ELIS INNOVATION HUB s.r.l.

Modello di Organizzazione Gestione e Controllo ex Decreto Legislativo 8 giugno 2001, n° 231

Approvato dal Consiglio di Amministrazione nella seduta del 20.04.2022

1 PARTE GENERALE: ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO 3
1.1 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO 4
1.1.1 Formazione delle risorse e diffusione del Modello 7
1.1.2 Sistema disciplinare 7
1.1.3 Organismo di Vigilanza 8
1.1.4 Aggiornamento del Modello 10
2 PARTE SPECIALE: DIVERSE TIPOLOGIE DI REATO, AREE A RISCHIO PER ATTIVITÀ DI ELIS INNOVATION HUB S.R.L. 11
2.1 REATI CONTRO LA PUBBLICA AMMINISTRAZIONE E L'AMMINISTRAZIONE DELLA GIUSTIZIA 12
2.1.1 Aree a rischio reato, principi generali di comportamento e controlli preventivi 12
2.1.2 Compiti dell'Organismo di Vigilanza 24
2.2 REATI AMMINISTRATIVI/SOCIETARI 26
2.2.1 Aree a rischio reato, principi generali di comportamento e controlli preventivi 26
2.2.2 Compiti dell'Organismo di Vigilanza 29
2.3 CORRUZIONE TRA PRIVATI 30
2.3.1 Aree a rischio reato, principi generali di comportamento e controlli preventivi 30
2.3.2 Compiti dell'Organismo di Vigilanza 39
2.4 REATI IN VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO 40
2.4.1 Aree a rischio reato in tema di salute e sicurezza sul lavoro 40
2.4.2 Sistema aziendale per la tutela della salute e sicurezza sul lavoro 41
2.4.3 Documento di Valutazione dei Rischi 41
2.4.4 Rapporti con i fornitori: qualifica, informazione, coordinamento e clausole contrattuali 42
2.4.5 Monitoraggio degli infortuni e incidenti 42
2.4.6 Audit 42
2.4.7 Riesame della Direzione 43
2.4.8 Compiti dell'Organismo di Vigilanza 43

2.5 REATI INFORMATICI - VIOLAZIONE DEL DIRITTO D'AUTORE 44

2.5.1 Aree a rischio reato, principi generali di comportamento e controlli preventivi 45

2.5.2 Protocolli a presidio dei reati in oggetto 48

2.5.3 Compiti dell'Organismo di Vigilanza 50

2.6 TRATTAMENTO ILLECITO DEI DATI PERSONALI 51

2.6.1 Aree a rischio reato, principi generali di comportamento e controlli preventivi 52

2.6.2 Compiti dell'Organismo di Vigilanza 55

2.7 REATI TRIBUTARI 56

2.7.1 Aree a rischio reato, principi generali di comportamento e controlli preventivi 57

2.7.2 Compiti dell'Organismo di Vigilanza 62

1 PARTE GENERALE: ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

1.1 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Il Decreto Legislativo 8 giugno 2001, n. 231 (in seguito Decreto) ha introdotto per la prima volta nel nostro ordinamento la responsabilità degli enti per alcuni reati commessi, nel loro interesse o vantaggio, da soggetti dipendenti o anche solo in rapporto funzionale con l'ente stesso, responsabilità che va ad aggiungersi a quella della persona fisica che ha commesso effettivamente il reato. Le sanzioni previste sono particolarmente significative e possono arrivare fino all'interdizione definitiva dell'attività.
Il Decreto stabilisce un principio base:

Le Società possono essere sanzionate per reati commessi dai vertici o dai dipendenti e collaboratori.

Ai sensi dell'art. 5, comma 1 del Decreto, la Società può essere ritenuta responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- da soggetti in posizione apicale, vale a dire da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa avente autonomia finanziaria e funzionale;
- da soggetti in posizione di fatto apicale, vale a dire da persone che esercitano anche di fatto, senza formale investitura, la gestione e il controllo dell'ente;
- da soggetti direttamente subordinati alle posizioni di vertice, vale a dire da persone sottoposte alla direzione o alla vigilanza di un soggetto in posizione apicale.

Il Decreto, tuttavia, all'art. 6, punto 1, prevede che la Società non risponde dei reati commessi se prova che:

- la Direzione abbia adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e gestione idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e sull'osservanza del modello e di proporne l'aggiornamento sia stato affidato a un Organismo di Vigilanza (in seguito OdV) dotato di autonomi poteri di iniziativa e controllo;
- le persone abbiano eluso coscientemente e volutamente i modelli di organizzazione e gestione;
- non vi sia stata omessa o insufficiente vigilanza da parte dell'OdV.

L'adozione di un modello di organizzazione e gestione da parte della Società è, quindi, facoltativa, ma è "*conditio sine qua non*" perché la stessa sia esonerata dalla responsabilità. Tale esonero è riconosciuto a valle del procedimento giudiziale. Un buon modello, peraltro, è indispensabile per un armonico ed efficiente sviluppo della Società e per una consapevole gestione dei rischi operativi.
ELIS Innovation Hub s.r.l. (in seguito EIH o Società), al fine di assicurare che il comportamento di tutti coloro che operano per suo conto o nel suo interesse sia sempre conforme alle normative e coerente con i principi di correttezza e trasparenza nella conduzione delle sue attività, ha adottato il presente Modello di Organizzazione, Gestione e Controllo (in seguito Modello) in linea con le prescrizioni del Decreto. Il Modello si applica nella sede di Roma (Via Sandro Sandri 81) e nella sede secondaria di Catania (Via Caronda 129).

EIH ha per oggetto, in via prevalente, lo sviluppo, la produzione e la commercializzazione di prodotti o servizi innovativi ad alto valore tecnologico e più specificamente lo sviluppo, la produzione, la commercializzazione, l'implementazione, la gestione e il coordinamento di

programmi di ricerca e sviluppo, digital transformation, open innovation, digital consulting, attraverso metodologie innovative e servizi ad alto valore tecnologico basati sul paradigma Industria 4.0. Tali attività hanno l'obiettivo di aiutare i giovani capaci e volenterosi a sviluppare i propri talenti superando le difficoltà di inserimento sociale e lavorativo determinate da condizioni familiari e ambientali e saranno svolte in sinergia con gli altri Enti che aderiscono ai principi del Manifesto ELIS (Educazione, Lavoro, Istruzione, Sport), condividendone quindi la stessa finalità: l'educazione e la formazione al lavoro dei giovani per offrire a ciascuno la possibilità di costruire il proprio progetto di vita. Essi s'impegnano per questo ad annullare le distanze che separano i giovani e i disoccupati da una formazione di alta specializzazione, le periferie sociali dai centri dello sviluppo, le start-up dalle grandi aziende, i sistemi della formazione dal mondo del lavoro. Attuano programmi di formazione in assetto lavorativo, per trasmettere competenze adeguate all'evolversi delle professioni. Realizzano percorsi di formazione e affiancamento per lo sviluppo delle potenzialità umane e professionali di chi già lavora in azienda. Promuovono le virtù umane e le attitudini relazionali della persona, proponendo un ideale di lavoro che sia opportunità di crescita al servizio degli altri e per il bene comune.
EIH potrà svolgere inoltre altre attività secondarie rispetto alla prevalente come riportato nello Statuto.

Sono destinatari del presente Modello e, come tali, tenuti alla sua conoscenza e osservanza nell'ambito delle specifiche competenze:

- i membri del Consiglio di Amministrazione nel perseguimento degli obiettivi di EIH;
- tutti i dipendenti e i collaboratori con i quali si intrattengono rapporti contrattuali a qualsiasi titolo, anche temporanei o semplicemente occasionali, sia onerosi sia a titolo gratuito.

Il Modello è costituito da:

- una Parte Generale, dove sono illustrate le componenti essenziali del Modello, con particolare riferimento alla formazione del personale e alla diffusione nel contesto operativo, al sistema disciplinare e alle misure da adottare in caso di mancata osservanza delle prescrizioni dello stesso e all'Organismo di Vigilanza;
- una Parte Speciale, dove sono illustrate le diverse tipologie di reato e illecito contemplate nel Decreto, alle quali EIH è considerata esposta nello svolgimento delle sue attività:
    1. **Reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia;**
    2. **Reati Amministrativi/Societari;**
    3. **Corruzione tra Privati;**
    4. **Reati in Violazione delle Norme sulla Tutela della Salute e Sicurezza sul Lavoro;**
    5. **Reati Informatici - Violazione del Diritto d'Autore;**
    6. **Trattamento Illecito dei Dati Personali;**
    7. **Reati Tributari.**

L'inserimento della tipologia di reato n. 6 è finalizzato alla prevenzione degli illeciti contemplati nel Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (Protezione delle Persone Fisiche con Riguardo al Trattamento dei Dati Personali). Ciò anche per garantire un necessario coordinamento tra "modello 231" e "modello privacy" e non creare un sistema di controlli interno ridondante.
Per le prime tre tipologie, per il trattamento illecito dei dati personali e per i reati tributari possono identificarsi alcune aree aziendali specificamente esposte al rischio di commissione, mentre per gli altri reati si ritiene di non localizzare il rischio in aree specifiche, ma di valutarlo come **rischio diffuso**, in considerazione del fatto che essi potrebbero essere astrattamente posti in essere in qualsiasi ambito di attività. Per questa ragione EIH ha da tempo adottato opportune misure

preventive, predisponendo il **Documento per la Valutazione dei Rischi** e il **Disciplinare delle Risorse Informatiche per i Dipendenti e i Collaboratori degli Enti Aderenti al Manifesto ELIS**, ai quali il presente Modello fa riferimento, e ha previsto vari interventi formativi.

Il Modello si fonda sui seguenti punti.

