seguito le informazioni da trasmettere all'OdV al verificarsi dell'evento:

- a cura di Legal Business Partner:
  - i provvedimenti 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'articolazione dei poteri e il sistema delle deleghe adottato dalla Società ed eventuali modifiche che intervengano sullo stesso e sulla struttura organizzativa della Società;
  - gli atti di citazione relativi ai contenziosi;
  - le clausole contrattuali D.Lgs 231, a seguito di ogni modifica sostanziale;
  - l'indicazione dei terzi che non hanno aderito al Code of Ethics and Business Conduct;
- a cura di Human Resources le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;
- a cura della Funzione/Area competente, il modulo/verbale compilato a valle di un'ispezione ricevuta da rappresentanti della Pubblica Amministrazione;
- a cura del SPP (tramite ufficio personale/Payroll Specialist), la comunicazione circa gli eventuali infortuni/incidenti sul lavoro;
- a cura di EMEA IT Security, qualsiasi informazione riguardanti incidenti IT che hanno un impatto sulla Società;
- a cura di EMEA Regional Compliance, i report:
  - di Internal Audit che hanno ad oggetto verifiche sulla Società;
  - della società di revisione sul bilancio della Società.

2.2. OBBLIGHI DI INFORMATIVA PERIODICA

Di seguito le informazioni da trasmettere all'OdV con cadenza periodica:

- da parte di EMEA Regional Compliance:
  - le dichiarazioni trimestrali rilasciate dai referenti aziendali individuati nel MyComplianceManager tool;
  - i risultati che riepiloga la partecipazione dei dipendenti della Società ai compliance training svolti a livello di EMEA. L'invio è annuale;
- a cura di Human Resources:
  - l'elenco delle assunzioni con indicazione del nominativo, della qualifica e relativa previsione a budget e dell'accettazione del Codice Etico e di Condotta. L'invio è semestrale;
  - l'elenco dei provvedimenti premianti (bonus, premi, aumenti e promozioni) con indicazione del nominativo e della qualifica. L'invio è semestrale/annuale;
  - le evidenze dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate. L'invio è semestrale;
  - la documentazione relativa alla partecipazione del personale alla formazione svolta in attuazione del Modello. L'invio è annuale;
- a cura di RSPP, il verbale della riunione periodica ex art. 35 del D.Lgs 81/08 e s.m.i.. L'invio è annuale;

- a cura di Finance Manager:
  - il bilancio. L'invio è annuale;
  - il budget e i forecast. L'invio è trimestrale;
- a cura del Legal Business Partner, un report trimestrale relativo ai contenziosi in essere, con evidenza dei legali incaricati di seguire gli stessi e gli eventuali accordi transattivi.

3. AREE A RISCHIO REATO

In considerazione delle caratteristiche delle attività di business proprie della Società, del contesto operativo in cui esse si svolgono, della struttura organizzativa e di controllo adottate, le *aree a rischio-reato* identificate dalla Società sono le seguenti:

- attività commerciale e di vendita (paragrafo 3.1);
- installazione dei beni/erogazione dei servizi (paragrafo 3.2);
- acquisizione, progressione e gestione del personale (paragrafo 3.3);
- approvvigionamento di beni, servizi e consulenze (paragrafo 3.4);
- affari societari (paragrafo 3.5);
- amministrazione, finanza e controllo (paragrafo 3.6);
- risorse finanziarie (paragrafo 3.7);
- sistemi informativi (paragrafo 3.8);
- salute e sicurezza sul lavoro (paragrafo 3.9);
- tematiche ambientali (paragrafo 3.10);
- gestione precontenzioso e contenzioso (paragrafo 3.11);
- rapporti con istituzioni ed enti pubblici (paragrafo 3.12);
- donazioni, liberalità e omaggi (paragrafo 3.13).

L'individuazione delle aree a rischio, ovvero le modalità di gestione delle stesse, possono mutare nel tempo, in considerazione di diversi fattori, quali ad esempio:

- l'ampliamento/modifica delle fattispecie di reato previste dal D.Lgs. 231/01;
- il mutamento della struttura organizzativa/societaria/di business della Società;
- la rilevazione di comportamenti non in linea con le prescrizioni del Modello;
- la valutazione dell'inadeguatezza di determinate prescrizioni del Modello, non idonee a prevenire la commissione di reati nell'ambito delle aree a rischio reato.

Conseguentemente nel tempo, al mutare dei fattori sopra evidenziati o di altri fattori al momento non prevedibili, la Società verificherà, anche dietro impulso dell'OdV, la necessità di integrare/modificare le aree a rischio sopra evidenziate.

3.1. ATTIVITA' COMMERCIALE E DI VENDITA

3.1.1 DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Lo svolgimento delle attività commerciali e di vendita espone, in via potenziale, la Società alla commissione, in via diretta o strumentale, dei seguenti reati:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti Internazionali o degli organi delle Comunità Europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.), corruzione tra privati (art. 2635 comma 3 c.c.) e istigazione alla corruzione tra privati (art. 2635-bis comma 1 c.c.). Tali reati potrebbero essere commessi al fine di ottenere favori nell'ambito dello svolgimento delle attività aziendali attraverso la promessa di denaro o altra utilità a Funzionario Pubblico o soggetto appartenente ad una società privata, al fine di acquisire ordini/contratti con la PA o con il privato;
- traffico di influenze illecite (art. 346-bis c.p.). Tale ipotesi di reato potrebbe configurarsi qualora un esponente della Società ovvero un terzo, venuto a conoscenza che è in corso la finalizzazione di un contratto con una Pubblica Amministrazione, si offra di intercedere con un incaricato della stessa, suo conoscente, affinché consenta alla Società di concludere il contratto a condizioni particolarmente vantaggiose, chiedendo come corrispettivo di tale attività, il riconoscimento di una retribuzione maggiorata (nel caso di dipendente nella società) o di altra utilità (nel caso di soggetto terzo);
- truffa (art. 640, comma 2, n.1, c.p.). Tale reato potrebbe essere commesso attraverso la predisposizione di documentazione non veritiera in fase di offerta, ad esempio attraverso l'indicazione di aspetti tecnici non veritieri o di referenze non esistenti;
- induzione indebita a dare o promettere utilità (art. 319-quater c.p.), nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio induca la Società a dargli o promettere di dargli denaro o altra utilità, per ottenere l'assegnazione di un contratto con la PA;
- riciclaggio (art. 648-bis c.p.), nel caso in cui, nell'attività di vendita, la Società ceda un bene, per la cui produzione è stato utilizzato denaro, beni o altre utilità provenienti da delitto non colposo;
- ricettazione (art. 648 c.p.), nel caso in cui la Società venga pagata dal Cliente attraverso l'utilizzo di somme di provenienza illecita;
- associazione per delinquere ed associazione di tipo mafioso anche straniere (artt. 416 e 416-bis c.p.), nel caso in cui la Società ottenga il supporto di esponenti di associazioni delle tipologie suddette nell'aggiudicazione di appalti privati e pubblici;
- vendita di prodotti industriali con segni mendaci (art. 517 c.p.) e fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.). Tali reati si potrebbero verificare se la Società, nella predisposizione di un'offerta commerciale, utilizzasse segni mendaci oppure usurpasse titoli di proprietà industriale, ovvero utilizzasse disegni/pezzi coperti da proprietà industriale;
- terrorismo ed eversione dell'ordine democratico (art. 25-quater D.Lgs. 231/01), nel caso in cui coloro che supportano la Società nell'attività di vendita oppure i beneficiari dei beni/servizi erogati, sono direttamente o indirettamente, legati a soggetti che intendono porre in essere tali reati;
- delitti informatici e trattamento illecito di dati, contemplati dall'art. 24-bis D.Lgs. 231/01, tra cui:
  - reati di accesso abusivo ad un sistema informatico o telematico (615-ter c.p.);
  - detenzione, diffusione e installazione abusiva di apparecchiature, codici o altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.).

I delitti informatici potrebbero essere commessi attraverso l'accesso di un dipendente ai server/sistemi di un competitor nell'ambito del quale si appropri di dati/informazioni utili a conoscere le strategie commerciali applicate;

- autoriciclaggio (art. 648-ter.1 c.p.), nel caso in cui la Società, a seguito della commissione o del concorso in commissione di uno dei reati sopra indicati, nonché di altri delitti di cui al D.Lgs. 231/01, ottiene delle utilità che impiega, sostituisce o trasferisce, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

3.1.2 ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

Di seguito si evidenziano le macro attività individuate dalla Società come a potenziale rischio nell'attività commerciale e di vendita e gli Enti aziendali coinvolti nella loro gestione:

- Vendita Diretta (Responsabile attività Sales Team – Funzioni coinvolte Country Leader, Sales Team, Presales, Sales Operation, Global Services Operations, Professional Services, Global Delivery, Customer Support, Sales Finance, Order Management, Legal Business Partner);
- Vendita indiretta e gestione di distributori e rivenditori (Responsabile attività Partner&Alliance – Funzioni coinvolte Country Leader, Sales Team, Presales, Order Management, Legal Business Partner Sales Finance);
- Gestione degli eventi di marketing (Responsabile attività Marketing EMEA e/o Corporate – Funzioni coinvolte Marketing & Communication, Country Leader, Sales Team, Presales);
- Gestione degli ordini (Responsabile attività Order Management– Funzioni coinvolte Country Leader, Sales Team, Presales, Sales Operation, Global Services Operations, Professional Services, Global Delivery, Customer Support, Sales Finance, Order Management, Legal Business Partner).

3.1.3 PROTOCOLLI DI CONTROLLO SPECIFICI

Oltre che in conformità ai principi espressi nel Codice Etico e di Condotta e, con riferimento alla gestione dei rapporti con i Partner, ai principi contenuti nel *"Hitachi Vantara Partner Code of Ethics and Business Conduct"*; le attività connesse con la presente area a rischio devono essere gestite nel rispetto delle procedure aziendali/di Gruppo che prevedono:

- l'identificazione del Cliente, destinatario ultimo della fornitura, e la conduzione di verifiche circa la sua affidabilità (ad esempio in termini di rispetto della normativa antiriciclaggio, di terrorismo internazionale, etc.) sulla base di documenti, dati o informazioni ottenuti da fonti affidabili ed indipendenti;
- la gestione delle fasi di sviluppo/approvazione dell'offerta mediante il sistema informativo che garantisce:
  - il coinvolgimento di più Funzioni in fase di predisposizione, sia per quanto riguarda la definizione degli aspetti economici che tecnici;
  - un'adeguata segregazione delle mansioni tra le diverse Funzioni coinvolte nelle attività di negoziazione dell'offerta e sottoscrizione del contratto;
  - la determinazione del prezzo di vendita dei beni/erogazione di servizi e l'applicazione dell'eventuale scontistica:
    - sulla base di listini di prezzo standard preventivamente approvati e configurati a sistema;
    - richiedendo specifica autorizzazione al procuratore abilitato in caso di applicazione di prezzi/sconti che si discostino dai listini standard;
  - un'adeguata tracciabilità del processo di autorizzazione/approvazione delle offerte/contratti;

- l'archiviazione e conservazione della documentazione prodotta;

- la definizione di condizioni generali standard valide per tutti i clienti, ed il coinvolgimento del Legal Business Partner in caso di deroghe alle stesse;
- l'utilizzo di apposito portale informatico per la gestione delle candidature dei Partner commerciali/Rivenditori/Distributori e per la selezione degli stessi;
- la selezione dei Partner commerciali/Rivenditori/Distributori previo svolgimento di valutazioni ("due diligence") basate su una serie di elementi che comprendono:
  - il profilo storico dei Partner commerciali/Distributori/Rivenditori;
  - l'analisi della loro struttura e della solidità finanziaria;
  - le concrete e reali referenze possedute (quali ad es.: clienti, esperienza nell'attività di rivendita, esperienza nell'attività consulenziale, esperienza quale systems integrator, capacità esecutiva nel campo dei servizi, livello qualitativo delle attività di supporto);
- gli accordi con i Partner commerciali/Rivenditori/Distributori sono definiti per iscritto con l'evidenziazione di tutte le condizioni dell'accordo stesso e sono verificati ed approvati in base alle vigenti procedure e nel rispetto dei poteri conferiti;
- la definizione dei criteri per il riconoscimento di premi/incentivi agli Agenti / Partner / Distributori / Rivenditori che operano per la società e lo svolgimento di un'opportuna attività di monitoraggio sull'erogazione degli stessi;
- la definizione di condizioni contrattuali standard per la vendita di beni/erogazione di servizi, differenziate in funzione della tipologia prodotto/servizio offerto, contenenti in particolare:
  - clausole generali standard utilizzate in tutti contratti di vendita;
  - condizioni di licenza software, per tutelare la proprietà dei software e limitarne l'utilizzo (ad esempio regole in materia di: concessione della licenza e del software; licenza software a scopo di valutazione, software di terzi, open source software, restrizioni d'uso, copie autorizzate, cessioni di software, cessazione licenze);
  - condizioni di garanzia, manutenzione e assistenza (clausole che disciplinano, tra l'altro: durata e gestione della garanzia; gestione dei piani di manutenzione ed assistenza; esclusioni dalla garanzia, manutenzione e assistenza; svolgimento di servizi di monitoraggio a distanza; corrispettivi e pagamento, limitazioni di responsabilità, legge regolatrice, risoluzione);
  - clausole per i servizi in hosting, volte a regolare i diritti di licenza del software e di utilizzo dello stesso da parte del cliente nell'ambito dei servizi in hosting;
- la previsione nell'ambito dei diversi contratti della clausola di impegno al rispetto del D.Lgs. 231/01, con l'espressa possibilità della Società di risolvere il contratto, nonché di rivalersi in sede legale, con i soggetti che agiscono in maniera difforme alle regole aziendali;
- l'accettazione da parte del Partner/Rivenditore/Distributore del documento "Hitachi Vantara Partner Code of Ethics and Business Conduct".

La Società prevede inoltre:

- con riferimento alla gestione delle comunicazioni verso l'esterno e dei rapporti con i media:
  - che i rapporti con la stampa e con gli altri mezzi di comunicazione di massa sono riservati al Country Leader e chi da lui autorizzato e/o delegato e che tutte le informazioni rilasciate ai media devono essere approvate dalla Capogruppo e non devono riguardare informazioni riservate;
  - un'adeguata tracciabilità delle interviste;
  - rigorosi controlli, relativamente ai comunicati stampa, attinenti le informazioni privilegiate riguardanti la situazione economico patrimoniale e finanziaria della Società;

- con riferimento alla gestione delle sponsorizzazioni, dell'attività pubblicitaria e della partecipazione/organizzazione di eventi:
  - una chiara definizione dell'iter seguito nella scelta di partecipare/sponsorizzare un evento, effettuare attività pubblicitaria su un determinato mezzo e delle modalità di formalizzazione degli accordi con eventuali partner/controparti;
  - la formalizzazione ed approvazione delle analisi relative alle motivazioni che hanno portato alla scelta di un determinato canale pubblicitario ovvero alla decisione di partecipare ad un determinato evento;
  - l'iter seguito nella scelta e programmazione di un evento;
  - le modalità operative seguite nella preparazione, allestimento e disallestimento dell'evento, individuando i soggetti coinvolti;
  - le forme di rendicontazione sui costi e ritorni derivanti dall'evento;
  - la verifica, nel caso di sponsorizzazioni di soggetti privati, dell'attendibilità commerciale e professionale del partner. In ogni caso, le decisioni in merito alle sponsorizzazioni devono attenersi ai limiti di budget e devono essere sottoposte all'approvazione del soggetto a ciò preposto a livello di Capogruppo;
  - le modalità di archiviazione della documentazione di supporto e le attività di controllo svolte.