- Un **sistema normativo,** basato sui principi e i valori espressi nel proprio Codice Etico. EIH proclama il lavoro come un cammino di arricchimento personale, di solidarietà sociale e di miglioramento di sé stessi e degli altri. Il valore straordinario del lavoro in tutte le sue forme, sia manuale sia intellettuale, è la ricchezza che tante persone hanno scoperto e scoprono negli enti che aderiscono al Manifesto ELIS ed è garanzia nella prevenzione dei reati.
- Una **struttura organizzativa** coerente con le attività, idonea ad assicurare la correttezza dei comportamenti e una chiara attribuzione dei compiti, applicando un'appropriata segregazione delle funzioni attraverso un organigramma e un sistema autorizzativo.
- Un **sistema di controllo di gestione e dei flussi finanziari** nelle attività a rischio. In particolare, il sistema di controllo di gestione è articolato nelle diverse fasi di elaborazione del budget annuale, di elaborazione delle previsioni e di analisi dei consuntivi.
- Un **sistema di formazione** finalizzato a rendere tutti i destinatari del Modello consapevoli dei principi e delle regole cui la normale operatività deve conformarsi.
- Un **sistema disciplinare** idoneo a sanzionare qualsiasi violazione del Modello.
- Un **Organismo di Vigilanza** dotato di autonomia, indipendenza, professionalità, continuità di azione, poteri e accesso alle informazioni necessarie allo svolgimento dell'attività, con il compito di vigilare sul funzionamento e sull'osservanza del Modello e di proporne l'aggiornamento.

Il Modello si propone di:

- **ribadire che ELIS Innovation Hub non tollera comportamenti illeciti, perché contrari ai valori contenuti nel proprio Codice Etico e, dunque, in contrasto con il suo interesse;**
- predisporre un sistema per la prevenzione e il controllo finalizzati alla riduzione del rischio di commissione dei reati connessi all'attività;
- informare e formare i destinatari del Modello sull'esistenza di detto sistema e sulla necessità che l'operatività sia costantemente conforme ad esso;
- rendere tutti coloro che operano in nome, per conto o comunque nell'interesse di EIH consapevoli del fatto che la commissione di un reato nel presunto interesse della medesima la espone a problemi finanziari, operativi e d'immagine;
- rendere tutti coloro che operano in nome, per conto o comunque nell'interesse di EIH consapevoli del fatto che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di provvedimenti disciplinari, indipendentemente dall'eventuale commissione di fatti costituenti reato.

L'adozione e le successive modifiche e integrazioni del Modello competono al Consiglio di Amministrazione, in conformità alle prescrizioni del Decreto.

L'Organismo di Vigilanza dispone le modifiche formali al Modello, avvalendosi della Direzione della Società.

1.1.1 Formazione delle risorse e diffusione del Modello

L'adozione di un programma di formazione per tutte le risorse, indipendentemente dalla posizione e dal livello gerarchico, costituisce uno dei presupposti per la corretta ed efficace attuazione del Modello e per l'esenzione di responsabilità della Società in caso di commissione dei reati di cui al D. Lgs. 231/2001.

EIH promuove la conoscenza del Modello, del sistema normativo interno e dei relativi aggiornamenti tra tutti i dipendenti, che sono pertanto tenuti a conoscerne il contenuto e a osservarlo. Ai fini dell'attuazione del Modello, Risorse Umane gestisce, in cooperazione con l'Organismo di Vigilanza, la formazione del personale, che potrà essere erogata con modalità "e-learning", attraverso sessioni formative in aula ed e-mail occasionali di aggiornamento.

In tale contesto, le azioni comunicative prevedono:

- la disponibilità del Codice Etico e del Modello per tutto il personale in forza e la distribuzione ai nuovi assunti;
- l'aggiornamento sulle modifiche al Modello, conseguenti a variazioni normative e/o organizzative rilevanti ai fini del Decreto.

Eventuali sessioni formative di aggiornamento saranno effettuate in caso di modifiche rilevanti apportate al Modello o relative a sopraggiunte normative rilevanti per l'attività di EIH.

La partecipazione al corso con modalità e-learning, così come quella alle eventuali sessioni formative in aula, è obbligatoria. Risorse Umane controlla che il percorso formativo sia fruito da tutto il personale.

EIH promuove la conoscenza e l'osservanza del Codice Etico e del Modello anche tra i collaboratori a vario titolo, i partner, i clienti e i fornitori.

L'informativa avviene attraverso la diffusione di una comunicazione ufficiale sull'esistenza del Modello, con indicazioni per la consultazione su ELIS ERP (Enterprise Resource Planning).

EIH provvede a inserire nei contratti con le controparti e i consulenti apposite clausole che prevedono la possibile risoluzione del vincolo negoziale in caso di inosservanza dei principi etici stabiliti.

1.1.2 Sistema disciplinare

L'esistenza di un sistema disciplinare in caso di violazione delle prescrizioni contenute nel Modello è condizione essenziale per assicurarne l'effettività.

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

Costituiscono condotte oggetto di sanzione le azioni o i comportamenti in violazione del Modello. Essendo quest'ultimo costituito anche dal complesso del corpo normativo, che ne è parte integrante, ne deriva che per "violazione del Modello" deve intendersi anche la violazione di una o più procedure a esso correlate e dei principi contenuti nel Codice Etico.

L'applicazione delle sanzioni disciplinari prescinde da un eventuale procedimento penale, perché le regole del Modello sono assunte in piena autonomia da EIH.

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

- gravità dell'illecito;

- circostanze e modalità in cui si è realizzato l'illecito;
- commissione di più illeciti nell'ambito della medesima condotta;
- concorso di più soggetti nella commissione dell'illecito;
- recidività dell'autore dell'illecito.

Il sistema disciplinare è costantemente monitorato da Risorse Umane, che ne riferisce all'Organismo di Vigilanza, ed è valido per i membri del Consiglio di Amministrazione, per il personale dipendente, dirigente e no, per i collaboratori, consulenti, partner, terzi e soggetti esterni destinatari del Modello.

1.1.3 Organismo di Vigilanza

Il Decreto stabilisce (art. 6, comma 1, lett. b) che il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello, nonché quello di curarne l'aggiornamento, sia affidato a un Organismo di Vigilanza, nominato dal Consiglio di Amministrazione.

L'OdV possiede competenze adeguate alle funzioni che è chiamato a svolgere e indipendenza per svolgere il proprio ruolo, senza condizionamenti diretti o indiretti da parte dei soggetti controllati. A garanzia dell'indipendenza, l'OdV riferisce direttamente al Consiglio di Amministrazione.
L'OdV deve:

- operare con continuità per il rispetto e l'applicazione del Modello;
- non svolgere mansioni operative che possano distrarre dall'attività che a esso si richiede;
- curare l'aggiornamento del Modello.

Ai fini di un migliore e più efficace espletamento dei propri compiti, l'OdV può avvalersi degli enti interni che, di volta in volta, si potranno rendere utili.
L'OdV può anche delegare lo svolgimento di compiti specifici a uno dei suoi componenti, con l'obbligo di riferire in merito all'OdV nella sua collegialità, che mantiene in ogni caso la responsabilità.

Per lo svolgimento dei suoi compiti l'OdV può:

- accedere a ogni documento e/o informazione rilevante;
- ricorrere a consulenti esterni di provata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo o di aggiornamento del Modello, seguendo le procedure interne previste per l'assegnazione di incarichi di consulenza;
- procedere, qualora si renda necessario, all'audizione diretta dei membri del Consiglio di Amministrazione e dei dipendenti;
- richiedere informazioni a collaboratori, consulenti esterni, partner e revisori.

L'OdV relaziona formalmente su base periodica il Consiglio di Amministrazione in merito alle attività svolte, alle segnalazioni ricevute, agli interventi correttivi e migliorativi del Modello e al loro stato di implementazione. In ogni caso l'OdV deve informare senza indugio il Consiglio di Amministrazione in caso di violazioni del Codice Etico e del Modello di cui sia venuto a conoscenza e che abbia accertato esso stesso e, nei casi di necessità, modificare il Modello.

Flussi informativi nei confronti dell'Organismo di Vigilanza

Il Decreto prevede (art. 6, comma 2, lett. d) obblighi informativi nei confronti dell'OdV sul funzionamento e l'osservanza del Modello.

L'efficacia dell'attività di vigilanza richiede un sistema d'informazioni e segnalazioni da tutti i destinatari del Modello, relative a tutti gli atti, i comportamenti e gli eventi di cui vengano a conoscenza, che potrebbero determinare una violazione del Modello o che, più in generale, siano potenzialmente rilevanti ai fini del Decreto.

Al fine di facilitare il flusso d'informazioni e le segnalazioni verso l'OdV di attività potenzialmente in contrasto con le disposizioni del Decreto, sono stati istituiti canali informativi ad hoc, consistenti in un indirizzo e-mail alias (odv@elis.org), che inoltra il messaggio ai singoli componenti, e una cassetta postale dedicata per le comunicazioni cartacee.

L'OdV valuta le segnalazioni ricevute, comprese quelle in forma anonima, e determina le eventuali iniziative, ascoltando eventualmente l'autore della segnalazione, il responsabile della presunta violazione e ogni altro soggetto che riterrà utile, motivando per iscritto ogni conclusione raggiunta.

I flussi informativi per l'OdV possono essere occasionali o accessibili in modo sistematico.

I flussi informativi occasionali indirizzati all'OdV da esponenti aziendali o da terzi riguardano criticità attuali o potenziali e possono consistere in:

- notizie dalle quali si evinca lo svolgimento d'indagini o accertamenti riguardanti EIH per i reati di cui al Decreto;
- richieste di assistenza legale da parte del personale, dirigente e no, in caso di avvio di procedimento giudiziario per i reati di cui al Decreto;
- commissione di reati o comportamenti finalizzati alla commissione degli stessi;
- rapporti dai quali emergano elementi di criticità rispetto all'osservanza del Modello;
- esistenza di situazioni di conflitto d'interesse tra uno dei destinatari del Modello ed EIH;
- infortuni sul lavoro, ovvero provvedimenti assunti dalle Autorità in materia di salute e sicurezza sul lavoro;
- notizie dalle quali si evinca la violazione di dati personali custoditi da EIH.