3.2. INSTALLAZIONE DEI BENI/EROGAZIONE DEI SERVIZI

3.2.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Lo svolgimento delle attività di installazione dei beni ed erogazione dei servizi espone, in via potenziale, la Società alla commissione dei reati:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti Internazionali o degli organi delle Comunità Europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.), nel caso in cui la Società offra o prometta dei benefici non dovuti ad un cliente o persona diversa, esponente della PA, (es. promessa di denaro, sostenimento di spese di ospitalità al di fuori dell'ordinarietà, ecc.) al fine di ottenere la validazione dell'attività svolta;
- traffico di influenze illecite (art. 346-bis c.p.). Tale ipotesi di reato potrebbe configurarsi qualora un esponente della Società ovvero un terzo, venuto a conoscenza che è in corso l'esecuzione di un contratto con un ente della Pubblica Amministrazione o con una società incaricata di un pubblico servizio, si offra di intercedere con un incaricato di tale ente/società, suo conoscente, affinché consenta alla Società di fatturare dei servizi non prestati, chiedendo come corrispettivo di tale attività, il riconoscimento di una retribuzione maggiorata (nel caso di dipendente nella società) o di altra utilità (nel caso di soggetto terzo);
- truffa (art. 640, comma 2, n.1, c.p.). Tale reato potrebbe essere commesso attraverso:
  - falsificazione, alterazione e omissione di dati documentali al fine di ottenere la validazione delle attività altrimenti non dovuta;
  - falsificazione, alterazione ed omissione di rendiconti periodici da rilasciare alla PA al fine di ottenere il benestare sulla consegna dei beni/raggiungimento degli obiettivi contrattuali.
- frode nelle pubbliche forniture (art. 356 c.p.), nel caso in cui la Società consegnasse ad un Cliente pubblico una fornitura significativamente difforme, ad esempio da un punto di vista qualitativo, rispetto a quanto pattuito;
- vendita di prodotti industriali con segni mendaci (art. 517 c.p.) e fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.). Tali reati si potrebbero verificare se la Società, nella realizzazione di una commessa, utilizzasse segni mendaci oppure usurpasse titoli di proprietà industriale, ovvero utilizzasse disegni/pezzi coperti da proprietà industriale;
- induzione indebita a dare o promettere utilità (art. 319-quater c.p.), nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio del cliente per il quale si sta lavorando, induca la Società a dargli o promettere di dargli denaro o altra utilità, per ottenere l'approvazione su un stato avanzamento dei lavori senza che siano stati raggiunti gli obiettivi contrattuali o l'attestazione di avvenuta prestazione senza che sia effettivamente avvenuta la consegna di materiale;
- corruzione tra privati (art. 2635 comma 3 c.c.) e istigazione alla corruzione tra privati (art. 2635-bis comma 1 c.c.), nell'ipotesi in cui un referente della Società corrompa, mediante offerta/promessa di denaro o altra utilità, il Project Manager (o altro dipendente) del cliente privato, al fine di ottenere, mediante la falsificazione/alterazione/omissione di dati documentali, la validazione delle attività altrimenti non dovuta;
- terrorismo ed eversione dell'ordine democratico (art. 25-quater D.Lgs. 231/01), nel caso in cui coloro che supportano la Società nell'erogazione dei servizi oppure i beneficiari dei servizi erogati dalla Società, sono direttamente o indirettamente, legati a soggetti che intendono porre in essere tali reati;
- delitti informatici e trattamento illecito di dati, contemplati dall'art. 24-bis D.Lgs. 231/01, tra cui:

- reati di accesso abusivo ad un sistema informatico o telematico (615-ter c.p.);
- detenzione, diffusione e installazione abusiva di apparecchiature, codici o latri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.);

ed alcuni reati in materi di violazione del diritto d'autore contemplati dall'art. 25-novies D.Lgs. 231/01, tra cui:

- abusiva duplicazione, per trarne profitto, di programmi per elaboratore;
- importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE.

I delitti informatici potrebbero essere commessi attraverso l'accesso di un dipendente ai server/sistemi del cliente nell'ambito del quale si appropri di dati/informazioni per utilizzarli a vantaggio della Società ovvero nell'introduzione di malware nei sistemi del cliente che necessitano lo svolgimento di un intervento di manutenzione da parte della Società altrimenti non necessario. L'abusiva duplicazione di un programma per elaboratore potrebbe essere commessa da un dipendente per potere rivedere il programma abusivamente procurando un vantaggio a favore della Società;

- emissione di fatture o altri documenti per operazioni inesistenti (art. 25-quinquiesdecies D.Lgs. 231/01 - art. 8 co. 1 e 2-bis d.lgs. 74/00). Tale reato potrebbe essere commesso qualora, al fine di consentire ad un terzo l'evasione delle imposte sui redditi o sul valore aggiunto, emetta fatture o altri documenti per operazioni mai rese, a fronte del riconoscimento da parte del terzo di un vantaggio economico per la Società quale, ad esempio, l'approvazione di una variante d'ordine da parte del Cliente;
- autoriciclaggio (art. 648-ter.1 c.p.), nel caso in cui la Società, a seguito della commissione o del concorso in commissione di uno dei reati sopra indicati, nonché di altri delitti di cui al D.Lgs. 231/01, ottiene delle utilità che impiega, sostituisce o trasferisce, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

3.2.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

Di seguito si evidenziano le macro attività individuate dalla Società come a potenziale rischio nell'installazione dei beni/erogazione dei servizi e gli Enti aziendali coinvolti nella loro gestione:

- Installazione e configurazione dei macchinari e gestione del cliente (avanzamento dei lavori, manutenzione, etc) (Responsabile attività Customer Support – Funzione coinvolta Global Delivery);
- Erogazione dei servizi professionali e gestione del cliente (avanzamento dei lavori, manutenzione, etc) (Responsabile attività Global Delivery – Funzioni coinvolte Global Services Operations, Professional Services).

3.2.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Oltre che in conformità ai principi espressi nel Codice Etico e di Condotta, le attività connesse con la presente area a rischio devono essere gestite nel rispetto delle procedure aziendali/di Gruppo che prevedono:

- la gestione degli ordini mediante il supporto del sistema informativo ("Sales Force"), che garantisce la tracciabilità di tutte le operazioni svolte;
- la verifica della disponibilità dei prodotti ordinati, la programmazione della consegna presso il cliente e la gestione delle relative problematiche;
- il coinvolgimento, ove necessario, di diverse Funzioni aziendali per la programmazione delle attività da svolgere e del cliente per analizzare e predisporre tutti i dettagli tecnici relativi alle attività da eseguire;

- lo svolgimento delle attività di manutenzione delle apparecchiature installate presso i Clienti previa verifica dello stato delle stesse;
- in fase di consegna delle apparecchiature al cliente e prima della relativa installazione, lo svolgimento di controlli di conformità del materiale consegnato rispetto all'ordine ricevuto e lo stato dello stesso;
- la verifica periodica dello stato avanzamento lavori opportunamente verbalizzato ed il monitoraggio della corretta esecuzione (collaudo/validazione) delle attività di installazione dei prodotti/erogazione dei servizi;
- formalizzazione delle attività svolte mediante la compilazione dei "Rapportino di installazione" e "Rapportino di disinstallazione";
- centralizzazione e razionalizzazione delle attività di accettazione e gestione di ogni tipologia di chiamata verso l'assistenza tecnica di Hitachi Vantara;
- automatismo di verifica dello stato contrattuale nella fase di presa in carico e apertura della chiamata cliente (via Hi-track e diretta) che consente di valutare e decidere attraverso Salesforce se accettare o meno la chiamata in assenza di contratto attivo di manutenzione.

3.3. ACQUISIZIONE, PROGRESSIONE E GESTIONE DEL PERSONALE

3.3.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Il processo di acquisizione, progressione di carriera e gestione del personale può comportare, in via teorica, il rischio di commissione dei reati:

- di terrorismo ed eversione dell'ordine democratico (art. 25-quater D.Lgs. 231/01), nel caso in cui si forniscano, direttamente o indirettamente, ma comunque volontariamente, fondi a favore di soggetti che intendono porre in essere reati di terrorismo, attraverso ad esempio l'assunzione di persone appartenenti/vicine ad associazioni aventi tali finalità o l'attribuzione di bonus/altri incentivi non dovuti a tali persone;
- di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies D.Lgs. 231/01), nel caso in cui la Società assuma ed impieghi personale straniero non in regola con il permesso di soggiorno. Tale reato può essere commesso anche nel corso del rapporto di lavoro, nel caso in cui venga a scadere in tale periodo il permesso di soggiorno del lavoratore;
- associazione per delinquere (art. 416 c.p.) di tipo mafioso anche straniera (art 416 bis c.p.), nel caso si assumano persone ad essa riconducibile o si riconoscano progressioni di carriera o si attribuiscano bonus/altri incentivi non dovuti a personale ad essa riconducibile.

Il processo di selezione, progressione di carriera e gestione del personale costituisce inoltre una delle modalità strumentali attraverso cui, in linea di principio, potrebbero essere commessi i reati:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.), concussione (art. 317 c.p.) e di induzione indebita a dare o premettere utilità (art. 319-quater c.p.);
- traffico di influenze illecite (art. 25 D.Lgs. 231/01 - art. 346-bis c.p.);
- di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.);
- di corruzione tra privati (art. 2635 comma 3 c.c.) e istigazione alla corruzione tra privati (art. 2635-bis comma 1 c.c.).

Per quanto riguarda le possibili modalità di commissione di tali reati, a titolo esemplificativo si riporta quanto segue:

- nella fase di selezione, l'assunzione o la promessa di assunzione, anche tramite interposta persona, di persona "vicina" o "gradita" a soggetti pubblici/privati da corrompere per ottenere favori nell'ambito dello svolgimento delle attività (es.: ottenimento di autorizzazioni da soggetti pubblici, anche per il tramite di qualcuno che eserciti influenze illecite, attribuzioni di commesse, ottenimento di condizioni di miglior favore per una fornitura, ecc.), non basata su criteri strettamente meritocratici;
- nella fase di progressione di carriera e gestione del personale, il riconoscimento o promessa, anche per interposta persona, di:
    - promozioni/avanzamenti di carriera/aumenti di stipendio/altre utilità a personale "vicino" o "gradito" a soggetti pubblici o assimilabili o a soggetti privati a fini corruttivi, non informati a criteri strettamente meritocratici;
    - bonus/incentivi "falsati/gonfiati" al fine di rendere disponibili somme di denaro utilizzabili per fini corruttivi sia direttamente attraverso l'accreditamento da parte del lavoratore dipendente di somma, o parte di essa, su un conto intestato ad una società estera facente capo al pubblico funzionario/privato da corrompere sia indirettamente attraverso la creazione di fondi occulti a disposizione della Società;

- per quel che riguarda il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, potrebbe ad esempio essere commesso attraverso l'assunzione di persona "vicina" a chi è tenuto a rendere dichiarazioni all'autorità giudiziaria o attraverso l'attribuzione di un bonus "gonfiato" o la promozione di una persona "gradita" a chi deve rilasciare dichiarazioni all'autorità giudiziaria.

3.3.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

Di seguito si evidenziano le principali attività individuate dalla Società come a potenziale rischio nell'acquisizione, progressione e gestione del personale e gli Enti aziendali coinvolti nella loro gestione:

- Selezione, gestione e formazione del personale (Responsabile attività Human Resources);
- Gestione delle buste paga, delle ferie e permessi, dei rimborsi spese, dell'erogazione dei bonus e delle commissioni, e dei relativi rapporti con il consulente esterno (Responsabile attività Human Resources, Payroll Specialist e Country Leader – Funzioni coinvolte Sales Finance);
- Gestione delle auto aziendali e delle fuel card (Responsabile attività Payroll Specialist – Funzioni coinvolte Country Leader, Sales Finance).

3.3.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Le attività connesse con la presente area a rischio devono essere gestite nel rispetto del Codice Etico e di Condotta, nonché dalle procedure aziendali/di Gruppo che prevedono:

- per quanto riguarda il processo di selezione e assunzione di personale:
  - la gestione delle richieste di nuovo personale e dell'iter di selezione mediante appositi sistemi informativi che garantiscano lo svolgimento di corretti iter autorizzativi e la tracciabilità delle operazioni;
  - le richieste di nuovo personale devono trovare adeguata previsione e copertura nel budget relativo al fabbisogno di organico approvato dal CdA; in caso contrario, è necessario effettuare una revisione del budget, che dovrà essere approvato dal Vertice aziendale, prima di avviare il processo di selezione e assunzione;
  - nella fase di individuazione del candidato da assumere, deve essere previsto il coinvolgimento di una pluralità di soggetti. Inoltre in tale fase deve essere garantito/a:
    - la tracciabilità delle fonti dei curricula in fase di acquisizione e di gestione degli stessi (e-recruitment, inserzioni, domande spontanee, presentazioni interne, ecc.);
    - il monitoraggio, in caso di ricorso ad agenzia interinale per il reclutamento dei candidati, sulle modalità di attivazione della stessa sul suo operato;
    - l'individuazione di una rosa di candidati, per quanto possibile in considerazione della tipologia di professionalità da assumere;
    - la valutazione sia tecnica che psico-attitudinale del candidato;
    - l'assegnazione della responsabilità delle varie tipologie di valutazione a soggetti distinti;
    - lo svolgimento di controlli in background sul candidato selezionato relativamente agli studi condotti e alle precedenti esperienze lavorative, nonché un "global sanction check";
    - la sottoscrizione da parte del candidato selezionato di una dichiarazione di assenza di conflitti d'interesse, in particolare per i casi di rapporti in corso (o avuti negli ultimi tre anni) con la Società (direttamente o da parte di parenti entro il secondo grado), in qualità di: rappresentante della PA con potere decisionale; cliente/fornitore/partner;