Oltre alle notizie comunicate in modo occasionale, l'OdV accede in modo sistematico alle informazioni concernenti:

- variazioni organizzative e procedurali significative ai fini del Modello;
- articolazione dei poteri e sistema di deleghe adottato e relative modifiche;
- richiesta, erogazione e gestione di eventuali finanziamenti pubblici;
- eventuali transazioni di natura finanziaria e commerciale fatte in Paesi con normativa fiscale privilegiata;
- attività di formazione svolta in attuazione del Modello;
- procedure a presidio della salute e sicurezza sul lavoro;
- eventuali infortuni verificatisi in EIH e i così detti "quasi-infortuni" che, pur non avendo dato luogo ad eventi lesivi per i lavoratori, possano considerarsi sintomatici di debolezze o lacune del sistema di salute e sicurezza sul lavoro;
- prevenzione di comportamenti illeciti nell'utilizzo degli strumenti e sistemi informatici e nel trattamento dei dati.

Con riferimento all'ultimo punto, l'aumento del lavoro da remoto a seguito della pandemia da covid 19 ha causato un innalzamento del rischio di reati informatici nelle fattispecie contemplate dal Decreto, che saranno presi in considerazione nel Modello.

1.1.4 Aggiornamento del Modello

A norma dell'art. 6 del Decreto, il Consiglio di Amministrazione sovrintende all'aggiornamento e adeguamento del Modello, d'intesa con l'OdV e avvalendosi della collaborazione di Risorse Umane e delle altre strutture competenti.

Gli eventi che potranno essere presi in considerazione ai fini dell'aggiornamento o adeguamento del Modello, a titolo esemplificativo, sono riconducibili a:

- novità legislative;
- riscontri di carenze, lacune e violazioni significative del Modello a seguito di verifiche sull'efficacia del medesimo;
- cambiamenti significativi della struttura organizzativa;
- considerazioni derivanti dall'applicazione del Modello.

2 PARTE SPECIALE: DIVERSE TIPOLOGIE DI REATO, AREE A RISCHIO PER ATTIVITÀ DI ELIS INNOVATION HUB S.R.L.

2.1 REATI CONTRO LA PUBBLICA AMMINISTRAZIONE E L'AMMINISTRAZIONE DELLA GIUSTIZIA

Questa parte del Modello è finalizzata alla prevenzione dei reati contemplati negli articoli 23, 24 e 25 del Decreto, che presuppongono l'esistenza di rapporti con la Pubblica Amministrazione, intesa in senso lato e comprendente anche quella di Stati esteri:

- truffa aggravata a danno dello Stato o di altro ente pubblico,
- truffa aggravata per il conseguimento di erogazioni pubbliche,
- malversazione a danno dello Stato,
- indebita percezione di erogazioni a danno dello Stato,
- frode informatica a danno dello Stato o di altro ente pubblico,
- concussione,
- corruzione,
- induzione indebita a dare o promettere utilità,
- peculato,
- inosservanza delle sanzioni interdittive,
- traffico di influenze illecite,
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria,
- favoreggiamento personale,
- impiego di cittadini di Paesi terzi il cui soggiorno è irregolare.

2.1.1 Aree a rischio reato, principi generali di comportamento e controlli preventivi

Le aree di attività considerate a rischio in relazione ai reati contro la Pubblica Amministrazione sono ritenute le seguenti.

1. Negoziazione, stipula e gestione di contratti con la Pubblica Amministrazione.
2. Gestione dei finanziamenti pubblici o agevolati.
3. Gestione dei rapporti con istituzioni, enti pubblici e organismi di controllo, in particolare per quanto riguarda adempimenti, autorizzazioni, licenze, ispezioni e visite da parte di delegazioni degli enti stessi.
4. Gestione dei rapporti con enti certificatori, nazionali e internazionali, di natura pubblica.
5. Gestione dei rapporti con l'Amministrazione Finanziaria (calcolo delle imposte, elaborazione dei modelli fiscali, ecc.).
6. Gestione di finanza e tesoreria, contabilità e bilancio.
7. Approvvigionamento di beni e servizi.
8. Gestione dei rapporti con la Pubblica Amministrazione per adempimenti connessi all'amministrazione del personale.
9. Gestione dei contratti di consulenza e prestazione professionale.
10. Selezione, assunzione, valutazione e incentivazione del personale.

11. Amministrazione del personale, gestione delle missioni e dei rimborsi spese.
12. Gestione del contenzioso e coinvolgimento in procedimenti giudiziali e arbitrali.
13. Pianificazione e controllo.

Principi generali di comportamento

In conformità alle normative vigenti, ai principi contenuti nel Codice Etico e alle procedure aziendali, per tutti i destinatari del presente Modello che si trovano a operare nelle suddette aree è vietato:

- assumere comportamenti tali da integrare i reati considerati, anche in forma di concorso o tentativo o tali da agevolarne la commissione;
- assumere comportamenti tali da favorire qualsiasi situazione di conflitto di interessi nei confronti di esponenti della Pubblica Amministrazione;
- effettuare dazioni di denaro a esponenti della Pubblica Amministrazione o accordare vantaggi di qualsiasi natura (promesse di assunzione, utilizzo di beni aziendali, ecc.) eccedenti le normali pratiche commerciali o di cortesia;
- effettuare pagamenti in contanti o in natura e pagamenti di facilitazione (spesso utilizzati presso le amministrazioni di Paesi esteri) allo scopo di favorire prestazioni comunque dovute da parte di esponenti della Pubblica Amministrazione;
- riconoscere compensi o effettuare prestazioni in favore dei partner commerciali e collaboratori esterni, che non trovino adeguata giustificazione in relazione al rapporto con gli stessi;
- fornire, in qualsiasi forma, informazioni non veritiere o incomplete alla Pubblica Amministrazione;
- condizionare in qualsiasi forma e con qualsiasi mezzo soggetti chiamati a rendere dichiarazioni all'Autorità Giudiziaria;
- destinare somme ricevute dalla Pubblica Amministrazione a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli ai quali erano destinate;
- prestarsi ad attività di utilizzazione o intermediazione illecita di manodopera, consentendo al committente di utilizzare il lavoro di personale non assunto direttamente, ma dipendente e retribuito da altri.

Facendo riferimento alle suddette aree sensibili, a titolo esemplificativo, sono di seguito commentate le modalità attraverso le quali i reati stessi possono essere commessi e i principi generali di controllo preventivo.

Area a rischio 1

Negoziazione, stipula e gestione di contratti con la Pubblica Amministrazione

Attività sensibili/modalità di commissione dei reati

Negoziazione e stipula del contratto. EIH, per ottenere una commessa o condizioni contrattuali più vantaggiose:

- potrebbe offrire o promettere indebite utilità ai Pubblici Ufficiali o Incaricati di Pubblico Servizio;
- potrebbe alterare i documenti di partecipazione e fornire una falsa rappresentazione della realtà per indurre la Pubblica Amministrazione a prendere decisioni che altrimenti non avrebbe preso.

Controlli preventivi

- Identificazione formale, mediante il sistema di procure, dei soggetti che possono rappresentare EIH e intrattenere rapporti con la Pubblica Amministrazione, italiana ed estera;
- identificazione dei soggetti responsabili della predisposizione dell'offerta;
- formalizzazione di accordi con i partner in caso di partecipazione a gare in forma congiunta, nei quali sono definite le condizioni che regolano la partecipazione;
- trasparenza nell'identificazione dei sub contraenti, ove previsti, con richiesta di offerte competitive a più sub contraenti in caso di importi significativi della sub fornitura;
- segregazione delle funzioni tra i soggetti che predispongono l'offerta e quelli che ne fanno il riesame e la verifica;
- autorizzazione formale, nel rispetto delle deleghe, alla trasmissione dell'offerta;
- autorizzazione formale, nel rispetto delle deleghe, di eventuali variazioni dell'offerta a seguito della negoziazione con il cliente;
- revisione del contratto da parte dell'ufficio legale prima della sottoscrizione;
- sottoscrizione formale, nel rispetto delle procure, del contratto.

Gestione del contratto. EIH potrebbe offrire o promettere indebite utilità ai Pubblici Ufficiali o Incaricati di Pubblico Servizio (inclusi i casi di varianti contrattuali, ritardi o anticipi di consegna, penali, ecc.), per ottenere vantaggi non dovuti nella gestione delle attività contrattuali, ad esempio ottenere il pagamento di una fattura non ancora prevista dal contratto.

Controlli preventivi

- Utilizzo di idonei strumenti di project management;
- monitoraggio della corretta gestione dei contratti;
- sottoscrizione formale, nel rispetto delle procure, del verbale di modifica nel caso in cui il cliente richieda un emendamento del contratto, che non abbia impatto sull'oggetto, sulla durata o sul prezzo;
- sottoscrizione formale, nel rispetto delle procure, dell'atto aggiuntivo al contratto nel caso in cui il cliente richieda un emendamento, che abbia impatto sull'oggetto, sulla durata o sul prezzo;
- identificazione formale dei soggetti responsabili di accettazione e collaudo;
- sottoscrizione formale del verbale di accettazione e collaudo nel rispetto delle deleghe.

Area a rischio 2

Gestione dei finanziamenti pubblici o agevolati

Attività sensibili/modalità di commissione dei reati

- Conseguimento di contributi o finanziamenti mediante artifici e raggiri quali, ad esempio, l'alterazione dei documenti e dei dati attestanti la sussistenza dei requisiti previsti per l'erogazione dei fondi.
- Alterazione della documentazione attestante la destinazione delle somme percepite per destinarle a scopi diversi da quelli stabiliti.

Controlli preventivi

- Segregazione delle funzioni tra chi finalizza il contratto di finanziamento e chi lo autorizza;
- monitoraggio periodico della normativa di riferimento e della presenza di nuovi bandi;
- verifica della completezza e correttezza dei dati contenuti nella richiesta di finanziamento da trasmettere all'ente finanziatore e della loro rispondenza a quanto stabilito dal bando di gara;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, dell'istanza di finanziamento;
- sottoscrizione del contratto di finanziamento, nel rispetto delle deleghe e delle procure;
- definizione di un piano di rendicontazione;
- segregazione di funzioni tra chi raccoglie ed elabora le informazioni e i dati contenuti nella rendicontazione, chi li verifica e li trasmette all'ente finanziatore;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, dei dati e della documentazione sulla rendicontazione da trasmettere all'ente finanziatore;
- verifica dell'incasso ottenuto rispetto agli importi previsti dal finanziamento;
- archiviazione della documentazione.