- in fase di formulazione dell'offerta ed assunzione, devono essere previste le seguenti attività:
    - verificare l'esistenza della documentazione accertante il corretto svolgimento delle fasi precedenti, da parte di un soggetto diverso da quello richiedente o da colui il quale ha partecipato attivamente alla selezione;
    - garantire che la definizione delle condizioni economiche sia coerente con la posizione ricoperta dal candidato e le responsabilità/compiti a lui assegnati;
    - prevedere che il contratto di assunzione sia sottoscritto da persona dotata di idonea procura;
    - verificare, in caso di assunzione di personale extracomunitario, la regolarità del permesso di soggiorno;
    - definire un kit di documenti da richiedere al candidato prima della sua assunzione per verificare l'esistenza di adeguati requisiti etici e morali;
- in fase di assunzione, devono essere previste le seguenti attività:
    - erogazione nei confronti del neoassunto di un'attività formativa sui contenuti del Modello e del Codice Etico e di Condotta;
    - ottenimento della dichiarazione di ricezione e dell'impegno al rispetto contenuti dei documenti di cui al punto precedente;
    - informativa al neoassunto relativamente a:
        - caratteristiche della funzione e delle mansioni da svolgere;
        - elementi normativi e retributivi, come regolati dal Contratto Collettivo Nazionale di Lavoro e da eventuali regolamenti aziendali;
        - norme e procedure da adottare per evitare i possibili rischi per la salute associati all'attività lavorativa;
    - comunicazione dell'assunzione all'outsourcer per assolvere agli obblighi nei confronti degli enti pubblici di riferimento;
- l'archiviazione in formato cartaceo/informatico dei dati/documenti/atti, mediante creazione di apposito fascicolo per ogni dipendente, predisposti nel corso delle attività di selezione, per assicurare la tracciabilità del processo di selezione ed assunzione;

- per quanto riguarda il processo di gestione del personale:
    - la definizione delle principali attività nonché dei ruoli e delle responsabilità nel processo di gestione del personale;
    - adeguati sistemi di rilevazione e verifica delle presenze ;
    - la definizione di regole per la gestione delle richieste e del rilascio delle autorizzazioni per ferie e permessi, per le comunicazioni di malattie e per tutto ciò che concerne la determinazione del costo del personale;
    - l'autorizzazione alle trasferte ed il rimborso delle relative spese, prevedendo in particolare:
        - le modalità di autorizzazione delle trasferte mediante apposito sistema applicativo;
        - la presentazione da parte dei dipendenti al proprio Responsabile, di un "rapporto di spesa" riepilogativo delle spese sostenute durante la trasferta con allegati i relativi giustificativi;
        - le tipologie ed i limiti delle spese rimborsabili e le modalità di effettuazione, rendicontazione, verifica, autorizzazione, registrazione e rimborso delle stesse;
        - il sostenimento delle spese di trasferta mediante utilizzo di eventuali carte di credito aziendale/carta carburante e rendicontazione delle stesse;

- la definizione, formalizzazione ed attuazione di un sistema di valutazione delle performance del personale, con il supporto di appositi strumenti informatici;
- la definizione, approvazione ed erogazione di eventuali provvedimenti di politica retributiva (es. *"bonus ad personam"*, incrementi di stipendi), sulla base del processo di valutazione delle performance del personale dipendente di cui al punto precedente e conformemente ai limiti di budget prefissati, con il coinvolgimento delle competenti funzioni del Gruppo;
- il rispetto del principio che prevede che la determinazione degli obiettivi aziendali ed i relativi programmi di incentivazione deve essere condotta 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;
- laddove necessario, la definizione di uno scadenziario circa il mantenimento della regolarità del permesso di soggiorno nel tempo per il personale extracomunitario assunto a tempo indeterminato/determinato;
- l'assegnazione di eventuali asset aziendali (ad esempio autovetture, sim, telefoni, tablet), mediante l'utilizzo di apposite/i comunicazioni/moduli standard per loro presa in consegna, sottoscritti per accettazione, e contenenti anche l'impegno al corretto utilizzo nel rispetto delle disposizioni del Gruppo, della Società e della legislazione vigente, prevedendo, per i neo-assunti, l'inserimento di tali clausole nel relativo contratto di assunzione;
- l'archiviazione in formato cartaceo/informatico, mediante creazione di apposito fascicolo per ogni dipendente, dei dati/documenti/atti predisposti nel corso del rapporto di lavoro (es. progressioni di carriera, assegnazione di bonus, permessi di soggiorno).

3.4. APPROVVIGIONAMENTO DI BENI E SERVIZI E CONSULENZE

3.4.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

L'attività di approvvigionamento di beni, servizi e consulenze può comportare, in via teorica, il rischio di commissione dei reati di:

- ricettazione (art. 648 c.p.), nell'ipotesi ad esempio di acquisto di beni provenienti da un qualsiasi delitto, ovvero nel caso di utilizzazione da parte del fornitore di risorse di provenienza illecita (ad esempio impianti e macchinari per lo svolgimento della propria attività);
- terrorismo ed eversione dell'ordine democratico (art. 25-quater D.Lgs. 231/01) nel caso in cui si forniscano, direttamente o indirettamente, ma comunque volontariamente, fondi a favore di soggetti che intendono porre in essere reati di terrorismo, attraverso la selezione e/o gestione di fornitori / subappaltatori;
- omicidio colposo (art. 589 c.p.) e lesioni personali colpose (art. 590, comma 3, c.p.), reati ambientali (art. 25-undecies D.Lgs. 231/01), reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies D.Lgs. 231/01), delitti contro la personalità individuale (art. 25-quinquies D.Lgs. 231/01) nell'ipotesi in cui gli stessi siano commessi dai fornitori/appaltatori all'interno di aree aziendali e/o comunque sotto il controllo della Società;
- associazione per delinquere (art. 416 c.p.) di tipo mafioso anche straniera (art. 416-bis c.p.), nel caso in cui la Società si rivolga a fornitori / appaltatori ad esse riconducibili;
- corruzione tra privati (art. 2635 comma 3 c.c.) e istigazione alla corruzione tra privati (art. 2635-bis comma 1 c.c.), nel caso in cui la Società dia, offra o prometta, anche per interposta persona, un compenso o altra utilità, ad un commerciale di un fornitore per ottenere un indebito beneficio/utilità non dovuto/a (es. sconto fuori mercato) o al tecnico del fornitore per evitare che evidenzi delle problematiche riscontrate nello svolgimento delle sue attività;
- indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 ter c.p.), nell'ipotesi in cui un soggetto apicale o sottoposto della Società effettui pagamenti per l'acquisizione di beni e servizi mediante carta di pagamento a lui non intestata o altro strumento diverso dal contante, e, quindi, mediante utilizzo indebito, per ottenere da quell'operazione un vantaggio per la Società;
- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 25-quinquiesdecies D.Lgs. 231/01 - art. 2 co. 1 e 2-bis D.Lgs. 74/00), dichiarazione fraudolenta mediante altri artifici (art. 25-quinquiesdecies D.Lgs. 231/01 - art. 3 D.Lgs. 74/00). Tali reati potrebbero, infatti, essere commessi in via astratta nel caso in cui la Società, allo scopo di evadere le imposte, utilizzi fatture passive fittizie che alterano i valori della dichiarazione annuale ovvero impieghi ad esempio mezzi fraudolenti atti ad ostacolare l'accertamento dell'amministrazione finanziaria;
- autoriciclaggio (art. 648-ter.1 c.p.), nel caso in cui la Società, a seguito della commissione o del concorso in commissione di uno dei reati sopra indicati, nonché di altri delitti di cui al D.Lgs. 231/01, ottiene delle utilità che impiega, sostituisce o trasferisce, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Il processo di approvvigionamento di beni, servizi e consulenze potrebbe in via astratta essere inoltre lo strumento attraverso il quale vengono realizzati i reati:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti Internazionali o degli organi delle Comunità Europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.);
- traffico di influenze illecite (art. 25 D.Lgs. 231/2001 - art. 346-bis c.p.);
- di induzione indebita a dare o promettere utilità (art. 319-quater c.p.);

- concussione (art. 317 c.p.);
- di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.).

Tali reati potrebbero, infatti, essere commessi in via astratta attraverso la gestione poco trasparente del processo di selezione del fornitore. Pertanto l'emissione di ordini di acquisto può risultare strumentale alla creazione di fondi utilizzabili a fini corruttivi nei confronti di pubblici ufficiali/incaricati di pubblico servizio o di privati ad esempio:

- nel caso dell'attribuzione o promessa di un fittizio contratto a favore di un pubblico ufficiale o di un privato (o di familiari o persone o società agli stessi riconducibili o graditi) al fine di ricompensarli per gli indebiti favori o per ottenere un indebito vantaggio;
- tramite la creazione di fondi a seguito di servizi contrattualizzati a prezzi superiori a quelli di mercato, da dare o promettere al pubblico ufficiale o al privato, per ottenere favori nell'ambito delle attività aziendali.

3.4.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

Di seguito si evidenziano gli Enti aziendali coinvolti nella gestione dell'attività a rischio Approvvigionamento di beni, servizi e consulenze (Responsabile attività DI - Supply Chain - Procurement – Funzioni coinvolte Country Leader, Sales Finance, Sales Team, Sales Operation, Global Services Operations, Professional Services, Global Delivery, Customer Support, Sales Finance, Order Management, Legal Business Partner, Marketing & Communication).

3.4.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Le attività connesse con la presente area a rischio devono essere gestite nel rispetto delle procedure aziendali/di Gruppo che, oltre a inglobare i principi espressi nel Codice Etico e di Condotta, prevedono:

- la definizione delle principali attività nonché dei ruoli e delle responsabilità delle Funzioni/Aree coinvolte, garantendo in ogni fase una separazione delle mansioni/ruoli. Più in particolare si riportano di seguito gli elementi cardine:
  - per quel che riguarda la fase di *richiesta di acquisto*, si prevede:
    - un'adeguata formalizzazione, attraverso l'utilizzo dei sistemi informativi aziendali;
    - una adeguata verifica di congruità della spesa rispetto al budget;
  - in fase di *selezione e scelta delle offerte di fornitura*:
    - la verifica, in via preventiva, delle informazioni disponibili (incluse informazioni finanziarie) su controparti fornitori, partner e consulenti, per appurare la loro rispettabilità e la legittimità della loro attività, prima di instaurare con questi rapporti d'affari;
    - il rispetto del principio che la selezione dei fornitori di beni, prestazioni e servizi deve avvenire sulla base di criteri di valutazione oggettivi, trasparenti e documentabili, in conformità ai principi del Codice Etico e di Condotta;
  - in fase di *definizione dell'ordine/contratto* deve essere previsto:
    - la definizione di condizioni economiche coerenti con la tipologia di fornitura richiesta;
    - la sottoscrizione dell'ordine/contratto di fornitura da parte di soggetto dotato di idonea procura in tal senso;
  - la fase di *ricezione, controllo e valutazione della fornitura e di autorizzazione al pagamento* deve prevedere che:

- la ricezione, per quanto possibile, dei beni sia effettuata da soggetto (richiedente della fornitura) diverso da chi gestisce la fase di offerta e negoziazione con il fornitore e da chi effettua il pagamento della fornitura/ prestazione;
- eventuali criticità o difficoltà di qualsiasi genere nell'esecuzione dei rapporti contrattuali, ivi inclusi eventuali inadempimenti o adempimenti parziali di obbligazioni contrattuali, siano 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;
- l'attività prestata dal fornitore/consulente sia debitamente documentata e la Funzione che si è avvalso/a della loro opera deve, prima della liquidazione dei relativi onorari, attesti l'effettività della prestazione;
- i flussi finanziari in uscita siano autorizzati in base alle procure della Società e gestiti in base all'iter definito;
- debba essere monitorato il permanere in capo ai fornitori dei requisiti di affidabilità, correttezza, professionalità e onorabilità;

- l'inserimento dei fornitori in un "Elenco Fornitori Qualificati", previo superamento di un periodo di prova, il cui esito deve essere formalizzato;
- la predisposizione delle condizioni generali di fornitura standard, nell'ambito delle quali sia prevista tra l'altro la clausola secondo cui, qualsiasi violazione commessa dal fornitore (ed accertata da parte della Società e/o dalle autorità competenti), con riferimento al D.Lgs. 231/01 o del Code of Ethics and Business Conduct, comporterà la possibilità di risoluzione del contratto, nonché di rivalersi in sede legale con i soggetti che hanno compiuto tale violazione;
- adeguate modalità di conservazione della documentazione rilevante, così da garantire la tracciabilità delle operazioni svolte.

3.5. AFFARI SOCIETARI

3.5.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Il processo di gestione degli affari societari è potenzialmente esposto al rischio di commissione (o di concorso in commissione) dei seguenti reati:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti Internazionali o degli organi delle Comunità Europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.), nonché di induzione indebita a dare o promettere utilità (art. 319-quater c.p.) e induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.), in considerazione del fatto che gestire gli affari societari comporta sistematici contatti ed adempimenti verso i funzionari della PA (a mero titolo esemplificativo e non esaustivo: es. Notai, Camera di Commercio, Tribunali, Uffici del Registro, etc.). A tal fine, il contatto con i funzionari pubblici potrebbe rappresentare un'occasione per offrire denaro o altra utilità agli stessi per ottenere un trattamento di favore, ad es. inducendoli ad omettere/attenuare l'irrogazione di sanzioni da comminarsi a seguito di irregolarità emerse in occasione di controlli (per l'analisi dell'area a rischio relativa ai rapporti con la PA, si rimanda al paragrafo 3.11 della presente Parte Speciale);
- illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.) e operazioni in pregiudizio dei creditori (art. 2629 c.c.); ciò alla luce del fatto che l'attività degli organi sociali può portare a delibere consiliari/assembleari connesse con operazioni sul capitale (quali ad es. l'acquisto o la sottoscrizione, fuori dei casi consentiti dalla legge, di azioni o quote sociali, la riduzioni del capitale sociale o la fusione con altra società o scissioni, o una scissione in violazione degli art. 2306, 2445 e 2503 c.c.) che, in via potenziale, possono ledere l'integrità del capitale sociale e le ragioni dei creditori;
- 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. Tale fattispecie, potrebbe concretizzarsi nell'impiego di quote non collocate, nell'esercizio sotto altro nome del diritto di voto, oppure nell'uso di altri mezzi illeciti;
- false comunicazioni sociali (art. 2621 c.c.), fatti di lieve entità (art. 2621-bis c.c.), impedito controllo (art. 2625 c.c.), indebita restituzione di conferimenti (art. 2626 c.c.), illegale ripartizione degli utili e delle riserve (art. 2627 c.c.), formazione fittizia del capitale (art. 2632 c.c.), indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.). Tra le modalità di realizzazione si segnala ad esempio l'occultamento in tutto o in parte con mezzi fraudolenti di informazioni/fatti che avrebbero dovuto essere comunicati all'Organo di Controllo riguardo la situazione economica, patrimoniale o finanziaria della Società o la falsificazione/omissione delle comunicazioni/adempimenti nei confronti dello stesso.

3.5.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

Di seguito si evidenziano gli Enti aziendali coinvolti nella gestione dell'attività a rischio Gestione degli affari societari (Responsabile attività Legal Business Partner – Funzioni coinvolte Country Leader, Legal Business Partner, Sales Finance).

3.5.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Oltre ai principi espressi nel Codice Etico e di Condotta, la Società prevede che:

- è richiesto ai Destinatari di 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;

- è fatto divieto di 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;
- è richiesto ai Destinatari di garantire il puntuale rispetto delle norme di legge che tutelano l'integrità e l'effettività del capitale sociale, per non creare nocumento alle garanzie dei creditori e, più in generale, ai terzi;
- le attività connesse con la presente area a rischio devono essere gestite secondo modalità operative che garantiscono la segregazione delle mansioni e una adeguata tracciabilità delle operazioni;
- 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, che possano potenzialmente ledere l'integrità del capitale sociale debbono essere ispirate ai seguenti principi:
  - trasparenza, correttezza e rispetto della normativa;
  - l'attribuzione al CdA della preventiva approvazione di operazioni societarie che possano comportare significativi impatti sotto il profilo economico, patrimoniale e finanziario;
  - l'assegnazione di responsabilità decisionali ed operative per le operazioni anzidette, nonché i meccanismi di coordinamento tra le diverse Funzioni/Aree aziendali coinvolte.

Con riferimento ai rapporti con l'Organo di controllo, la Società prevede:

- la tempestiva trasmissione allo stesso di tutti i documenti relativi ad argomenti posti all'ordine del giorno di Assemblee e CdA o sui quali il Sindaco debba esprimere un parere;
- la messa a disposizione dei documenti sulla gestione della Società per consentire allo stesso lo svolgimento delle attività di verifica;
- la previsione di riunioni periodiche tra Organo di Controllo e OdV per verificare l'osservanza delle regole e procedure aziendali in tema di normativa societaria;
- le modalità di archiviazione e conservazione della documentazione prodotta.

3.6. AMMINISTRAZIONE, FINANZA E CONTROLLO

3.6.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Le attività connesse alla redazione del budget, alla tenuta della contabilità, alla predisposizione del bilancio e alla gestione della fiscalità presentano i seguenti potenziali profili di rischio:

- una non corretta gestione delle stesse, impattando sulla rappresentazione della situazione patrimoniale, economica e finanziaria della Società, potrebbe costituire uno dei presupposti per la commissione o il concorso in commissione dei reati di false comunicazioni sociali (art. 2621), fatti di lieve entità (art. 2621-bis c.c.), operazioni in pregiudizio dei creditori (art. 2629 c.c.) e della formazione fittizia del capitale (art. 2632 c.c.). Tali fattispecie si realizzano con l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali rilevanti che non siano veritieri e possano indurre in errore i destinatari circa la situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, con l'intenzione di ingannare i soci, i creditori o il pubblico; ovvero l'omissione, con la stessa intenzione, di informazioni rilevanti sulla situazione medesima la cui comunicazione è imposta dalla legge. Pertanto tali reati potrebbero, in via astratta, verificarsi ad esempio attraverso:
  - l'esposizione di fatti materiali non corrispondenti al vero;
  - la sopravvalutazione o sottovalutazione delle poste estimative/valutative di bilancio;
  - la valutazione che si discosti, consapevolmente, dai criteri di stima normativamente fissati in modo concretamente idoneo ad indurre in errore i destinatari delle comunicazioni;
  - la modifica dei dati contabili presenti sul sistema informatico;
  - l'omissione di informazioni la cui comunicazione è imposta dalla legge, circa la situazione economica, patrimoniale o finanziaria della società o del gruppo cui essa appartiene, anche qualora le informazioni riguardino beni posseduti o amministrati dalla società per conto terzi, ecc.;
- truffa (art. 640, comma 2, n.1, c.p.). Tale reato potrebbe essere commesso attraverso la predisposizione di documentazione non veritiera nella predisposizione di dichiarazioni fiscali, ad esempio attraverso l'indicazione di aspetti non veritieri o non esistenti;
- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 25-quinquiesdecies D.Lgs. 231/01 - art. 2 co. 1 e 2-bis D.lgs. 74/2000). Tale reato potrebbe configurarsi qualora allo scopo di evadere le imposte, la Società indichi nella dichiarazione relativa alle imposte sui redditi o sul valore aggiunto elementi passivi fittizi. Nella dichiarazione annuale vengono indicati elementi passivi fittizi o attivi inferiori a quelli reali grazie ai documenti registrati;
- dichiarazione fraudolenta mediante altri artifici (art. 25-quinquiesdecies D.Lgs. 231/01 - art. 3 D.lgs. 74/00). Tale reato potrebbe configurarsi qualora la Società al fine di evadere le imposte e con la coscienza e volontà del superamento delle soglie di punibilità ex-lege pone in essere una falsa rappresentazione nelle scritture contabili obbligatorie oppure impiega mezzi fraudolenti atti ad ostacolare l'accertamento da parte dell'amministrazione finanziaria oppure presenta una dichiarazione non veritiera;
- emissione di fatture o altri documenti per operazioni inesistenti (art. 25-quinquiesdecies D.Lgs. 231/01 - art. 8 co. 1 e 2-bis d.lgs. 74/00). Tale reato potrebbe essere commesso qualora, al fine di consentire ad un terzo l'evasione delle imposte sui redditi o sul valore aggiunto, emetta fatture o altri documenti per operazioni mai rese, a fronte del riconoscimento da parte del terzo di un vantaggio economico per la Società quale, ad esempio, l'approvazione di una variante d'ordine da parte del Cliente;
- occultamento o distruzione di documenti contabili (art. 25 quinquiesdecies D.Lgs. 231/01 – art. 10 D.lgs 74/00) Tale reato potrebbe configurarsi qualora la Società proceda all'occultamento o alla distruzione delle scritture contabili o dei documenti di cui è obbligatoria la conservazione, per rendere impossibile la ricostruzione dei redditi e del volume degli affari della Società;

- sottrazione fraudolenta al pagamento delle imposte (art. 25 quinquiesdecies D.Lgs. 231/01 – art. 11 D.lgs 74/00). Tale reato potrebbe configurarsi qualora la Società compia simultaneamente atti fraudolenti su beni propri allo scopo di rendere inefficace, per sé o per altri, anche parzialmente, la procedura di riscossione coattiva, oppure indichi nella documentazione presentata ai fini della procedura di transazione fiscale, elementi attivi o passivi diversi da quelli reali per ottenere un pagamento inferiore delle somme complessivamente dovute;
- dichiarazione infedele (art. 25 quinquiesdecies D.Lgs. 231/01 – art. 4 D.lgs 74/00). Tale reato si potrebbe configurare nel caso in cui, al fine di evadere l'imposta sul valore aggiunto nel sistema transfrontaliero per un importo complessivo non inferiore a 10 milioni, nella dichiarazione annuale relativa alla citata imposta, indica elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti;
- omessa dichiarazione (art. 25 quinquiesdecies D.Lgs. 231/01 – art. 5 D.lgs 74/00). Tale reato si potrebbe configurare nel caso in cui, al fine di evadere l'imposta sul valore aggiunto nel sistema transfrontaliero per un importo complessivo non inferiore a 10 milioni, la Società non presenta, pur essendovi obbligata, la dichiarazione annuale relativa alla citata imposta;
- indebita compensazione (art. 25 quinquiesdecies D.Lgs. 231/01 – art. 10-quater D.lgs 74/00). Tale reato potrebbe realizzarsi nel caso in cui, al fine di evadere l'imposta sul valore aggiunto nel sistema transfrontaliero per un importo complessivo non inferiore a 10 milioni, la Società utilizzi in compensazione crediti inesistenti e/o non spettanti.

Infine le attività della presente area a rischio possono astrattamente configurare condotte riconducibili alla ricettazione (art. 648 c.p.), al riciclaggio (art. 648-bis c.p.), all'impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.), nonché all'autoriciclaggio (art. 648-ter.1 c.p.). Ad esempio la Società potrebbe incorrere in quest'ultimo reato se a seguito della commissione o del concorso in commissione di un delitto (tra quelli previsti dal D.Lgs. 231/01), ottiene delle utilità che impiega, sostituisce o trasferisce, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Il processo di approvvigionamento di beni, servizi e consulenze potrebbe in via astratta essere, inoltre, lo strumento attraverso il quale vengono realizzati i reati:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti Internazionali o degli organi delle Comunità Europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.);
- traffico di influenze illecite (art. 25 D.Lgs. 231/2001 - art. 346-bis c.p.);
- di induzione indebita a dare o promettere utilità (art. 319-quater c.p.);
- concussione (art. 317 c.p.);
- di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.);
- di corruzione tra privati (art. 2635 comma 3 c.c.) e istigazione alla corruzione tra privati (art. 2635-bis comma 1 c.c.).

Ciò in quanto tale processo può essere strumentale alla costituzione di fondi occulti utilizzabili per fini corruttivi, ad esempio attraverso:

- la contabilizzazione di poste fittizie (es. fatture false per prestazioni inesistenti);
- l'omessa contabilizzazione di poste;
- la sopravvalutazione di beni della Società.

3.6.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

Di seguito si evidenziano le principali attività da considerare astrattamente a rischio e gli Enti aziendali coinvolti nella loro gestione:

- Predisposizione del budget e analisi periodica degli scostamenti (Responsabile attività Country Leader e Finance EMEA – Funzioni coinvolte Sales Finance, Sales Operations);
- Ricezione, verifica e registrazione delle fatture dei fornitori (Società Gruppo Hitachi - Finance EMEA – Funzioni coinvolte Country Leader, Order Management, Sales Finance);
- Emissione delle fatture attive (Finance EMEA - Funzioni coinvolte Country Leader, Sales Finance);
- Effettuazione delle scritture contabili (Finance EMEA - Funzioni coinvolte Country Leader, Sales Finance, Legal Business Partner);
- Predisposizione bilancio e delle dichiarazioni fiscali (Responsabile attività Finance EMEA - Funzioni coinvolte Country Leader).

3.6.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Le attività connesse con la presente area a rischio devono essere gestite, oltre che in conformità ai principi contenuti nel Codice Etico e di Condotta, nel rispetto delle procedure aziendali/di Gruppo che prevedono:

- con riferimento alla formazione del reporting, la redazione periodica del "forecast" di costi e di un budget delle vendite al fine di garantire il monitoraggio dell'andamento aziendale;
- con riferimento alla tenuta della contabilità, alla predisposizione ed approvazione del Bilancio e delle altre comunicazioni sociali aventi carattere amministrativo contabile e alla gestione della fiscalità:
  - lo svolgimento di attività di verifica e di controllo sulla correttezza delle fatture emesse (es. corretta applicazione dell'IVA, della ritenuta di acconto) prima della loro approvazione;
  - l'emissione delle fatture attive:
    - in modalità manuale, previo accertamento dell'esito positivo del collaudo o del rilascio dell'attestazione di prestazione del servizio da parte del Cliente;
    - in modalità automatica da parte del sistema informativo, al momento della chiusura dell'ordine a sistema;
  - la predisposizione di chiusure contabili periodiche;
  - l'elencazione dei dati e delle notizie che ciascuna Funzione aziendale deve fornire alla Funzione responsabile, nonché dei criteri per la loro elaborazione e la tempistica di consegna;
  - la trasmissione dei dati ed informazioni alla Funzione responsabile per via informatica, così da tracciare i vari passaggi e identificare i soggetti che inseriscono i dati nel sistema;
  - la tracciabilità delle operazioni contabili, di predisposizione del bilancio, con particolare riferimento a quelle relative alle scritture di accertamento e assestamento ovvero quelle che comportino la necessità di effettuare delle stime;
  - la tempestiva trasmissione a tutti i membri del CdA e all'Organo di Controllo della bozza di bilancio, nonché un'idonea registrazione di tale trasmissione;
  - lo svolgimento di riunioni almeno annuali congiunte tra il Country Leader, l'Organo di Controllo e l'OdV;

- adeguate modalità di archiviazione e conservazione della documentazione amministrativa / contabile nel rispetto della normativa civilistica e fiscale, in modo da assicurarne una immediata rintracciabilità.

3.7. RISORSE FINANZIARIE

3.7.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

La gestione delle risorse finanziarie può comportare, in via teorica, il rischio di commissione dei reati di:

- ricettazione (art. 648 c.p.), riciclaggio (art. 648-bis c.p.), impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.) e autoriciclaggio (art. 648-ter1 c.p.) attraverso la movimentazione dei flussi finanziari connessi alle attività di acquisto e alle attività inerenti la vendita di prodotti/l'erogazione dei servizi (si rimanda a tali attività per gli approfondimenti sul profilo di rischio specifico);
- associazione per delinquere ed associazione di tipo mafioso anche straniere (artt. 416 e 416-bis c.p.), nel caso in cui, ad esempio, la Società procacci in maniera consapevole risorse finanziarie da destinare a soggetti riconducibili a tali tipologie di associazioni;
- corruzione tra privati (art. 2635 comma 3 c.c.) e istigazione alla corruzione tra privati (art. 2635-bis comma 1 c.c.), nel caso in cui ad esempio un referente della Società dia/prometta/offra un compenso non dovuto (ad es. denaro o altra utilità):
  - alla compagnia assicurativa, per ottenere condizioni migliori e/o il rilascio di una garanzia che non sarebbe stata data;
  - al funzionario di banca, per ottenere un vantaggio da un istituto di credito (es. migliori condizioni di finanziamento, mancata revoca di un fido a fronte del non rispetto di covenant stabiliti nelle condizioni per avere il fido).

  Si precisa che nello svolgimento di alcune attività (quali, ad esempio, la gestione dei crediti agevolati), gli istituti di credito sono di fatto e di diritto equiparati alla Pubblica Amministrazione: in questo caso non sussisterebbe i reati di corruzione tra privati/istigazione alla corruzione tra privati, ma quelli di corruzione/istigazione previsti nell'ambito dei delitti verso la Pubblica Amministrazione;
- indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 ter c.p.), nell'ipotesi in cui un soggetto apicale o sottoposto di HVI effettui un pagamento o anche prelievo mediante carta di pagamento a lui non intestata o altro strumento diverso dal contante (con specifico riferimento all'accesso ai dati e alle credenziali di soggetti terzi – esterni e interni - funzionali all'utilizzo di strumenti di pagamento diversi dal contante), e quindi mediante utilizzo indebito, per ottenere da quell'operazione un vantaggio illecito per la Società. Il reato potrebbe, inoltre, realizzarsi nell'ipotesi in cui un soggetto apicale o sottoposto di HVI si appropri indebitamente delle credenziali e dei dati identificativi e bancari di un cliente (ad es. carta di identità, IBAN, C.F.) per aprire un sistema di pagamento attraverso il quale riceva pagamenti a favore della Società stessa o mediante il quale effettui indebitamente pagamenti a favore di terzi (fornitori, consulenti, ecc.);
- trasferimento fraudolento di valori (art. 512-bis c.p.) che potrebbe configurarsi qualora un esponente di HVI, effettui intestazioni/trasferimenti fittizi di beni e/o valori finalizzati a evitare il sequestro/confisca degli stessi ovvero commettere reati di riciclaggio, autoriciclaggio.