Area a rischio 3

Gestione dei rapporti con istituzioni, enti pubblici e organismi di controllo, in particolare per quanto riguarda adempimenti, autorizzazioni, licenze, ispezioni e visite da parte di delegazioni degli enti stessi

Attività sensibili/modalità di commissione dei reati

- Trasmissione di documentazione non veritiera a istituzioni, enti pubblici e organismi di controllo, anche in caso di richiesta d'informazioni o chiarimenti.
- Promessa di un'utilità indebita a un Pubblico Funzionario o Incaricato di Pubblico Servizio in occasione della verifica dell'ottemperanza alle prescrizioni stabilite o di un accertamento ispettivo.

Controlli preventivi

- Rispetto di ruoli, compiti e responsabilità stabiliti dall'organigramma aziendale nella gestione dei rapporti con istituzioni, enti pubblici e organismi di controllo;
- identificazione formale dei Pubblici Ufficiali o Incaricati di Pubblico Servizio che accedono nelle sedi aziendali;
- correttezza, tempestività, trasparenza e spirito di collaborazione nei confronti dei Pubblici Ufficiali o Incaricati di Pubblico Servizio, agevolandone l'attività e fornendo le informazioni e i dati eventualmente richiesti per lo svolgimento dei loro compiti in maniera completa e corretta;
- assicurazione del coordinamento di tutte le strutture interessate e delegate in caso d'ispezione delle Autorità di controllo, affinché sia garantita la più completa e tempestiva collaborazione.

Area a rischio 4

Gestione dei rapporti con enti certificatori, nazionali e internazionali, di natura pubblica

Attività sensibili/modalità di commissione dei reati

- Trasmissione di documentazione non veritiera a enti certificatori di natura pubblica per facilitare il rilascio o rinnovo della certificazione, anche in relazione alla richiesta d'informazioni o chiarimenti.
- Promessa di utilità a un esponente di un ente certificatore di natura pubblica che, in violazione dei propri obblighi, attesta falsamente il rispetto delle norme di riferimento in sede di rilascio o rinnovo della certificazione.

Controlli preventivi

- Rispetto di ruoli, compiti e responsabilità stabiliti dall'organigramma aziendale nella gestione dei rapporti con enti di certificazione di natura pubblica;
- correttezza, tempestività, trasparenza e spirito di collaborazione, agevolando l'attività dell'ente e fornendo le informazioni e i dati eventualmente richiesti in adempimento dei compiti dell'ente medesimo;
- assicurazione, in caso d'ispezione dell'ente certificatore, del coordinamento di tutte le strutture interessate e delegate, affinché sia garantita la più completa e tempestiva collaborazione.

Area a rischio 5

Gestione dei rapporti con l'Amministrazione Finanziaria (calcolo delle imposte, elaborazione dei modelli fiscali, ecc.)

Attività sensibili/modalità di commissione dei reati

- Trasmissione di dichiarazioni non complete o non veritiere per ottenere un beneficio derivante dal pagamento di contributi inferiori rispetto al dovuto a danno dello Stato.
- Promessa di un'utilità indebita a un Pubblico Ufficiale o Incaricato di Pubblico Servizio in occasione di un'ispezione per la verifica dell'ottemperanza alle prescrizioni fiscali.

Controlli preventivi

- Identificazione formale dei soggetti deputati a rappresentare EIH e a intrattenere rapporti con l'Amministrazione Finanziaria, anche in sede d'ispezioni e accertamenti;
- monitoraggio dell'evoluzione della normativa di riferimento per garantire l'adeguamento alle novità in materia fiscale;
- segregazione dei compiti tra chi predispone la documentazione da trasmettere all'Amministrazione Finanziaria, chi la controlla e ne autorizza l'invio;
- monitoraggio delle tempistiche da rispettare per comunicazioni e adempimenti verso l'Amministrazione Finanziaria;
- completa, corretta e trasparente trasmissione delle informazioni e dei dati per assolvere gli adempimenti richiesti dall'Amministrazione Finanziaria;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, al pagamento delle imposte correnti.

Area a rischio 6

Gestione di finanza e tesoreria, contabilità e bilancio

Attività sensibili/modalità di commissione dei reati

- Disposizioni d'incasso per un importo inferiore a quanto dovuto a favore di un Pubblico Ufficiale o Incaricato di Pubblico Servizio per ottenere indebiti vantaggi.
- Gestione degli incassi e dei pagamenti finalizzata a creare disponibilità extracontabili da destinare a scopi non corretti nei confronti di Pubblici Ufficiali o Incaricati di Pubblico Servizio.
- Prelievi dalla cassa per spese fittizie o per ammontare diverso da quello delle spese effettivamente sostenute per creare disponibilità extracontabili per scopi non corretti.
- Contabilizzazione di fatti non rispondenti al vero per creare disponibilità finanziarie da utilizzare a scopi non corretti (ad esempio fatturazione per prestazioni inesistenti, sopravalutazione di beni di EIH, contabilizzazione di costi per beni e servizi non forniti, registrazione di operazioni inesistenti, ecc.).

Controlli preventivi

- Autorizzazione formale, nel rispetto delle deleghe e delle procure, delle operazioni sui conti correnti di EIH;
- controlli formali per accertare la completezza e validità della documentazione intercorsa con l'Istituto Bancario;

- limitazione degli accessi al sistema di homebanking tramite l'assegnazione di credenziali personali di accesso (username, password) e token ai procuratori aziendali;
- monitoraggio del sistema di homebanking per accertare la corrispondenza tra gli incassi, i pagamenti e la distinta di supporto;
- definizione formale delle modalità di determinazione del fabbisogno finanziario, sulla base delle previsioni d'incasso e di spesa;
- monitoraggio della correttezza delle transazioni dal sistema di gestione della tesoreria al sistema di contabilità generale;
- controllo che i bonifici siano autorizzati dai procuratori abilitati;
- in caso di pagamenti all'estero, verifica che il conto indicato dal fornitore non risieda in uno Stato considerato a rischio (sulla base delle liste stilate dalle organizzazioni sovranazionali) o con regime fiscale privilegiato, in questi casi il Responsabile Amministrativo dovrà fare le opportune valutazioni;
- definizione delle tipologie di spese che possono essere sostenute tramite cassa, del relativo ammontare massimo e dei soggetti abilitati ad autorizzarle;
- verifica della corrispondenza tra le spese autorizzate e i relativi giustificativi di spesa;
- riconciliazione bancaria e di cassa eseguite periodicamente;
- rispetto dei principi di compilazione dei documenti contabili ai sensi dell'art. 2423 comma 2 c.c.: "Il bilancio deve essere redatto con chiarezza e deve rappresentare in modo veritiero e corretto la situazione patrimoniale della Società e il risultato economico dell'esercizio".

Area a rischio 7

Approvvigionamento di beni e servizi

Attività sensibili/modalità di commissione dei reati

- Qualifica e selezione di fornitori fittizi.
- Qualifica di fornitori legati direttamente o indirettamente alla Pubblica Amministrazione o da questa segnalati, anche se privi dei requisiti di onorabilità e professionalità richiesti, per ottenere indebiti vantaggi.
- Ricorso a fornitori che impiegano personale di Paesi terzi privi di permesso di soggiorno o il cui permesso di soggiorno è scaduto o irregolare o che impiegano minori.
- Gestione impropria degli ordini, dei contratti e delle attività di ricezione di beni e servizi al fine di creare disponibilità extracontabili (ad esempio, sovrafatturazione o fatturazione per operazioni inesistenti).
- Pagamento di prestazioni non dovute o per un importo maggiore rispetto a quello dovuto in favore di fornitori, al fine di indurli a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria.

Controlli preventivi

- Identificazione dei responsabili degli approvvigionamenti e dell'autorizzazione degli ordini di acquisto, nel rispetto delle deleghe e delle procure;

- qualificazione formale e valutazione dei fornitori;
- esistenza di un albo dei fornitori qualificati, aggiornato su base periodica;
- segregazione di funzioni tra chi definisce il budget annuale di spesa di ciascuna unità/ufficio/attività e chi lo approva ed è incaricato della revisione;
- segregazione di funzioni tra chi emette la richiesta di acquisto e chi la controlla, una volta verificata la compatibilità con gli standard aziendali;
- motivazione formale degli acquisti extra budget e relativa autorizzazione;
- invio della richiesta di offerta ad almeno due fornitori, in precedenza qualificati e inseriti nell'albo, per acquisti d'importo superiore alle soglie definite;
- registrazione delle fatture esclusivamente in presenza di un ordine di acquisto approvato e della rispondenza del bene/servizio ricevuto a quanto descritto nell'ordine medesimo;
- divieto di pagamento in contanti per importi superiori a quello previsto dalla normativa vigente;
- controlli, per le attività in Paesi esteri, atti a verificare l'appartenenza del fornitore a Paesi cosiddetti black listed.

Area a rischio 8

Gestione dei rapporti con la Pubblica Amministrazione per adempimenti connessi all'amministrazione del personale

Attività sensibili/modalità di commissione dei reati

- Trasmissione di dichiarazioni non veritiere per il pagamento di contributi inferiore rispetto al dovuto in danno dello Stato.
- Promessa di un'utilità indebita a un Funzionario Pubblico in occasione di un accertamento ispettivo per la verifica dell'ottemperanza alle prescrizioni.

Controlli preventivi

- Rispetto di compiti, ruoli e responsabilità definiti dall'organigramma aziendale nella gestione dei rapporti con la Pubblica Amministrazione connessi ad adempimenti previdenziali e assistenziali;
- identificazione formale dei soggetti autorizzati a rappresentare EIH nei rapporti con gli enti previdenziali e assistenziali, anche in sede d'ispezioni e accertamenti;
- segregazione di funzioni e compiti tra chi predispone la documentazione da inviare alla Pubblica Amministrazione e chi la controlla prima dell'invio;
- monitoraggio costante delle tempistiche da rispettare per comunicazioni e adempimenti nei confronti della Pubblica Amministrazione;
- assenza di comportamenti volti a influenzare indebitamente gli enti previdenziali e assistenziali nell'espletamento degli adempimenti richiesti;

- rispetto di quanto stabilito dagli adempimenti richiesti da enti previdenziali e assistenziali, eventuali criticità o difficoltà vanno evidenziate in forma scritta e gestite dalle strutture competenti nel rispetto delle norme vigenti e delle procedure interne;
- trattamento della documentazione relativa alle richieste degli enti previdenziali e assistenziali in modo da garantirne riservatezza, integrità e disponibilità.

Area a rischio 9

Gestione dei contratti di consulenza e prestazione professionale

Attività sensibili/modalità di commissione dei reati

- Assegnazione di contratti di consulenza a soggetti della Pubblica Amministrazione o a Pubblici Ufficiali, o ad essi riconducibili, al fine di ottenere vantaggi.
- Attribuzione di contratti di consulenza fittizi o riconoscimento di compensi superiori a quelli dovuti a favore di un consulente al fine di compensarne gli indebiti favori o di ottenere un indebito vantaggio.
- Utilizzazione o intermediazione illecita di manodopera. Assegnazione di contratti a EIH per utilizzare il lavoro di personale non assunto direttamente, ma dipendente e retribuito da quest'ultima, prevedendo la sola fornitura di personale per contare su una forza lavoro aggiuntiva per la propria attività e non il compimento dell'opera o la prestazione di un servizio.

Controlli preventivi

- Segregazione di funzioni tra chi richiede la prestazione professionale e chi la valida e l'approva;
- verifica della professionalità e della competenza del professionista (persona fisica o giuridica) riguardo alle specifiche attività da svolgere;
- verifica che non sussistano condizioni d'incompatibilità o conflitto d'interessi (rapporti di parentela, relazioni di carattere personale o professionale) del professionista con i soggetti coinvolti nelle attività oggetto dell'incarico;
- verifica della situazione economico/patrimoniale, societaria e di business (area di attività) del professionista;
- verifica che il professionista non sia residente o non abbia sede in Paesi a regime fiscale privilegiato, individuati in conformità alla normativa fiscale italiana, a meno che il Paese stesso sia il medesimo in cui le prestazioni professionali devono essere svolte;
- verifica, per le attività in Paesi esteri, che il professionista non sia presente nelle liste stilate dalle Organizzazioni internazionali in relazione alle normative antiterrorismo (liste ONU, UE);
- formulazione di una richiesta di offerta competitiva a più professionisti, in base al valore del contratto da sottoscrivere;

- durata contrattuale limitata al tempo necessario e sufficiente per lo scopo prefissato, di regola non superiore a un anno, fatta salva la possibilità di rinnovo o proroga da concordarsi per iscritto alla scadenza, previa valutazione della sussistenza di tutti i requisiti richiesti;
- determinazione dei compensi e dei rimborsi spese commisurata alle prassi vigenti, tenendo conto dell'oggetto delle prestazioni professionali, del territorio o Paese in cui sono svolte, della natura e la durata dell'incarico, del ruolo e delle competenze del professionista;
- pagamento esclusivamente tramite bonifico bancario e a seguito di presentazione delle fatture;
- divieto di pagamento su conti di un Paese diverso da quello in cui il professionista ha la residenza o la sede, che non deve essere un Paese a regime fiscale privilegiato a meno che in tale Paese il professionista abbia sede/residenza e in tale Paese debba essere svolta l'attività;
- divieto di pagamento a favore di persona fisica o giuridica diversa dal professionista cui è stato conferito l'incarico, al di fuori delle scadenze previste contrattualmente e per prestazioni non strettamente attinenti all'incarico;
- sottoscrizione dell'impegno da parte del professionista a eseguire le attività oggetto dell'incarico nel pieno rispetto delle normative applicabili, del Codice Etico e del presente Modello;
- monitoraggio dello svolgimento della prestazione da parte dell'ente richiedente e autorizzazione formale al pagamento delle fatture dopo verifica della prestazione del professionista;
- definizione dell'oggetto contrattuale e del perimetro dell'attività con il committente, sia essa il compimento di un'opera o la prestazione di un servizio;
- accordo con il committente che il personale deve essere impegnato in conformità alle disposizioni concordate nel contratto;
- informazione/formazione del personale sulle attività da svolgere e sui comportamenti corretti da assumere prima che sia inviato presso la sede del committente;
- organizzazione di incontri periodici con il personale per controllare il corretto svolgimento delle attività.

Area a rischio 10

Selezione, assunzione, valutazione e incentivazione del personale

Attività sensibili/modalità di commissione dei reati

- Selezione e assunzione di personale legato direttamente o indirettamente alla Pubblica Amministrazione, quale forma di utilità.
- Selezione e assunzione di cittadini di Paesi terzi privi di permesso di soggiorno o il cui permesso di soggiorno è scaduto o irregolare.
- Definizione e riconoscimento di incrementi retributivi, bonus, fringe benefits e promozioni in deroga alle procedure/prassi in favore di un soggetto legato direttamente o indirettamente alla Pubblica Amministrazione per ottenere vantaggi indebiti.

- Maggiorazione retributiva o concessione di promozioni nei confronti di un dipendente, per indurlo a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria.

Controlli preventivi

- Segregazione tra chi manifesta la necessità di assumere personale e seleziona i candidati e chi ne autorizza l'assunzione;
- definizione formale di un budget delle assunzioni;
- verifica della coerenza dell'assunzione rispetto al budget definito, prima dell'avvio delle attività di selezione;
- definizione delle posizioni delle risorse da assumere e delle relative competenze richieste;
- preliminare ricerca interna di un soggetto adeguato al profilo tracciato;
- eventuale successiva ricerca esterna, previa consultazione delle candidature pervenute;
- definizione formale della tipologia contrattuale e del range salariale relativo alla posizione da ricoprire;
- analisi delle candidature e verifica della loro idoneità attraverso i curricula vitae dei candidati e lo svolgimento di colloqui attitudinali;
- formalizzazione dell'esito della selezione e scelta del candidato;
- verifica della documentazione necessaria all'assunzione del candidato;
- verifica dell'assenza di cause di conflitto d'interessi tra candidato ed EIH;
- verifica, per i candidati stranieri, della validità del passaporto o carta d'identità, del permesso di soggiorno, dell'idoneità alloggiativa del Comune di domiciliazione, codice fiscale;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, della lettera di assunzione;
- definizione formale di un budget degli incentivi;
- segregazione tra chi fa la valutazione delle performance del personale e chi le approva;
- definizione formale degli obiettivi assegnati ai dipendenti in base ai quali sono decisi gli incentivi e i bonus da erogare, nonché gli eventuali avanzamenti di carriera, basata su criteri di specificità, misurabilità e raggiungibilità;
- approvazione formale dell'esito delle valutazioni delle performance del personale;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, dei provvedimenti retributivi e delle promozioni del personale sulla base delle performance.

Area a rischio 11

Amministrazione del personale, gestione delle missioni e dei rimborsi spese

Attività sensibili/modalità di commissione dei reati

- Riconoscimento di stipendi maggiorati rispetto al dovuto per creare disponibilità extracontabili da destinare a scopi non corretti nei confronti di esponenti della Pubblica Amministrazione.
- Rimborsi per spese fittizie o per ammontare diverso da quanto effettivamente sostenuto per creare disponibilità extracontabili per scopi non corretti nei confronti di Pubblici Ufficiali o Incaricati di Pubblico Servizio.
- Omissione di controlli atti ad accertare la regolarità del permesso di soggiorno di cittadini di Paesi extra comunitari impiegati presso EIH.
- Alterazione del permesso di soggiorno di cittadini di Paesi extra comunitari.

Controlli preventivi

- Esistenza di un sistema automatico di rilevazione delle presenze;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, delle disposizioni di pagamento relative alle retribuzioni e agli oneri fiscali e previdenziali;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, delle richieste di ferie/straordinari/permessi o delle omesse timbrature (assenze o trasferte);
- autorizzazione formale, nel rispetto delle deleghe e delle procure, all'esecuzione di trasferte;
- segregazione tra chi verifica le note spese in trasferta e chi ne autorizza il rimborso;
- definizione formale delle tipologie di spese rimborsabili e dei relativi limiti d'importo (viaggio, soggiorno, ecc.);
- verifica dei giustificativi forniti per assicurare la coerenza delle spese sostenute con le attività lavorative svolte;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, dell'eventuale superamento dei limiti d'importo ammessi;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, delle richieste di rimborso delle spese di trasferta.

Area a rischio 12

Gestione del contenzioso e coinvolgimento in procedimenti giudiziali e arbitrali

Attività sensibili/modalità di commissione dei reati

- Selezione di un legale vicino alla Pubblica Amministrazione per ottenere vantaggi per EIH.
- Negoziazione di tariffe professionali fittizie o superiori a quanto dovuto per creare disponibilità extracontabili da destinare a scopi non corretti.
- Dazione di denaro o altra utilità a Pubblico Ufficiale o Incaricato di Pubblico Servizio per favorire EIH in un processo civile, penale o amministrativo.
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria, nel corso di udienze riguardanti procedimenti d'interesse per EIH.

Controlli preventivi

- Rispetto di ruoli, compiti e responsabilità definiti dall'organigramma aziendale;
- monitoraggio dello stato di avanzamento dei contenziosi;
- selezione di legali e consulenti nel rispetto dei criteri di serietà e competenza, che condividano i principi del Codice Etico e il presente Modello;
- monitoraggio dei compensi dei legali incaricati, con evidenza documentale della prestazione ricevuta e delle spese sostenute prima della liquidazione, che permetta di valutare la congruità dell'onorario rispetto al valore della prestazione.