La gestione dei flussi finanziari costituisce una delle modalità strumentali attraverso cui, in linea di principio, potrebbero essere commessi i reati:

- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti Internazionali o degli organi delle Comunità Europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.);
- induzione a dare o promettere utilità (art. 319-quater c.p.);

- traffico di influenze illecite (art. 346-bis c.p.);
- truffa (art. 640, comma 2, n.1, c.p.).

Tali reati potrebbero, infatti, essere commessi in via astratta attraverso una gestione poco trasparente e corretta dei flussi monetari e finanziari, che potrebbe portare alla costituzione di "disponibilità" funzionali alla realizzazione di condotte illecite tra cui, tipicamente, quelle corruttive ad esempio attraverso:

- l'utilizzo improprio dei conti correnti societari al fine di rendere disponibili somme di denaro o per rendere non agevole la tracciabilità delle movimentazioni di fondi;
- l'effettuazione dei pagamenti di fatture fittizie al fine di creare delle "disponibilità";
- il riconoscimento di rimborsi spese o anticipi fittizi in tutto o in parte;
- l'utilizzo delle somme della cassa al fine di creare delle "disponibilità";
- la costituzione di fondi a fronte di fatture false, in tutto o in parte.

3.7.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

Di seguito si evidenziano le principali attività da considerare astrattamente a rischio e gli Enti aziendali coinvolti nella loro gestione:

- Gestione dei pagamenti e degli incassi (Responsabile attività Finance EMEA – Funzioni coinvolte Country Leader, Sales Finance);
- Gestione dei rapporti con gli istituti di credito e assicurazioni (Responsabile attività Finance EMEA – Funzioni coinvolte Country Leader, Sales Finance).

3.7.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Oltre ai principi espressi nel Codice Etico e di Condotta, la Società prevede in generale che:

- ogni atto di natura finanziaria della Società deve essere previamente autorizzato dagli uffici competenti, garantendo la sua rispondenza all'interesse della stessa, la congruità del costo, l'effettiva e completa destinazione delle somme erogate e deve essere disposto secondo i poteri aziendali conferiti;
- 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 della Società, garantendo pertanto la possibilità di risalire al soggetto che ha disposto l'operazione;
- 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);
- sono vietati pagamenti indirizzati a conti cifrati o a conti per i quali non si è in grado di individuare con precisione le generalità dell'intestatario;
- è vietato avere rapporti con soggetti aventi sede o comunque operanti in Paesi che non garantiscono la trasparenza societaria;
- è vietato compiere operazioni tali da impedire la ricostruzione del flusso finanziario o da renderlo meno agevole quali, ad esempio, pagamenti/versamenti frazionati effettuati a tale scopo.

Inoltre è previsto/a:

- con riferimento ai pagamenti delle fatture passive, l'obbligo di:
  - svolgere, prima dell'esecuzione dei pagamenti, un'attività di controllo e valutazione della fornitura/prestazioni a cura della Funzione richiedente;

  - verificare la rispondenza tra quanto autorizzato e i relativi documenti di riferimento (contratto/ordine di acquisto, cedolini, F24, Nota Spese, ecc.);
- con riferimento alla gestione deli incassi e alla politica di recupero crediti:
  - la concessione di linee di credito ai Clienti, in base a criteri definiti, debitamente formalizzate ed autorizzate da persone a ciò delegate;
  - la definizione di modalità operative, flussi informativi, strumenti e responsabilità relativamente al monitoraggio del credito scaduto ed al sollecito del Cliente, garantendo un'adeguata segregazione e tracciabilità delle attività;
- che la decisione di apertura dei conti corrente spetti all'Headquarter, tenendo conto anche delle necessità ed esigenze rilevate delle singole Società locali;
- la definizione di adeguate modalità di archiviazione e conservazione della documentazione prodotta, in modo da assicurarne la tracciabilità.

3.8. SISTEMI INFORMATIVI

3.8.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

La gestione dei sistemi informativi può in via astratta comportare la commissione dei reati:

- di frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter, comma 1, c.p.);
- di delitti informatici e trattamento illecito di dati (art. 24-bis D.Lgs. 231/01), di seguito riportati:
  - falsità in un documento informatico pubblico avente efficacia probatoria (491-bis c.p.);
  - accesso abusivo ad un sistema informatico o telematico (615-ter c.p.);
  - detenzione, diffusione e installazione abusiva di apparecchiature, codici o altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.);
  - 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.);
  - intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
  - detenzione, diffusione e installazione abusiva di apparecchiature e altri mezzi atti a intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);
  - danneggiamento di informazioni, dati e programmi informatici (635-bis c.p.);
  - danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (635-ter c. p.);
  - danneggiamento di sistemi informatici o telematici (635-quater c.p.);
  - danneggiamento di sistemi informatici o telematici di pubblica utilità (635-quinquies c.p.);
- di detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (493 quater c.p.) e di frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (640 ter comma 2 c.p.) rispettivamente nell'ipotesi in cui:
  - un soggetto apicale o sottoposto di HVI detenga indebitamente programmi informatici o software appositamente funzionali ad effettuare illecite operazioni di trasferimento di fondi, con l'intento di procurare un vantaggio economico alla Società;
  - un soggetto apicale o sottoposto di HVI servendosi di un codice di accesso a lui non attribuito ovvero di risorse ICT a lui non assegnate, penetri abusivamente nel sistema informatico bancario (es. home banking) ed effettui illecite operazioni di trasferimento di fondi al fine di occultarne la provenienza illecita e procurare un vantaggio alla Società
- alcuni di quelli contemplati dall'art. 25-novies (delitti in materia di violazione del diritto d'autore), tra cui quelli di seguito riportati:
  - abusiva messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa;
  - abusiva duplicazione, per trarne profitto, di programmi per elaboratore;
  - importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE;
  - predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori;

- riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati.

Il processo di gestione dei sistemi informativi costituisce, in linea di principio, uno strumento attraverso il quale possono essere commessi alcuni tra i reati delle fattispecie previste dal D.Lgs. 231/01, tra i quali si segnalano i reati di:

- false comunicazioni sociali (art. 2621 c.c.) e fatti di lieve entità (art. 2621-bis c.c.);
- impedito controllo (art. 2625 c.c.);
- truffa (art. 640, comma 2 n. 1, c.p.);
- traffico di influenze illecite (art. 346-bis c.p.);
- corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), induzione indebita a dare o promettere utilità (art. 319-quater c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti Internazionali o degli organi delle Comunità Europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.) e di induzione indebita a dare o promettere utilità (art. 319-quater c.p.);
- di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.);
- di corruzione tra privati (art. 2635 comma 1 c.c.) e istigazione alla corruzione tra privati (art. 2635-bis comma 3 c.c.).

I reati sopra elencati potrebbero essere commessi ad esempio attraverso la gestione anomala:

- della sicurezza dei sistemi, che potrebbe consentire di accedere, alterare e/o cancellare dati ed informazioni destinate alla Pubblica Amministrazione, a soggetti terzi portatori di interessi o, comunque, all'esterno;
- dei cambiamenti dei sistemi, che potrebbero consentire di effettuare modifiche non autorizzate a sistema e/o di danneggiare/cancellare informazioni, dati e programmi informatici;
- dei backup/restore, che potrebbero consentire l'accesso e/o la modifica non autorizzata a dati e la perdita di informazioni, dati e programmi informatici, impedendo od ostacolando lo svolgimento delle attività di controllo.

3.8.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

Di seguito si evidenzia che l'attività a rischio Gestione dei sistemi informativi è gestita dalla Capogruppo.

È opportuno evidenziare che i dipendenti di Hitachi Vantara Italia che utilizzano ordinariamente sistemi informatici hanno conseguentemente ampia possibilità di accesso a strumenti e dati informatici e telematici nel contesto dell'ordinaria attività lavorativa. Per tale motivo, stante la capillare diffusione presso la Società di sistemi e strumenti informatici, per quanto concerne i reati informatici ed il trattamento illecito dei dati contemplati dall'art. 24-bis, si ritiene di valutare diffuso e non localizzato il rischio della loro commissione, infatti questi potrebbero essere astrattamente realizzati in ciascuna attività sensibile in capo alle diverse Funzioni.

3.8.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Le attività connesse con la presente area a rischio devono essere gestite nel rispetto dei principi contenuti nel Codice Etico e di Condotta e delle procedure aziendali/di Gruppo, che definiscono i flussi informativi, gli strumenti e le responsabilità, relativamente a:

- la gestione dei rischi ICT, consentendo lo svolgimento di un'attività di valutazione dei rischi ICT e la preparazione dei Piani d'Azione per la loro gestione;
- la gestione della sicurezza ICT, con riferimento alle attività:
  - di backup di dati e programmi, prevedendo lo svolgimento di attività di ritenzione e definendo le cadenze elaborative dei salvataggi;
  - relative alla gestione della sicurezza, della protezione dei sistemi, dell'integrità e riservatezza dei dati.

  In particolare sono illustrati i seguenti aspetti:
  - le linee guida per l'attribuzione degli identificativi e dei diritti di accesso, nel rispetto delle necessità informative, del ruolo aziendale e secondo il principio della "Segregation of duties" (SOD), ad utenti, personale ICT e terzi, nell'ambito delle quali, tra l'altro, è prevista/o:
    - l'identificazione, autenticazione e abilitazione agli accessi alle applicazioni, all'infrastruttura ed alla rete mediante assegnazione a ciascuna risorsa (personale o soggetti terzi) di codici identificativi personali ("user" e "password"), e l'implementazione di opportuni meccanismi per lo scambio in sicurezza di informazioni tramite e-mail ed internet;
    - l'adozione, da parte di ciascuna risorsa, di adeguate misure volte ad assicurare la segretezza delle proprie credenziali di accesso, e il divieto di divulgarle o renderle note ad altri;
    - l'attribuzione di credenziali che non contengano riferimenti agevolmente riconducibili al soggetto interessato e la definizione della periodicità con la quale le credenziali devono essere rinnovate, anche in funzione della sensibilità dei dati trattati;
    - il dovere da parte di ciascuna risorsa di non lasciare incustodita o accessibile la propria postazione di lavoro informatica, al termine dell'orario lavorativo, durante le pause di lavoro, o durante riunioni lontane dalla propria postazione;
    - la richiesta e la concessione di privilegi di accesso ai diversi sistemi aziendali nel rispetto di un principio di (SOD) ed in funzione delle mansioni svolte, nonché il controllo periodico degli stessi con modifica e/o rimozione di quelli non più conformi all'evoluzione della situazione aziendale;
  - 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 e la previsione della rimozione di apparati e software irregolari e/o della loro regolarizzazione, per ripristinare la situazione di sicurezza dei sistemi;
  - appositi sistemi di protezione per l'utilizzo dei dispositivi sia all'interno dei locali aziendali, sia all'esterno (es. sistemi di criptazione e di salvataggio automatico dei dati per i PC; sistemi di criptazione ed utilizzo di apposite applicazioni per i cellulari);
- la gestione della domanda ICT, vale a dire la gestione delle richieste degli utenti (in particolare, dotazioni HW e SW, connessioni a internet, dotazione di e-mail, manutenzioni applicative/ infrastrutturali) e quindi la regolamentazione delle attività di richiesta, valutazione e autorizzazione, presa in carico, delivery e chiusura, con le relative responsabilità operative ed autorizzative;
- la gestione degli asset ICT, dalla fase della loro acquisizione a quella di dismissione, disciplinando anche le attività di assegnazione, riconsegna, dismissione con aggiornamento costante e riconciliazione periodica dell'inventario;
- la raccolta delle iniziative ICT, da intendersi come la raccolta dei fabbisogni ICT (applicativi, infrastrutturali), la loro valutazione ed approvazione nel rispetto del piano strategico/operativo ICT e del budget aziendale;

- la gestione delle modifiche applicative e infrastrutturali, e l'assegnazione di responsabilità operative/autorizzative nelle fasi della manutenzione ordinaria ed evolutiva (applicazioni ed infrastrutture), garantendo un'adeguata segregazione degli ambienti (sviluppo, collaudo, produzione);
- gli accessi ai locali CED. In particolare sono definiti i criteri e le modalità per il rilascio delle autorizzazioni per accedere a tali locali. Al riguardo è prevista:
  - l'assegnazione da parte della Corporate di badge aziendali abilitati in funzione del ruolo svolto presso la Società (con limitazione accessi, con accessi ad aree specifiche, ecc.);
  - diversi iter di autorizzazione degli accessi/assegnazione dei badge, a seconda degli utenti richiedenti (es. impiegato, visitatore, fornitore o stagista) e in funzione delle necessità;
- la gestione della sicurezza delle sedi, prevedendo:
  - un'attività di identificazione di aree potenzialmente critiche;
  - un sistema di videosorveglianza gestita direttamente e in modo univoco dalla Corporate;
  - l'attribuzione di badge con limitazione di fascia oraria per l'accesso dei fornitori che si occupano della manutenzione delle sedi (es. ditta di pulizie).

Inoltre la Società (per il tramite della struttura di gruppo competente) garantisce:

- la predisposizione e manutenzione del Piano di Disaster Recovery;
- un'attenta analisi volta a definire i profili di sistema, in particolare per quei sistemi che impattano il reporting finanziario o che contengono dati riservati, sensibili o particolarmente critici per la Società, definendo dei profili standard sulla base delle posizioni aziendali, nel rispetto delle incompatibilità della SOD;
- la formalizzazione delle nomine ad amministratore di sistema;
- la sottoscrizione da parte dei terzi a cui si dia accesso alla rete gestita dalla Società, di una dichiarazione nella quale si impegnano ad utilizzarla nel rispetto della legge e del Codice Etico e di Condotta;
- sistemi di blocco all'accesso ai siti internet non autorizzati;
- la regolamentazione dell'apertura e dell'uso della PEC, prevedendo in particolare la sottoscrizione da parte della/e risorsa/e che accede/accedono alla stessa e che non ha/hanno poteri di rappresentanza per la Società di una dichiarazione di impegno ed utilizzo secondo le indicazioni ricevute dal procuratore abilitato;
- una periodica attività di monitoraggio mediante:
  - la verifica aggregata dei log di sistema ed applicativi, in modo da individuare tempestivamente attività non conformi alle regole aziendali;
  - il controllo della rete per verificare l'esistenza di accessi e la trasmissione di dati non conformi alle regole aziendali;
  - la verifica degli account c.d. "*generici*" (utenze non nominali), per:
    - controllare che gli account siano univocamente assegnati e pertanto riconducibili sempre ad uno specifico utente;
    - provvedere alla modifica e/o rimozione di quelle non più conformi all'evoluzione della situazione aziendale;
- lo svolgimento di un'attività di formazione continua a distanza, a cura della Corporate nei confronti del personale, circa il corretto comportamento da tenere nell'utilizzo dei cellulari e di eventuali altri dispositivi aziendali, nonché interventi di sensibilizzazione mediante la tenuta di incontri informativi/formativi rivolti al personale.

Si evidenzia, inoltre, che:

- tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
- le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;
- la postazione di lavoro deve essere:
  - utilizzata solo per scopi legati alla propria attività lavorativa;
  - utilizzata in modo esclusivo da un solo utente;
  - protetta, evitando che terzi possano accedere ai dati senza essere autorizzati;
- è dovere del dipendente:
  - non utilizzare in Azienda risorse informatiche private (PC, periferiche, token, ecc.);
  - non installare alcun software sulle postazioni di lavoro o sui portatili/dispositivi aziendali;
  - non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate;
  - ;
- gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative. Sono vietati comportamenti che possano arrecare danno alla Società. In particolare, l'utente dovrà osservare le seguenti regole:
  - è consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate;
  - non è consentito scaricare software gratuiti (freeware o shareware) prelevati da siti Internet;
  - non è consentita la registrazione a siti internet o partecipare a Forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa;
  - è vietato aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali;
  - non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto in quanto tale atto assicura al mittente l'esistenza del destinatario;
  - è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione;
  - è consentito solo l'utilizzo dei programmi ufficialmente installati dai sistemi informativi di Corporate;
  - è vietato installare autonomamente programmi;
  - è vietato modificare le caratteristiche impostate sulle dotazioni od installare dispositivi di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, wi-fi ecc.), collegare alla rete aziendale qualsiasi apparecchiatura (ad es. switch, hub, apparati di memorizzazione di rete, ecc), effettuare collegamenti verso l'esterno di qualsiasi tipo (ad es. tramite modem) utilizzando un pc che sia contemporaneamente collegato alla rete aziendale;
- è posto l'obbligo, nei confronti di tutti coloro che hanno ricevuto apparecchiature/dispositivi informatici aziendali in dotazione, di segnalare tempestivamente alla Funzione competente ogni eventuale furto, danneggiamento, smarrimento, utilizzo o funzionamenti anomali delle/degli stesse/i;
- è posto il divieto di:
  - trasferire all'esterno della Società file elettronici e qualsiasi documentazione riservata di proprietà della Società;

- utilizzare password di altri utenti aziendali;
- utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- compiere operazioni personali, per conto proprio o per conto terzi anche per interposta persona, effettuate utilizzando informazioni riservate acquisite in ragione delle proprie funzioni, nonché il divieto di raccomandare o indurre altri a compiere operazioni utilizzando le predette informazioni;
- scaricare o condividere in rete materiale coperto da diritti d'autore senza la specifica approvazione del proprietario.

3.9. SALUTE E SICUREZZA SUL LAVORO

3.9.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Le attività relative alla implementazione e gestione di sistemi di sicurezza e tutela dell'igiene dei luoghi di lavoro presentano, oltre ad un profilo di rischio diretto per i reati di corruzione, traffico di influenze illecite, truffa e induzione indebita a dare o promettere utilità (per le modalità di commissione dei reati si rimanda al paragrafo 3.12 Rapporti con Istituzioni ed Enti Pubblici) e di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (per le modalità di commissione dei reati si rimanda al paragrafo 3.3. Acquisizione, progressione e gestione del personale), un profilo di rischio diretto in quanto potrebbero originare illeciti di cui alle fattispecie previste dal D.Lgs. 231/01 art. 25 septies, in materia di sicurezza sul lavoro vale a dire omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme, nel caso in cui si verificassero incidenti sul lavoro.

3.9.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

I Documenti di Valutazione dei Rischi ex D.Lgs. 81/08 riportano la valutazione di tutti i rischi per la sicurezza e la salute dei lavoratori presenti nei luoghi di lavoro e l'indicazione delle misure di prevenzione e di protezione attuate a seguito della valutazione.

Ferma restando l'individuazione e valutazione dei rischi di cui ai Documenti di Valutazione dei Rischi redatti ai sensi del D.Lgs. 81/08 e s.m.i., di seguito si esplicitano le principali attività individuate dalla Società come a potenziale rischio ai fini della commissione degli illeciti di cui alle fattispecie previste dal D.Lgs. 231/01 art. 25-septies unitamente alle Funzioni coinvolte:

- gestione delle deleghe di responsabilità e nomine/designazioni delle funzioni rilevanti per la sicurezza (a cura del Datore di Lavoro o suo Delegato nei limiti dei poteri conferiti);
- gestione della manutenzione degli impianti generali e delle infrastrutture nel rispetto degli standard tecnico strutturali e monitoraggio e controllo agenti fisici, chimici e biologici nei luoghi di lavoro (Regional Facilities Manager con la collaborazione dei Delegati del Datore di Lavoro, nei limiti dei poteri conferiti, e con il supporto del RSPP);
- valutazione dei rischi e predisposizione delle misure di prevenzione e protezione (Datore di Lavoro con la collaborazione del RSPP, RLS, Medico Competente);
- gestione delle emergenze e primo soccorso e delle relative prove periodiche (Datore di Lavoro o suo Delegato, nei limiti dei poteri conferiti, con la collaborazione del RSPP e della squadra di emergenza e primo soccorso);
- gestione dei contratti d'appalto, d'opera o di somministrazione e della sicurezza nei cantieri temporanei o mobili (Datore di Lavoro o suo Delegato, nei limiti dei poteri conferiti);
- gestione delle riunioni periodiche della sicurezza e consultazione dei RLS (Datore di Lavoro o suo Delegato, nei limiti dei poteri conferiti, con la collaborazione del RSPP, del RLS e del Medico Competente);
- gestione della formazione, informazione e addestramento in materia di Salute e Sicurezza sul lavoro (Datore di Lavoro con il supporto di Facilities EMEA e la collaborazione del RSPP);
- gestione della sorveglianza sanitaria e degli infortuni (Datore di Lavoro e Medico Competente con la collaborazione di Facilities EMEA);
- acquisizione di documentazione e certificazioni obbligatorie di legge (Datore di Lavoro o suo Delegato, nei limiti dei poteri conferiti, con la collaborazione delle diverse Funzioni/Aree della Società, ciascuno nell'ambito delle proprie responsabilità e competenze ed il supporto del RSPP);
- vigilanza e verifiche periodiche in merito al rispetto delle procedure e delle istruzioni di lavoro in sicurezza e all'efficacia delle procedure adottate (Datore di Lavoro Dirigenti e Preposti con la collaborazione del RSPP).

3.9.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Le attività connesse con il presente profilo di rischio devono essere gestite nel rispetto dei principi generali di comportamento espressi nel presente Modello, nel Codice Etico e di Condotta e nel rispetto delle procedure aziendali che prevedono quanto segue:

- *gestione delle deleghe di responsabilità e nomine/designazioni delle funzioni rilevanti per la sicurezza.* Per la gestione delle tematiche relative alla salute e sicurezza sul lavoro la Società ha definito un sistema di poteri e deleghe adeguati allo svolgimento delle attività sensibili e coerente con la struttura organizzativa della Società. In particolare:

  - le nomine e le designazioni dei soggetti responsabili in materia di sicurezza sono adeguatamente formalizzate e pubblicizzate all'interno della Società;
  - è garantita la verifica del possesso e del mantenimento dei requisiti di competenza e professionalità richiesti per le figure rilevanti per la sicurezza;
  - le risorse 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.

  Con particolare riferimento alla delega di funzioni da parte del Datore di Lavoro, come previsto dall'art. 16 del D.Lgs. 81/2008 e s.m.i., ove non espressamente esclusa è ammessa nel rispetto dei seguenti principi di elaborazione giurisprudenziale:

  - effettività - sussistenza e compresenza di autonomia decisionale e finanziaria del delegato;
  - idoneità tecnico professionale ed esperienza del delegato;
  - vigilanza sull'attività del delegato, non acquiescenza, non ingerenza;
  - certezza, specificità e consapevolezza;

- *Gestione della manutenzione degli impianti generali e delle infrastrutture nel rispetto degli standard tecnico strutturali e monitoraggio e controllo agenti fisici, chimici e biologici nei luoghi di lavoro.* Con riferimento a tale gestione è prevista:

  - l'individuazione e il rispetto degli standard tecnico-strutturali di legge riguardanti attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici applicabili;
  - la formalizzazione degli aspetti contrattuali che regolano l'occupazione dei locali aziendali garantendo la chiara ripartizione delle responsabilità in merito alla gestione della manutenzione ordinaria e straordinaria di strutture e impianti generali;
  - la pianificazione e gestione di interventi di manutenzione ordinaria e straordinaria, programmata e a guasto di dispositivi di sicurezza, attrezzature, macchine ed impianti;
  - la verifica e il controllo periodico di attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici nel rispetto della normativa applicabile attraverso organismi pubblici o privati abilitati.

  Sono inoltre previsti idonei flussi informativi tra il servizio SPP e le Funzioni coinvolte nel processo di approvvigionamento per assicurare la valutazione preliminare dei rischi che possono essere introdotti nella Società in fase di approvvigionamento;

- *Valutazione dei rischi e predisposizione delle misure di prevenzione e protezione*. Con riferimento a tale valutazione è prevista:

  - la valutazione dei rischi per la sicurezza e la salute dei lavoratori, ivi compresi il rischio incendio e quelli riguardanti gruppi di lavoratori esposti a rischi particolari, tra cui quelli collegati allo stress lavoro-correlato, quelli connessi all'utilizzo di auto aziendale o derivanti da attività svolte fuori sede, quelli riguardanti le lavoratrici in stato di gravidanza, nonché quelli connessi alle differenze di genere, all'età, alla provenienza da altri Paesi e quelli connessi alla specifica tipologia contrattuale attraverso cui viene resa la prestazione di lavoro. Tale valutazione dovrà essere effettuata secondo le modalità e i contenuti previsti dagli artt. 28 e 29 del D.Lgs. 81/08 e s.m.i.;

- l'aggiornamento periodico della valutazione dei rischi secondo le modalità previste dagli artt. 28 e 29 del D.Lgs. 81/08 e s.m.i.;
- la redazione, a seguito della valutazione di cui ai punti precedenti, dei Documenti di Valutazione dei Rischi (DVR) riportanti i contenuti di cui all'art. 28 c. 2 del D.Lgs. 81/08 e s.m.i. nel rispetto delle indicazioni previste dalle specifiche norme sulla valutazione dei rischi contenute nei successivi titoli del citato Decreto;

- *Gestione delle emergenze e primo soccorso e delle relative prove periodiche*. Con riferimento a tale aspetto è prevista:
  - la designazione e formazione di 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. Il numero di incaricati designati all'emergenza è definito in considerazione della struttura organizzativa e operativa della Società e delle possibili assenze degli incaricati per ferie/malattie/altro;
  - l'individuazione delle possibili emergenze e la pianificazione delle relative modalità di gestione, organizzando i necessari rapporti con i servizi pubblici competenti e formalizzando procedure affinché i lavoratori possano cessare la loro attività, o mettersi al sicuro, abbandonando il luogo di lavoro;
  - l'informazione dei lavoratori e del personale esterno circa le misure predisposte e i comportamenti da adottare in caso di emergenza;
  - la pianificazione e esecuzione, nel rispetto della periodicità prevista dalla normativa, di prove periodiche di emergenza ed evacuazione;
  - la disponibilità di adeguati presidi di primo soccorso e di mezzi di estinzione idonei alla classe di incendio ed al livello di rischio presenti sul luogo di lavoro, tenendo anche conto delle particolari condizioni in cui possono essere usati;
  - la presenza di planimetrie con l'indicazione delle vie di fuga e la localizzazione dei presìdi antincendio e di primo soccorso;
- *Gestione dei contratti d'appalto, d'opera o di somministrazione e della sicurezza nei cantieri temporanei o mobili*. Con riferimento a tale aspetto è prevista:
  - una gestione dei contratti d'appalto o d'opera o di somministrazione e dei relativi rischi di interferenza in conformità a quanto previsto dall'art 26 del D.Lgs. 81/08 e s.m.i. e dal titolo IV del citato decreto (cantieri temporanei o mobili), ove applicabile;
  - 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;
  - la comunicazione agli appaltatori delle procedure pertinenti e, se necessario, del nominativo del soggetto di riferimento per l'attività oggetto dell'appalto, nonché l'inserimento delle disposizioni disciplinari relative alla salute e sicurezza sul lavoro nel regolamento contrattuale fra le parti;
- *Gestione delle riunioni periodiche della sicurezza e consultazione dei Rappresentanti dei Lavoratori per la Sicurezza (RLS)*. Con riferimento a tale aspetto è prevista:
  - la consultazione del RLS in tutti i casi previsti dall'art 50 del D.Lgs. 81/08 lasciandone adeguata tracciabilità;
  - l'esecuzione, con periodicità almeno annuale, di una riunione cui partecipano il Datore di Lavoro o un suo rappresentante, il RSPP, il Medico Competente, i RLS. Nel corso della riunione, di cui si conserva adeguata tracciabilità, vengono trattati almeno i seguenti argomenti:
    - documento di valutazione dei rischi;

- andamento degli infortuni, delle malattie professionali e della sorveglianza sanitaria;
- criteri di scelta, caratteristiche tecniche ed efficacia dei dispositivi di protezione individuale;
- programmi di informazione e formazione in materia di salute e sicurezza salute sul lavoro.

- *Gestione della formazione, informazione e addestramento in materia di Salute e Sicurezza sul lavoro*. Con riferimento a tale aspetto è previsto/a:
  - 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 Stato - Regioni;
  - il possesso dei necessari requisiti da parte dei formatori della sicurezza in accordo a quanto definito dalla normativa vigente;
  - la verifica periodica dell'apprendimento.

  Nel pianificare le attività di formazione, informazione, addestramento è fatto obbligo di considerare l'eventuale presenza di lavoratori in distacco o distaccati.
- *Gestione della sorveglianza sanitaria e gestione degli infortuni*. Con riferimento a tale aspetto è previsto/a:
  - la predisposizione del protocollo sanitario e il relativo aggiornamento in relazione all'evolversi dell'organizzazione;
  - la visita medica:
    - preventiva e periodica intesa a constatare l'assenza di controindicazioni al lavoro cui il lavoratore è destinato, al fine di valutare la sua idoneità alla mansione specifica;
    - 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;
    - negli altri casi previsti dalla normativa vigente.