Area a rischio 13

Pianificazione e controllo

Attività sensibili/modalità di commissione dei reati

- Controllo di gestione diretto a nascondere situazioni anomale nell'andamento dei costi o dei ricavi.
- Predisposizione del budget annuale con la finalità di nascondere successive situazioni anomale nell'andamento dei costi o dei ricavi, che potrebbero portare alla creazione di disponibilità extracontabili da destinare a scopi non corretti.

Controlli preventivi

- Identificazione formale dei soggetti coinvolti nel processo di pianificazione e controllo, nonché delle modalità e delle tempistiche dello stesso;
- segregazione tra chi predispone il budget, chi ne monitora e analizza gli scostamenti e chi lo approva (compresi gli eventuali extra budget);
- definizione formale di un budget annuale;
- verifica di completezza delle informazioni riguardanti le singole voci del budget;
- approvazione formale del budget, nel rispetto delle deleghe e delle procure;
- diffusione e comunicazione del budget a tutti gli enti aziendali.

2.1.2 Compiti dell'Organismo di Vigilanza

L'OdV vigila sul funzionamento e sull'osservanza del Modello e ne cura l'aggiornamento al fine di assicurarne l'idoneità e l'efficacia a prevenire i reati di cui alla presente parte.
L'OdV indica integrazioni ai sistemi di gestione al fine di rilevare l'esistenza di eventuali situazioni atipiche e soggette a margini di discrezionalità.

L’OdV vigila sull’evoluzione verso un modello di lavoro agile, compatibile con l’organizzazione aziendale in relazione alle nuove modalità lavorative.
In tale contesto, devono intendersi integralmente richiamati i compiti dell’OdV presentati nella Parte Generale del Modello.

2.2 REATI AMMINISTRATIVI/SOCIETARI

Questa parte del Modello è finalizzata alla prevenzione dei reati contemplati nell'articolo 25 ter del Decreto:

- falsità nelle comunicazioni sociali,
- impedito controllo,
- illegale utilizzo degli utili e delle riserve,
- operazioni in pregiudizio dei creditori,
- omessa comunicazione del conflitto d'interessi,
- formazione fittizia del capitale,
- illecita influenza sull'assemblea,
- ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza.

2.2.1 Aree a rischio reato, principi generali di comportamento e controlli preventivi

Le aree di attività considerate a rischio con riguardo ai reati amministrativi/societari sono ritenute le seguenti:

1. Contabilità e bilancio.
2. Gestione degli adempimenti societari e dei rapporti tra i vari enti che aderiscono al Manifesto ELIS.
3. Gestione della finanza e della tesoreria.

Principi generali di comportamento

In conformità alle normative vigenti, ai principi contenuti nel Codice Etico e alle procedure aziendali, per tutti i destinatari del presente Modello che si trovano a operare nelle suddette aree è vietato:

- assumere comportamenti tali da integrare i reati considerati, anche in forma di concorso o tentativo, o tali da agevolarne la commissione;
- inserire nel bilancio o nelle altre comunicazioni sociali previste dalla legge dati non rispondenti al vero o incompleti sulla situazione economica, patrimoniale o finanziaria di EIH;
- effettuare operazioni volte a creare disponibilità extracontabili per scopi non corretti (ad esempio ricorrendo a fatture per operazioni inesistenti o alla sovra fatturazione);
- impedire od ostacolare in qualunque modo la corretta operatività degli organi sociali, di controllo o dei revisori o recare pregiudizio ai creditori;
- determinare o influenzare illecitamente le delibere dell'assemblea.

Facendo riferimento alle suddette aree sensibili, a titolo esemplificativo, sono di seguito commentate le modalità attraverso le quali i reati stessi possono essere commessi e i principi generali di controllo preventivo.

Area a rischio 1

Contabilità e bilancio

Attività sensibili/modalità di commissione dei reati

- Alterazione dei dati contabili e finanziari con la finalità di produrre informativa economico/patrimoniale/finanziaria non accurata o non veritiera nell'interesse di EIH (sopravalutazione di beni, fatturazioni per forniture inesistenti, contabilizzazione di costi per beni o servizi inesistenti, ecc.).
- Ostacolo allo svolgimento delle attività di controllo attraverso l'occultamento di documenti riguardanti le vicende contabili di EIH o attraverso la mancata archiviazione della documentazione.
- Esposizione in bilancio di valori inesistenti o difformi da quelli reali.

Controlli preventivi

- Rispetto dei ruoli e responsabilità definiti dall'organigramma aziendale, dal sistema autorizzativo e dalle procedure vigenti nella gestione della contabilità e del bilancio;
- rispetto dei principi di compilazione dei documenti contabili ai sensi dell'art. 2423 comma 2 c.c., a norma del quale "il bilancio deve essere redatto con chiarezza e deve rappresentare in modo veritiero e corretto la situazione patrimoniale della Società e il risultato economico dell'esercizio".

Area a rischio 2

Gestione degli adempimenti societari e dei rapporti tra i vari enti che aderiscono al Manifesto ELIS

Attività sensibili/modalità di commissione dei reati

- Ostacolo allo svolgimento delle attività di controllo, attraverso l'occultamento di documenti riguardanti le vicende contabili di EIH o la mancata archiviazione della documentazione.
- Realizzazione di operazioni societarie in presenza di conflitto d'interessi degli Amministratori.
- Effettuazione di operazioni aventi per oggetto accensione e/o erogazione di finanziamenti tra enti del perimetro ELIS a condizioni non in linea con il mercato corrente.
- Porre in essere azioni e/o operazioni tra gli enti del perimetro ELIS al solo scopo di contabilizzare maggiori poste positive o minori poste negative in bilancio.

Controlli preventivi

- Rispetto dei compiti, ruoli e responsabilità definiti dall'organigramma aziendale e dal sistema autorizzativo nella gestione degli adempimenti societari;
- monitoraggio periodico degli aggiornamenti normativi in materia societaria;

- definizione formale delle modalità di convocazione e svolgimento dell'assemblea;
- definizione formale delle modalità di predisposizione, approvazione e conservazione della documentazione riguardante gli atti societari;
- messa a disposizione del Collegio Sindacale e della Società di revisione dei documenti gestionali per le verifiche proprie dei due organismi;
- esecuzione di verifiche e interventi da parte dei titolari degli uffici preposti ai controlli e dell'organo sindacale e di revisione;
- rispetto dei ruoli e delle modalità per l'accesso ai libri sociali (preventiva verifica della legittimazione del richiedente, rispetto della riservatezza, dell'integrità e della disponibilità dei libri medesimi, documentazione attestante l'attività svolta);
- rispetto dei principi alla base della redazione del bilancio rispondenti all'integrità, veridicità, universalità e correttezza dei dati contabili risultanti a fine esercizio.

Area a rischio 3

Gestione della finanza e della tesoreria

Attività sensibili/modalità di commissione dei reati

- Gestione non corretta degli incassi per alterare o non fornire l'informativa economico-finanziaria.
- Mancata o errata contabilizzazione di pagamenti o registrazione di pagamenti non corrispondenti al vero (destinatari fittizi o non coincidenti con i destinatari reali, prestazioni non ricevute), per alterare o non fornire l'informativa economico-finanziaria.

Controlli preventivi

- Autorizzazione formale, nel rispetto delle deleghe e delle procure, delle operazioni sui conti correnti;
- controlli formalizzati per accertare la completezza e validità della documentazione intercorsa con l'Istituto Bancario;
- limitazione degli accessi al sistema di homebanking tramite l'assegnazione di credenziali personali di accesso (username, password) e token ai procuratori aziendali;
- monitoraggio del sistema di homebanking per accertare la corrispondenza tra incassi, pagamenti e la documentazione di supporto;
- definizione formale delle modalità di determinazione del fabbisogno finanziario, sulla base delle previsioni d'incasso e di spesa;
- monitoraggio della correttezza delle transazioni dal sistema di gestione della tesoreria al sistema di contabilità generale;
- controlli atti ad accertare che i bonifici siano autorizzati dai procuratori abilitati;
- in caso di operazioni all'estero, verifica che il conto indicato dal fornitore non risieda in uno Stato considerato a rischio (sulla base delle liste stilate dalle organizzazioni sovranazionali)

o con regime fiscale privilegiato; in questi casi il Responsabile Amministrativo dovrà fare le opportune valutazioni;

- riconciliazioni bancarie e di cassa eseguite periodicamente;
- definizione formale delle tipologie di spese che possono essere sostenute tramite cassa, del relativo ammontare massimo e dei soggetti abilitati ad autorizzarle;
- verifica della corrispondenza tra le spese autorizzate e i relativi giustificativi.

2.2.2 Compiti dell'Organismo di Vigilanza

L'OdV vigila sul funzionamento e sull'osservanza del Modello e ne cura l'aggiornamento al fine di assicurarne l'idoneità e l'efficacia a prevenire i reati di cui alla presente parte. In tale contesto, oltre ai compiti presentati nella parte introduttiva del Modello, l'OdV dovrà altresì:

- verificare periodicamente i requisiti d'indipendenza della Società di revisione;
- verificare l'evenienza di situazioni tese all'adozione di iniziative e atti volti a creare utilità e vantaggi indebiti a favore di un altro ente del perimetro ELIS;
- indicare integrazioni ai sistemi di gestione finanziaria e contabile, al fine di rilevare l'esistenza di eventuali flussi finanziari atipici e soggetti a margini di discrezionalità.

L'OdV vigila sull'evoluzione verso un modello di lavoro agile, compatibile con l'organizzazione aziendale in relazione alle nuove modalità lavorative.

2.3 CORRUZIONE TRA PRIVATI

La legge 6 novembre 2012, n. 190, adeguando il nostro ordinamento a una serie di obblighi internazionali e nell'ambito di una più ampia riforma dei delitti di corruzione, ha introdotto nel novero dei reati presupposto della responsabilità dell'ente il reato di corruzione tra privati di cui all'art. 2635 c.c.

2.3.1 Aree a rischio reato, principi generali di comportamento e controlli preventivi

Il reato di corruzione tra privati ha come presupposto l'instaurazione di rapporti, diretti o indiretti, con soggetti privati in forma di Società o Consorzi.