    Le visite mediche per la sorveglianza sanitaria non possono essere effettuate per accertare stati di gravidanza e negli altri casi vietati dalla normativa vigente;
  - la vigilanza sull'assolvimento degli obblighi previsti per il Medico Competente con particolare riferimento all'esecuzione dei sopralluoghi annuali sui luoghi di lavoro e alla presentazione della relazione annuale sui dati anonimi collettivi della sorveglianza sanitaria;
  - l'assolvimento degli obblighi di registrazione e comunicazione in caso di infortuni;
  - l'analisi e monitoraggio degli infortuni.
- *Acquisizione di documentazione e certificazioni obbligatorie di legge.* Con riferimento a tale aspetto è prevista l'identificazione delle modalità operative atte ad assicurare l'individuazione, l'acquisizione e l'adeguata conservazione della documentazione, delle registrazioni e delle certificazioni obbligatorie di legge, o che la Società ritiene necessarie per attestare il rispetto degli standard tecnico-strutturali di legge e un efficace gestione della salute e sicurezza sul lavoro, 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.* Con riferimento a tale aspetto è prevista:
  - la vigilanza sul rispetto delle procedure e delle istruzioni di sicurezza da parte del personale aziendale ed esterno e la segnalazione dei rischi e delle difformità rilevate;
  - l'attuazione di verifiche periodiche e sistematiche dell'applicazione e dell'efficacia delle procedure adottate;

- la definizione e implementazione di adeguati piani di azione per sanare eventuali difformità e/o carenze riscontrate nel corso delle verifiche.

3.10. TEMATICHE AMBIENTALI

3.10.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Gli aspetti ambientali legati alle attività della Società presentano, oltre ad un profilo di rischio diretto per i reati di corruzione, truffa, traffico di influenze illecite e induzione indebita a dare o promettere utilità (per i quali si rimanda al paragrafo 3.12 Rapporti con Istituzioni ed Enti Pubblici), un profilo di rischio diretto in quanto, in caso di gestione non conforme ai disposti legislativi applicabili in materia di ambiente, potrebbero originare illeciti di cui alle fattispecie previste dal D.Lgs. 231/01 art. 25 undecies.

Le tipologie di reato individuate dalla Società come potenzialmente applicabili sono:

- Raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza o in violazione della prescritta autorizzazione, iscrizione o comunicazione (art. 256 c. 1 e 4 DLgs 152/06). la fattispecie di reato può ritenersi astrattamente realizzabile in ipotesi di concorso nella commissione del reato nel caso di affidamento delle attività di trasporto o smaltimento di rifiuti ad operatori terzi non autorizzati o che operano in difformità alle autorizzazioni e alla normativa applicabile;
- traffico illecito di rifiuti (art. 259 c. 1 D.Lgs. 152/06). Il reato potrebbe realizzarsi in caso di spedizione transfrontaliera di rifiuti in difformità a quanto previsto dalla normativa di settore, ad esempio in relazione alla spedizione di rifiuti erroneamente considerati "materiale tecnico";
- attività organizzate per il traffico illecito di rifiuti (art. 260 c. 1 D.Lgs. 152/06 - Abrogato dall'art. 7 D.Lgs. 21/18 ed inserito all'art. 452-quaterdecies del c.p). Il reato potrebbe realizzarsi in caso di affidamento delle attività di trasporto o smaltimento di rifiuti ad operatori terzi non autorizzati o che operano in difformità alle autorizzazioni e alla normativa applicabile;
- delitti colposi contro l'ambiente (452 quinquies c.p.). Il reato potrebbe realizzarsi in caso di incendio in relazione alle potenziali conseguenze ambientali;
- associazione a delinquere e associazione di tipo mafioso diretta, in via esclusiva o concorrente, allo scopo di commettere taluno dei delitti previsti nel titolo vi-bis del codice penale e associazione di tipo mafioso finalizzata all'acquisizione della gestione o comunque del controllo di attività economiche, di concessioni, di autorizzazioni, di appalti o di servizi pubblici in materia ambientale (art. 452 octies c.p.). Il reato potrebbe realizzarsi in caso di impedito controllo o compromissione degli esiti dell'attività di vigilanza e controllo ambientali da parte di autorità di controllo.

3.10.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

Di seguito si esplicitano le principali attività individuate dalla Società come a potenziale rischio ai fini della commissione dei reati in tema ambientale, unitamente alle Funzioni coinvolte:

- gestione dei rifiuti (Regional Facility Manager);
- prevenzione e gestione delle emergenze (Datore di Lavoro/Country Leader o suo Delegato, nei limiti dei poteri conferiti, con la collaborazione del RSPP e della squadra di emergenza e primo soccorso).

3.10.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Per la gestione delle tematiche ambientali la Società ha definito un sistema di poteri e deleghe adeguati allo svolgimento delle attività sensibili e coerente con la struttura organizzativa della Società stessa. In particolare è garantito il rispetto dei seguenti principi di elaborazione giurisprudenziale:

- effettività - sussistenza e compresenza di autonomia decisionale e finanziaria del delegato;
- idoneità tecnico professionale ed esperienza del delegato;
- vigilanza sull'attività del delegato, non acquiescenza, non ingerenza;
- certezza, specificità e consapevolezza.

Le attività connesse con il presente profilo di rischio devono essere gestite nel rispetto dei principi generali di comportamento espressi nel presente Modello, nel Codice Etico e di Condotta e nel rispetto delle procedure aziendali che prevedono quanto segue:

- gestione dei rifiuti:
  - il rispetto degli adempimenti previsti dalla normativa in capo al produttore del rifiuto, tra cui la corretta classificazione dei rifiuti mediante l'attribuzione del Codice CER e il rispetto dei criteri di assimilabilità dei rifiuti stabiliti dal Comune di riferimento di ciascuna unità aziendale;
  - la discriminazione tra quanto è soggetto alla disciplina dei rifiuti e quanto invece può essere considerato "materiale tecnico" da sottrarre alla disciplina dei rifiuti;
  - la tenuta del registro di carico/scarico in caso di produzione di rifiuti speciali pericolosi;
  - il trasporto e smaltimento dei rifiuti speciali nel rispetto della normativa applicabile con particolare riferimento a:
    - affidamento dei rifiuti speciali a intermediari, trasportatori e smaltitori autorizzati;
    - verifica della correttezza e completezza della documentazione di trasporto (Formulario di Identificazione dei rifiuti) dei rifiuti;
    - monitoraggio della documentazione attestante il corretto smaltimento dei rifiuti (es. IV° copia del Formulario di Identificazione dei rifiuti), nonché adozione dei provvedimenti di legge in caso di mancato rientro entro i tempi previsti dalla normativa;
  - l'inserimento, nei documenti contrattuali con appaltatori o subappaltatori operanti presso le unità aziendali, degli obblighi e divieti a loro carico in relazione alla gestione dei rifiuti da loro prodotti.

  Nell'ambito della gestione dei rifiuti è fatto divieto di:
  - miscelare rifiuti pericolosi con i rifiuti non pericolosi e rifiuti pericolosi che abbiano caratteristiche di pericolosità differenti;
  - effettuare trasporto in conto proprio di rifiuti;
  - effettuare spedizioni transfrontaliere di rifiuti ovvero, ove necessarie, effettuare tali spedizioni nel rispetto della normativa applicabile;
- Prevenzione e gestione delle emergenze:
  - individuazione delle tipologie di emergenza che possono cagionare danno all'ambiente e predisposizione di adeguati presidi tecnici ed organizzativi per prevenire le emergenze e mitigarne gli effetti.

Con riferimento a tale attività a rischio, le procedure aziendali regolamentano, inoltre:

- le modalità di archiviazione e conservazione della documentazione di supporto e delle attività di controllo svolte;
- la vigilanza sul rispetto di procedure e istruzioni in materia ambientale da parte del personale aziendale ed esterno e la segnalazione delle difformità rilevate;
- le verifiche periodiche e sistematiche dell'applicazione e dell'efficacia delle procedure adottate;
- definizione e implementazione di adeguati piani di azione per sanare eventuali difformità e/o carenze riscontrate.

E' fatto divieto, inoltre, di 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.

3.11. GESTIONE PRECONTENZIOSO E CONTENZIOSO

3.11.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

L'attività di gestione del pre-contenzioso e del contenzioso di qualsiasi natura esso sia, ovvero civile, penale, giuslavoristico, con l'amministrazione finanziaria, ecc. è potenzialmente esposta al rischio di commissione dei reati di:

- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies D.Lgs. 231/01 - art. 377-bis c.p.). Per quel che riguarda le finalità e le modalità di commissione della condotta illecita, esse in astratto sono individuate attraverso:
  - l'offerta o la promessa di denaro o altra utilità nei confronti di una persona chiamata a rendere, davanti all'autorità giudiziaria, dichiarazioni utilizzabili in un procedimento giudiziario;
  - atti di violenza o minaccia di atti di violenza, nei confronti di una persona chiamata a rendere, davanti all'autorità giudiziaria, dichiarazioni utilizzabili in un procedimento giudiziario;
- corruzione in atti giudiziari (art. 25 D.Lgs. 231/01 - art. 319-ter c.p.) ed istigazione alla corruzione (art. 25 D.Lgs. 231/01 - art. 322 c.p.);
- truffa (art. 24 D.Lgs. 231/01 - art.640, comma 2, n.1, c.p.);
- induzione indebita a dare o promettere utilità (art. 25 D.Lgs. 231/01 - art. 319-quater c.p.);
- traffico di influenze illecite (art. 346-bis c.p.);
- abuso d'ufficio (art. 25 D.Lgs. 231/01 - art. 323 c.p.). Tale reato potrebbe essere commesso in via astratta nel caso in cui, in una eventuale causa con l'Unione Europea per l'applicazione di sanzioni a fronte delle quali la Società effettua ricorso presso il Tribunale dell'Unione Europea, la Società persuade uno o più giudici ad agire in virtù delle loro funzioni, ad esempio accettando un ricorso pervenuto fuori tempo massimo, procurando così alla Società un vantaggio patrimoniale ed offendendo gli interessi finanziari dell'UE;
- corruzione tra privati (art. 25-ter D.Lgs. 231/01 - art. 2635, comma 3 c.c.) ed istigazione alla corruzione tra privati (art. 25-ter D.Lgs. 231/01 – 2635 bis c.c.);
- autoriciclaggio (art. 25-octies D.Lgs. 231/01 - art. 648-ter 1 c.p.).

3.11.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

Di seguito si evidenziano gli Enti aziendali coinvolti nella gestione dell'attività a rischio Gestione del precontenzioso e del contenzioso (Responsabile attività Legal Business Partner – Funzioni coinvolte Country Leader, Sales Finance).

3.11.3. PROTOCOLLI DI CONTROLLO SPECIFICI

Le attività connesse con la presente area a rischio devono essere gestite nel rispetto dei principi generali di comportamento espressi nel presente Modello, nel Codice Etico e di Condotta e nel rispetto delle procedure aziendali/di Gruppo che prevedono quanto segue:

- la definizione della strategia da seguire nella gestione dei contenziosi;
- la tracciabilità delle attività di gestione dei contenziosi e delle decisioni in merito alle strategie adottate mediante:
  - la predisposizione da parte della Funzione che segue il contenzioso di una specifica informativa in cui sono riepilogati gli elementi essenziali della causa in essere;
  - la predisposizione da parte di Legal Business Partner ovvero l'invio a Legal Business Partner da parte delle Funzioni competenti di "Report" periodici contenenti:
    - lo "status" dei contenziosi in essere o possibili contenziosi;

  - una sintetica descrizione degli stessi e dei possibili scenari di contenzioso che si potrebbero instaurare tra la Società e soggetti terzi (es. Partners, clienti, ecc.);
- la gestione dei rapporti con l'autorità giudiziaria esclusivamente ad opera delle Funzioni/Aree competenti;
- la scelta dei legali sulla base di criteri di serietà e competenza del professionista;
- la sottoscrizione da parte del legale di una dichiarazione di assenza di conflitti di interesse e di accettazione del Code of Ethics and Business Conduct della Società;
- la formalizzazione degli accordi transattivi;
- la corresponsione dei compensi ai legali esterni, sulla base di una descrizione delle attività svolte, che permetta di valutare la conformità dell'onorario al valore della prestazione resa e previa attestazione dell'effettività della prestazione da parte della Funzione/Area che si è avvalsa della loro opera.

Si rinvia anche all'area a rischio Rapporti con istituzioni ed enti pubblici per la descrizione dei protocolli di controllo specifici, nella gestione delle attività che prevedono un rapporto con un rappresentante della Pubblica Amministrazione.

3.12. RAPPORTI CON ISTITUZIONI ED ENTI PUBBLICI

3.12.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

Preliminarmente all'analisi del potenziale profilo di rischio in merito ai rapporti con istituzioni ed enti pubblici, si evidenzia che, per la definizione di pubblico ufficiale ed incaricato di pubblico servizio, sono presi a riferimento per la predisposizione del presente Modello, **gli artt. 357, 358 e 322-*bis* c.p.** In particolare, gli articoli anzidetti riportano la nozione di *pubblici ufficiali* e di *incaricati di un pubblico servizio* italiani ed appartenenti ad organismi internazionali:

1. soggetti che svolgono una pubblica funzione legislativa o amministrativa, quali, ad esempio:
    - parlamentari e membri del Governo;
    - consiglieri regionali e provinciali;
    - parlamentari europei e membri del Consiglio d'Europa;
    - soggetti che svolgono funzioni accessorie (addetti alla conservazione di atti e documenti parlamentari, alla redazione di resoconti stenografici, di economato, tecnici, ecc.);
2. soggetti che svolgono una pubblica funzione giudiziaria, quali, ad esempio:
    - magistrati (magistratura ordinaria di Tribunali, Corti d'Appello, Suprema Corte di Cassazione, Tribunale Superiore delle Acque, TAR, Consiglio di Stato, Corte Costituzionale, Tribunali militari, giudici popolari delle Corti d'Assise, giudici di pace, vice pretori onorari ed aggregati, membri di collegi arbitrali rituali e di commissioni parlamentari di inchiesta, magistrati della Corte Europea di Giustizia, nonché delle varie corti internazionali, ecc.);
    - soggetti che svolgono funzioni collegate (ufficiali ed agenti di polizia giudiziaria, guardia di finanza e carabinieri, cancellieri, segretari, custodi giudiziari, ufficiali giudiziari, testimoni, messi di conciliazione, curatori fallimentari, operatori addetti al rilascio di certificati presso le cancellerie dei tribunali, periti e consulenti del Pubblico Ministero, commissari liquidatori nelle procedure fallimentari, liquidatori del concordato preventivo, commissari straordinari dell'amministrazione straordinaria delle grandi imprese in crisi, ecc.);
3. soggetti che svolgono una pubblica funzione amministrativa, quali, ad esempio:
    - dipendenti dello Stato, di organismi internazionali ed esteri e degli enti territoriali (funzionari e dipendenti dello Stato, dell'Unione Europea, di organismi sopranazionali, di Stati esteri e degli Enti territoriali, ivi comprese le Regioni, le Province, i Comuni e le Comunità montane; soggetti che svolgano funzioni accessorie rispetto ai fini istituzionali dello Stato, quali componenti dell'ufficio tecnico comunale, membri della commissione edilizia, capo ufficio amministrativo dell'ufficio condoni, messi comunali, addetti alle pratiche riguardanti l'occupazione del suolo pubblico, corrispondenti comunali addetti all'ufficio di collocamento, dipendenti delle aziende di Stato e delle aziende municipalizzate; soggetti addetti all'esazione dei tributi, personale sanitario delle strutture pubbliche, personale dei ministeri, delle soprintendenze ecc.);
    - dipendenti di altri enti pubblici, nazionali ed internazionali (funzionari e dipendenti dell'Agenzia delle Dogane e dei Monopoli, della Banca d'Italia, delle Autorità di Vigilanza, degli istituti di previdenza pubblica, dell'ISTAT, dell'ONU, della FAO, ecc.).