Tenuto conto della molteplicità dei rapporti che EIH intrattiene con soggetti privati, sono state individuate le seguenti aree di attività ritenute maggiormente a rischio:

1. Negoziazione, stipula e gestione dei contratti con soggetti privati.
2. Gestione dei rapporti con enti certificatori nazionali e internazionali.
3. Gestione dei rapporti con istituzioni e operatori finanziari.
4. Gestione di finanza e tesoreria, contabilità e bilancio.
5. Approvvigionamento di beni e servizi.
6. Gestione dei contratti di consulenza e prestazione professionale.
7. Selezione, assunzione, valutazione e incentivazione del personale.
8. Amministrazione del personale, gestione delle missioni e dei rimborsi spese.
9. Gestione del contenzioso e coinvolgimento in procedimenti giudiziali o arbitrali.
10. Gestione della comunicazione e dei rapporti con i media.

Principi generali di comportamento

In conformità alle normative vigenti, ai principi contenuti nel Codice Etico e alle procedure aziendali, per tutti i destinatari del presente Modello che si trovano a operare nelle suddette aree è fatto divieto di:

- porre in essere comportamenti tali da integrare il reato di corruzione tra privati, anche nella forma di concorso o tentativo, o tali da agevolarne la commissione;
- porre in essere comportamenti non conformi alle normative vigenti, alle procedure aziendali o, comunque, non in linea con i principi espressi dal Codice Etico e dal presente Modello;
- fare dazioni di denaro o accordare vantaggi di qualsiasi natura (promesse di assunzione, utilizzo di beni aziendali, ecc.) in favore di esponenti di altre Società private che possano indurre un vantaggio indebito per EIH;
- fare dazioni di denaro o riconoscere altre utilità in favore di fornitori o collaboratori e consulenti, che non trovino adeguata giustificazione nel rapporto con gli stessi e che possano indurre un vantaggio indebito per EIH.

Facendo riferimento alle suddette aree sensibili, a titolo esemplificativo, sono di seguito commentate le modalità attraverso le quali i reati stessi possono essere commessi e i principi generali di controllo preventivo.

Area a rischio 1

Negoziazione, stipula e gestione dei contratti con soggetti privati

Attività sensibili/modalità di commissione dei reati

Negoziazione e stipula del contratto. EIH, al fine di ottenere l'aggiudicazione di un contratto, potrebbe offrire o promettere denaro o altre utilità a persone di una Società cliente o a persone o Società a esse collegate, affinché preferiscano EIH rispetto a una Società concorrente.

Controlli preventivi

- Formalizzazione dell'opportunità di predisporre l'offerta;
- identificazione dei soggetti responsabili della predisposizione dell'offerta;
- identificazione formale dei soggetti autorizzati a intrattenere rapporti con il cliente;
- segregazione delle funzioni tra i soggetti che predispongono l'offerta e chi ne fa la verifica, il riesame e l'autorizza;
- trasparenza e oggettività nell'identificazione degli eventuali sub fornitori (richiesta di offerte competitive a più sub fornitori in base agli importi della subfornitura, valutazione tecnico-economica delle offerte dei sub fornitori);
- verifica della documentazione riguardante la proposta di offerta per assicurare che sia coerente con la richiesta della medesima;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, della trasmissione dell'offerta al cliente;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, di eventuali variazioni dell'offerta a seguito della negoziazione con il cliente, che determinano la reiterazione del processo di predisposizione di offerta;
- supporto dell'Ufficio Legale per la definizione dei contratti e in particolare per le condizioni contrattuali non standard;
- autorizzazione formale del contratto, nel rispetto delle deleghe e delle procure.

Gestione del contratto. EIH potrebbe offrire o promettere denaro o altre utilità a persone di una Società cliente per ottenere una gestione favorevole e non dovuta delle attività contrattuali (ritardi/anticipi di consegna, penali, ecc.).

Controlli preventivi

- Utilizzo di idonei strumenti di project management;
- monitoraggio periodico della corretta gestione dei contratti;
- sottoscrizione formale, nel rispetto delle procure, degli atti di modifica nel caso in cui il cliente richieda un emendamento del contratto;

- verifica della completezza e della congruità dei requisiti di progetto/prodotto/servizio rispetto a quanto stabilito a livello contrattuale;
- identificazione formale dei soggetti responsabili di accettazione e collaudo;
- sottoscrizione formale del verbale di accettazione e collaudo nel rispetto delle deleghe e delle procure.

Area a rischio 2

Gestione dei rapporti con enti certificatori nazionali e internazionali

Attività sensibili/modalità di commissione dei reati

Offerta o promessa di utilità a un esponente di un ente certificatore, affinché compia atti contrari ai propri doveri per agevolare o consentire il rilascio o rinnovo della certificazione, attestando falsamente il rispetto delle norme di riferimento.

Controlli preventivi

- Rispetto di compiti, ruoli e responsabilità definiti dall'organigramma aziendale e dal sistema autorizzativo nella gestione dei rapporti con enti certificatori;
- correttezza, tempestività, trasparenza e spirito di collaborazione, agevolando l'attività dell'ente certificatore e fornendo le informazioni e i dati eventualmente richiesti in adempimento dei compiti dell'ente medesimo;
- assicurazione, in caso d'ispezione dell'ente certificatore, del coordinamento di tutte le strutture interessate e delegate, affinché sia garantita la più ampia e tempestiva collaborazione, fornendo dati e documenti richiesti e non ponendo alcun ostacolo alle attività di vigilanza (comportamenti ostruzionistici, risposte reticenti o incomplete, ritardi pretestuosi).

Area a rischio 3

Gestione dei rapporti con istituzioni e operatori finanziari

Attività sensibili/modalità di commissione dei reati

Gestione dei rapporti con istituzioni finanziarie e operatori bancari per la richiesta di finanziamenti: EIH potrebbe avere interesse a ottenere finanziamenti o fideiussioni a condizioni particolarmente vantaggiose, ricompensando con denaro o altra utilità il soggetto a ciò prestatosi.

Controlli preventivi

- Rispetto di compiti, ruoli e responsabilità definiti dall'organigramma aziendale e dal sistema autorizzativo nella gestione dei rapporti con istituzioni e operatori finanziari;
- correttezza e trasparenza nei rapporti con le istituzioni e gli operatori finanziari, non influenzando impropriamente le decisioni della controparte e non richiedendo trattamenti di favore, divieto di promettere, erogare o ricevere somme e benefici di qualsiasi natura;

- completezza e veridicità delle informazioni e dei dati trasmessi a istituzioni e operatori finanziari;
- definizione formale delle modalità di formazione, controllo e diffusione di comunicazioni sociali, studi, ricerche, piani strategici e finanziari e altre informazioni rilevanti relative a EIH.

Area a rischio 4

Gestione di finanza e tesoreria, contabilità e bilancio

Attività sensibili/modalità di commissione dei reati

- Gestione della contabilità generale, gestione della contabilità fornitori, clienti, dipendenti e collaboratori esterni, chiusura, redazione e approvazione del bilancio: creazione di documentazione contabile/patrimoniale/finanziaria non veritiera per creare disponibilità extracontabili, dare o promettere denaro o altra utilità a soggetti di una Società, al fine di far compiere od omettere atti che cagionino nocumento alla Società di appartenenza.
- Gestione delle operazioni sui conti correnti finalizzate alla creazione di disponibilità extracontabili da destinare a scopi non corretti.
- Gestione degli incassi e dei pagamenti per creare disponibilità extracontabili da destinare a scopi non corretti.
- Gestione della cassa per creare disponibilità economiche occulte da destinare a esponenti di altre Società per ottenere vantaggi indebiti.

Controlli preventivi

- Autorizzazione formale, nel rispetto delle deleghe e delle procure, delle operazioni sui conti correnti;
- controlli formali atti ad accertare la completezza e validità della documentazione intercorsa con l'Istituto Bancario;
- limitazione degli accessi al sistema di homebanking tramite l'assegnazione di credenziali personali di accesso (username, password) e token ai procuratori aziendali;
- monitoraggio del sistema di homebanking per accertare la corrispondenza tra gli incassi e i pagamenti e la documentazione di supporto;
- definizione formale delle modalità di determinazione del fabbisogno finanziario sulla base delle previsioni d'incasso e di spesa;
- monitoraggio della correttezza delle transazioni dal sistema di gestione della tesoreria al sistema di contabilità generale;
- controllo che i bonifici siano autorizzati dai procuratori abilitati;
- in caso di operazioni all'estero, verifica che il conto indicato dal fornitore non risieda presso uno Stato considerato a rischio (sulla base delle liste fornite dalle organizzazioni sovranazionali) o con regime fiscale privilegiato, in questi casi il Responsabile Amministrativo dovrà fare le opportune valutazioni;

- definizione delle tipologie di spese che possono essere sostenute tramite cassa, del relativo ammontare massimo e dei soggetti abilitati ad autorizzarle;
- verifica della corrispondenza tra le spese autorizzate e i relativi giustificativi;
- riconciliazione bancaria e di cassa eseguite periodicamente;
- rispetto dei principi di compilazione dei documenti contabili ai sensi dell'art. 2423 comma 2 c.c.: "Il bilancio deve essere redatto con chiarezza e deve rappresentare in modo veritiero e corretto la situazione patrimoniale della Società e il risultato economico dell'esercizio".

Area a rischio 5

Approvvigionamento di beni e servizi

Attività sensibili/modalità di commissione dei reati

- Verifica della contabilità fornitori, clienti e collaboratori esterni e dell'assenza di contabilizzazione di fatti non rispondenti al vero per creare disponibilità finanziarie da utilizzare per scopi non corretti (ad esempio fatturazione per prestazioni inesistenti, sopravalutazione di beni, contabilizzazione di costi per beni e servizi non forniti, ecc.).
- Verifica delle operazioni di chiusura del bilancio (omessa o infedele registrazione di dati anagrafici e/o contabili per la creazione di disponibilità extracontabili).