Non sono considerate pubblico servizio le attività che, pur disciplinate da norme di diritto pubblico o da atti autoritativi, consistono tuttavia nello svolgimento di semplici mansioni di ordine o nella prestazione di opera meramente materiale.

Le figure del pubblico ufficiale e dell'incaricato di pubblico servizio sono individuate non sulla base del criterio della appartenenza o dipendenza da un Ente pubblico, ma con riferimento alla natura dell'attività svolta in concreto dalla medesima, ovvero, rispettivamente, pubblica funzione e pubblico servizio.

Anche un soggetto estraneo alla Pubblica Amministrazione (di seguito "PA") può dunque rivestire la qualifica di pubblico ufficiale o di incaricato di pubblico servizio, quando eserciti una delle attività definite come tali dagli

artt. 357 e 358 c.p. (ad esempio dipendenti di istituti bancari ai quali siano affidate mansioni rientranti nel "pubblico servizio").

Passando ad analizzare il potenziale profilo di rischio dell'area rapporti con le istituzioni ed enti pubblici, la gestione dei rapporti con la PA espone la Società al rischio di commissione o concorso nei reati di:

- concussione (art. 317 c.p.), corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), istigazione alla corruzione (art. 322 c.p.), peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti Internazionali o degli organi delle Comunità Europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.);
- traffico di influenze illecite (art. 346-bis c.p.);
- induzione indebita a dare o promettere utilità (art. 319-quater c.p.)
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.).

Tali reati si potrebbero in astratto configurare ad esempio attraverso la dazione ovvero promessa di denaro o di altra utilità (anche per il tramite di una persona che eserciti influenze illecite) a:

- un funzionario della PA per non fare emettere provvedimenti/sanzioni nei confronti della Società nell'ambito di verifiche o altri adempimenti normativi a cui la Società è soggetta;
- un funzionario della PA per rendere ammissibili come rendicontazione di finanziamenti pubblici taluni dati non conformi;
- un dipendente chiamato a testimoniare, per indurlo a rilasciare dichiarazioni mendaci (o non rilasciare dichiarazioni) all'autorità giudiziaria;
- un testimone di un processo, per indurlo a rilasciare dichiarazioni mendaci (o per non rilasciare dichiarazioni) all'autorità giudiziaria.

Inoltre la gestione dei rapporti con la PA espone la Società al rischio di commissione o concorso nei reati di:

- truffa (art. 640, comma 2 n. 1, c.p.), truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.), malversazione di erogazioni pubbliche (art. 316-bis c.p.) e indebita percezione di erogazioni pubbliche (art. 316-ter c.p.). Per quel che riguarda le finalità e le modalità di commissione delle condotte illecite, esse in astratto sono individuate ad esempio:
  - nell'alterazione del contenuto della documentazione – in termini di incompletezza, non correttezza, ecc. - destinata agli Enti pubblici competenti in materia di personale appartenente alle categorie protette, oppure relativa a richieste di autorizzazione o per l'ottenimento di erogazioni pubbliche;
  - nella trasmissione all'amministrazione finanziaria di documentazione contenente false informazioni al fine di ottenere un rimborso fiscale non dovuto;
  - nell'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;
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.), che si configura, in via astratta, ad esempio attraverso la predisposizione e l'invio alle autorità di vigilanza di documentazione non veritiera o l'occultamento e/o omissione di documenti ed informazioni rilevanti in sede di ispezioni;
- frode informatica (art. 640-ter, comma 1, c.p.). Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro Ente pubblico. L'interferenza può realizzarsi in varie forme, in fase di:

- raccolta ed inserimento dei dati;
- elaborazione dei dati;
- emissione dei dati.

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, per quel che riguarda le modalità di commissione del reato esse in astratto potrebbero essere:

- la modificazione delle informazioni relative alla situazione contabile di un rapporto contrattuale in essere con un Ente pubblico;
- l'alterazione dei dati fiscali e/o previdenziali contenuti in una banca dati facente capo alla PA;

- corruzione tra privati (art. 2635, comma 3 c.c.) e istigazione alla corruzione tra privati (art. 2635-bis, comma 1, c.c.), nel caso in cui ad esempio un referente della Società corrompa o tenti di corrompere, anche per interposta persona, offrendo o promettendo denaro o altra utilità, il legale ovvero il consulente tecnico di parte della controparte, appartenenti ad uno Studio professionale.

3.12.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

La Società intrattiene una molteplicità di rapporti con la PA nell'esecuzione della propria attività (es. INAIL-INPS, Ispettorato del Lavoro, ISTAT). Di seguito si evidenziano gli Enti aziendali coinvolti nella gestione dell'attività a rischio rapporti con istituzioni ed enti pubblici (Responsabile attività Country Leader – Funzioni coinvolte Legal Business Partner, Sales Finance, Payroll Specialist e HR).

3.12.3. PROTOCOLLI DI CONTROLLO SPECIFICI

I rapporti con Istituzioni ed Enti pubblici devono essere gestiti, oltre che in conformità ai principi contenuti nel Codice Etico e di Condotta, nel rispetto di Linee guida definite dalla Società che prevedono:

- i seguenti criteri generali cui devono essere ispirati i rapporti con la PA:
  - nella gestione dei diversi rapporti con i vari enti della PA, deve essere garantita un'adeguata separazione delle funzioni;
  - nel caso di partecipazione a gare di qualsiasi tipo indette dalla PA, 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;
  - i contributi in denaro o in prodotti e servizi erogati a favore di Enti di beneficenza, ad Enti culturali, di istruzione, scuole e Fondazioni sono ammessi, purché effettuati nella massima trasparenza e nel rispetto delle regole, delle procedure interne e della normativa vigente;
  - con riferimento alla gestione di autorizzazioni, licenze e concessioni amministrative, 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 Funzioni aziendali competenti nel rispetto della legge e delle altre norme vigenti in materia;
  - l'utilizzo delle procedure informatiche deve avvenire secondo le modalità corrette;
  - è posto il divieto di:
    - 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;

- erogare qualsiasi forma di contributo a favore di partiti politici, pubblici ufficiali, etc. tramite ad esempio pagamenti diretti o indiretti, prestiti, anticipi, depositi o donazioni di denaro, prodotti o prestazione di servizi;

- la verifica di tutti i documenti (es. dichiarazioni) che devono essere inviati alla PA e la sottoposizione degli stessi alla firma del procuratore abilitato;
- criteri di escalation gerarchica nella gestione dei rapporti con la PA, soprattutto laddove si ravvisino criticità non risolvibili nell'ambito dell'ordinaria gestione;
- la tempestiva segnalazione alle Funzioni aziendali competenti ed all'OdV di ogni eventuale situazione anomala;
- adeguata tracciabilità, archiviazione e conservazione della documentazione relativa ai principali rapporti intrattenuti con la PA (ad esempio mediante scambio di email, redazione/sottoscrizione di verbali, comunicazioni tramite email al proprio superiore gerarchico di incontri tenuti con rappresentanti della PA).

Con riferimento alle attività di ispezione/verifica da parte di esponenti della PA, il personale Hitachi Vantara Italia deve rispettare i criteri di:

- qualità e tempestività delle comunicazioni alle autorità di vigilanza;
- attendibilità delle comunicazioni;
- adeguata formalizzazione delle attività;
- messa a disposizione con tempestività e completezza della documentazione richiesta e massima disponibilità e collaborazione all'espletamento degli accertamenti/attività di verifica.

Si rinvia anche alle precedenti aree a rischio per la descrizione dei protocolli di controllo specifici, nella gestione delle ulteriori attività che possono prevedere un rapporto con un rappresentante della PA.

3.13. DONAZIONI, LIBERALITÀ E OMAGGI

3.13.1. DESCRIZIONE DEL POTENZIALE PROFILO DI RISCHIO

La gestione delle donazioni, delle liberalità e degli omaggi, costituisce una modalità strumentale attraverso cui, in linea di principio, potrebbero essere commessi i reati di:

- corruzione per l'esercizio della funzione (art. 25 D.Lgs. 231/01 - art. 318 c.p.), corruzione per un atto contrario ai doveri d'ufficio (art. 25 D.Lgs. 231/01 - art. 319 c.p.), corruzione di persona incaricata di un pubblico servizio (art. 25 D.Lgs. 231/01 - art. 320 c.p.), istigazione alla corruzione (art. 25 D.Lgs. 231/01 - art. 322 c.p.), peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione, abuso d'ufficio di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.);
- traffico di influenze illecite (art. 346-bis c.p.);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies D.Lgs. 231/01 - art. 377-bis c.p.);
- induzione indebita a dare o promettere utilità (art. 25 D.Lgs. 231/01 - art. 319-quater c.p.);
- corruzione tra privati e istigazione alla corruzione tra privati (art. 25-ter, D.Lgs. 231/01 - artt. 2635, comma 3, e 2635-bis comma 1, c.c.).

Tali reati potrebbero, infatti, essere commessi in via astratta attraverso:

- la concessione o promessa di omaggi/liberalità/spese di ospitalità/sponsorizzazioni a soggetti pubblici o assimilabili o a soggetti privati, al fine di ottenere in cambio vantaggi, trattamenti di favore, mancata applicazione di una sanzione, ecc.;
- la concessione o promessa di beni/servizi aziendali a titolo gratuito a soggetti pubblici o assimilabili o a soggetti privati, al fine di ottenere in cambio vantaggi, trattamenti di favore, mancata applicazione di una sanzione, ecc.;
- l'invito ad eventi, graditi a soggetti pubblici o assimilabili o a soggetti privati al fine di ottenere in cambio vantaggi, trattamenti di favore, mancata applicazione di una sanzione, ecc..

Infine tale area è astrattamente a rischio per quel che riguarda il reato di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 ter c.p.) nell'ipotesi in cui un soggetto apicale o sottoposto di HVI effettui pagamenti per il sostenimento di omaggi o spese di rappresentanza mediante carta di pagamento a lui non intestata o altro strumento diverso dal contante, e quindi mediante utilizzo indebito, per ottenere da quell'operazione un vantaggio per la Società. Il reato potrebbe realizzarsi nell'ipotesi in cui un soggetto apicale o sottoposto di HVI effettui un pagamento o anche un prelievo mediante carta di pagamento a lui non intestata o altro strumento diverso dal contante, e, quindi, mediante utilizzo indebito, per ottenere da quell'operazione un vantaggio illecito per la Società.

3.13.2. ATTIVITÀ A RISCHIO ED ENTI COINVOLTI

Di seguito si evidenziano gli enti coinvolti nella gestione dell'attività a rischio Gestione di donazioni, liberalità e omaggi (Responsabile attività Country Leader).

3.13.3. PROTOCOLLI DI CONTROLLO SPECIFICI

La gestione dei regali/omaggi/spese di ospitalità ecc. ricevuti/offerti dal personale della Società, deve essere effettuata, oltre che in conformità ai principi contenuti nel Codice Etico e di Condotta e nel rispetto di Linee guida definite dalla Società che prevedono:

- che le spese relative ad ospitalità e rappresentanza dovranno essere ragionevoli e comunque tali da non poter essere interpretate come finalizzate a ottenere un trattamento di favore da parte del Destinatario;

- il divieto espresso di corrispondere pagamenti di facilitazione allo scopo di favorire prestazioni comunque dovute da parte della PA o di soggetti privati terzi;
- controlli formalizzati sull'approvazione degli omaggi e delle spese di rappresentanza;
- la verifica formale dei giustificativi di spesa e corrispondenza tra i giustificativi di spesa e le somme contabilizzate;
- gli omaggi e le spese di rappresentanza devono:
  - essere ragionevoli e comunque tali da non poter essere interpretati come finalizzati ad ottenere un trattamento di favore da parte del Destinatario;
  - essere rivolti verso Destinatari che svolgono ruoli inerenti le attività aziendali e che rispondono ai requisiti di reputazione e di onorabilità generalmente riconosciuti;
  - tenere conto del profilo del Destinatario, con riguardo alle consuetudini nei rapporti professionali e nel rispetto delle culture locali;
  - essere effettuati dagli amministratori, dai dirigenti e dai dipendenti in funzione dell'attività svolta e del ruolo ricoperto all'interno della Società;
  - essere previsti da specifiche disposizioni aziendali;
  - essere in linea con il budget e comunque preventivamente autorizzati dal responsabile competente della Società, in conformità alle applicabili procedure aziendali.

In particolare per gli omaggi e le spese di rappresentanza è predisposta da parte delle strutture competenti una reportistica di monitoraggio contenente le informazioni atte a tracciare chi ha offerto o ricevuto l'omaggio, la data dell'offerta o del ricevimento dell'omaggio, il valore attuale o stimato, l'indicazione dell'eventuale accettazione o rifiuto e delle relative motivazioni.

E' comunque vietata qualsiasi forma di omaggio ad esponenti di altre società private, o a loro familiari, che possa indurre ad assicurare un qualsiasi vantaggio per la Società. Gli omaggi offerti o ricevuti – salvo quelli di modico importo – devono essere documentati in modo adeguato.

Per quanto riguarda la gestione dei regali/omaggi/spese di ospitalità ecc. ricevuti/offerti dal personale della Società, le Policy di Gruppo definiscono i limiti ed i criteri sulla base dei quali la Società ammette tali operazioni. In particolare è previsto con riferimento all'offerta/ricevimento di regali e omaggi o al sostenimento delle spese di ospitalità (pasti/intrattenimento):

- il divieto di offrire/ricevere regali eccedenti il valore di 30$, e di offrire/ricevere spese di ospitalità eccedenti il valore di 100$, senza la previa approvazione scritta da parte del "local Legal Counsel or the Compliance Department";
- i regali devono consistere in gadget contenenti il logo della Società e non possono essere costituiti da denaro o equivalenti;
- il divieto di offrire/ricevere doni a coniugi o ai familiari di esponenti della PA;
- che nessun regalo/omaggio deve essere offerto/ricevuto in violazione di leggi vigenti.