Controlli preventivi

- Identificazione dei soggetti responsabili degli approvvigionamenti e dell'autorizzazione degli ordini di acquisto, nel rispetto delle deleghe e delle procure;
- qualificazione formale e valutazione dei fornitori;
- esistenza di un albo dei fornitori qualificati, aggiornato su base periodica;
- segregazione di funzioni tra chi definisce il budget annuale di spesa di ciascuna unità/ufficio/attività e chi lo approva ed è incaricato della sua revisione;
- segregazione di funzioni tra chi emette la richiesta di acquisto e chi la approva, una volta verificata la compatibilità con gli standard aziendali;
- motivazione formale degli acquisti extra budget e relativa autorizzazione;
- invio della richiesta di offerta ad almeno due fornitori, in precedenza qualificati e inseriti nell'albo, in base al valore del contratto da sottoscrivere;
- registrazione delle fatture esclusivamente in presenza di un ordine di acquisto approvato e della rispondenza del bene/servizio ricevuto a quanto riportato nel medesimo ordine;
- divieto di pagamento in contanti o con altri strumenti al portatore per importi superiori a quanto previsto dalla normativa vigente;
- verifica dell'appartenenza del fornitore a Paesi cosiddetti black listed per attività all'estero.

Area a rischio 6

Gestione dei contratti di consulenza e prestazione professionale

Attività sensibili/modalità di commissione dei reati

- Promessa di denaro o di altra utilità a una Società di consulenza o che fornisce una prestazione professionale al fine di ottenere un indebito vantaggio.
- Attribuzione di contratti di consulenza fittizi a favore di un esponente di una Società concorrente, o di persone fisiche o giuridiche a essa riconducibili, al fine di compensarne gli indebiti favori o di ottenere un indebito vantaggio.
- Utilizzazione o intermediazione illecita di manodopera. Assegnazione di contratti a EIH per utilizzare il lavoro di personale non assunto direttamente, ma dipendente e retribuito da quest'ultima, prevedendo la sola fornitura di personale per contare su una forza lavoro aggiuntiva per la propria attività e non il compimento dell'opera o la prestazione di un servizio.

Controlli preventivi

- Segregazione di funzioni tra chi richiede la prestazione professionale e chi la valida e l'approva;
- verifica della professionalità e della competenza del professionista (persona fisica o giuridica) sulle attività da svolgere;
- verifica che non sussistano condizioni d'incompatibilità o conflitto d'interessi (rapporti di parentela, relazioni di carattere personale o professionale) del professionista con i soggetti coinvolti nelle attività oggetto dell'incarico;
- verifica della situazione economico/patrimoniale, societaria e di business (area di attività) del professionista;
- verifica che il professionista non sia residente o non abbia sede in Paesi a regime fiscale privilegiato, individuati in conformità alla normativa fiscale italiana, a meno che il Paese stesso sia il medesimo in cui le prestazioni professionali devono essere svolte;
- verifica, per attività all'estero, che il professionista non sia presente nelle liste antiterrorismo fornite dalle Organizzazioni internazionali (ONU, UE);
- formulazione di una richiesta di offerta competitiva a più professionisti, in base al valore del contratto da sottoscrivere;
- durata del contratto limitata al tempo necessario e sufficiente per lo scopo prefissato, di regola non superiore a un anno, fatta salva la possibilità di rinnovo o proroga da concordarsi per iscritto alla scadenza, previa valutazione della sussistenza di tutti i requisiti richiesti;
- determinazione dei compensi e dei rimborsi spese commisurata alle prassi vigenti, tenendo conto dell'oggetto delle prestazioni professionali, del territorio o Paese in cui sono svolte, della durata dell'incarico, del ruolo e delle competenze del professionista;
- pagamento esclusivamente tramite bonifico bancario e a seguito di presentazione delle fatture;
- divieto di pagamento su conti di un Paese diverso da quello in cui il professionista ha la residenza o la sede, che non deve essere un Paese a regime fiscale privilegiato a meno che in tale Paese il professionista abbia sede/residenza e in tale Paese debba essere svolta l'attività;

- divieto di pagamento a favore di persona fisica o giuridica diversa dal professionista cui è stato conferito l'incarico, al di fuori delle scadenze previste contrattualmente e/o per prestazioni non attinenti allo svolgimento dell'incarico;
- sottoscrizione dell'impegno da parte del professionista a eseguire le attività oggetto dell'incarico nel pieno rispetto delle normative applicabili, del Codice Etico e del presente Modello;
- monitoraggio dello svolgimento della prestazione da parte dell'ente richiedente e autorizzazione formale al pagamento delle fatture dopo verifica della prestazione del professionista.
- definizione dell'oggetto contrattuale e del perimetro dell'attività con il committente, sia essa il compimento di un'opera o la prestazione di un servizio;
- accordo con il committente che il personale dev'essere impegnato in conformità alle disposizioni del contratto;
- informazione/formazione del personale sulle attività da svolgere e sui comportamenti corretti da assumere prima che sia inviato presso la sede del committente;
- organizzazione di incontri periodici con il personale per controllare il corretto svolgimento delle attività.

Area a rischio 7

Selezione, assunzione, valutazione e incentivazione del personale

Attività sensibili/modalità di commissione dei reati

Selezione e assunzione di soggetti appartenenti a Società competitrici o a queste collegate, con l'obiettivo di far compiere od omettere atti in violazione degli obblighi inerenti al loro ufficio, causando nocumento alla Società competitrice.

Controlli preventivi

- Segregazione tra chi manifesta la necessità di assumere personale e seleziona i candidati e chi ne autorizza l'assunzione;
- definizione formale del budget delle assunzioni;
- verifica della coerenza dell'assunzione rispetto al budget prima dell'avvio delle attività di selezione;
- definizione delle caratteristiche delle posizioni delle risorse umane da assumere e delle relative competenze richieste;
- preliminare ricerca interna di un soggetto adeguato al profilo tracciato;
- eventuale successiva ricerca esterna, previa consultazione dell'archivio delle candidature pervenute;
- definizione formale della tipologia contrattuale e del range salariale relativi alla posizione da ricoprire;
- analisi delle candidature e verifica della loro idoneità attraverso i curricula vitae dei candidati e i colloqui attitudinali;
- formalizzazione dell'esito della selezione e scelta del candidato;

- verifica della documentazione necessaria all'assunzione;
- verifica dell'assenza di cause di conflitto d'interessi tra candidato ed EIH;
- verifica, per i candidati stranieri, della validità del passaporto o carta d'identità, del permesso di soggiorno, dell'idoneità alloggiativa del Comune di domiciliazione, del codice fiscale;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, della lettera di assunzione;
- definizione formale di un budget degli incentivi;
- segregazione tra chi fa la valutazione delle performance del personale e chi l'approva;
- definizione formale degli obiettivi assegnati ai dipendenti in base ai quali sono decisi gli incentivi e i bonus da erogare, nonché gli eventuali avanzamenti di carriera, basata su criteri di specificità, misurabilità e raggiungibilità;
- approvazione formale dell'esito delle valutazioni delle performance del personale;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, dei provvedimenti retributivi e delle promozioni del personale sulla base delle performance.

Area a rischio 8

Amministrazione del personale, gestione delle missioni e dei rimborsi spese

Attività sensibili/modalità di commissione dei reati

Rimborsi per spese fittizie o per ammontare diverso da quello delle spese effettivamente sostenute, per creare disponibilità extracontabili a vantaggio di soggetti di altre Società, perché compiano od omettano atti in violazione degli obblighi inerenti al loro ufficio, causando nocumento alla Società di appartenenza.

Controlli preventivi

- Esistenza di un sistema automatico di rilevazione delle presenze;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, delle disposizioni di pagamento relative alle retribuzioni e agli oneri fiscali e previdenziali;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, delle richieste di ferie/straordinari/permessi o delle omesse timbrature (assenze o trasferte);
- autorizzazione formale, nel rispetto delle deleghe e delle procure, all'esecuzione di trasferte;
- segregazione tra chi verifica le note spese in trasferta e chi ne autorizza il rimborso;
- definizione formale delle tipologie di spese rimborsabili e dei relativi limiti d'importo (viaggio, soggiorno, ecc.);
- verifica dei giustificativi forniti per assicurare la coerenza delle spese sostenute con le attività lavorative svolte;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, dell'eventuale superamento dei limiti d'importo ammessi;

- autorizzazione formale, nel rispetto delle deleghe e delle procure, delle richieste di rimborso delle spese di trasferta.

Area a rischio 9

Gestione del contenzioso e coinvolgimento in procedimenti giudiziali o arbitrali

Attività sensibili/modalità di commissione dei reati

Dazione di denaro o di altra utilità a soggetti di Società controparti, anche attraverso consulenti legali, al fine di garantirsi un esito positivo della controversia.

Controlli preventivi

- Rispetto di ruoli, compiti e responsabilità definiti dall'organigramma aziendale;
- monitoraggio dello stato di avanzamento dei contenziosi;
- selezione di legali e consulenti secondo criteri di serietà e competenza, che condividano i principi del Codice Etico e il presente Modello;
- monitoraggio dei compensi dei legali incaricati, con evidenza documentale della prestazione ricevuta e delle spese sostenute prima della liquidazione, che permetta di valutare la congruità dell'onorario rispetto al valore della prestazione.

Area a rischio 10

Gestione della comunicazione e dei rapporti con i media

Attività sensibili/modalità di commissione dei reati

- Indebite promesse di denaro o di future utilità a esponenti del mondo della comunicazione, al fine di ottimizzare la propria posizione strategica e di promuovere la propria immagine.
- Occultazione di notizie fondatamente negative su EIH.

Controlli preventivi

- Rispetto di compiti, ruoli e responsabilità definiti dall'organigramma aziendale e dal sistema autorizzativo, con riferimento alla gestione dei rapporti con i media;
- correttezza e trasparenza nei rapporti con i media nel rispetto dei principi di veridicità di tutte le informazioni e dei dati trasmessi, non influenzando impropriamente le decisioni dei media;
- divieto di diffondere informazioni ai media e in generale a interlocutori esterni fuorvianti o non rispondenti al vero;
- monitoraggio delle comunicazioni alla stampa o ad altri mezzi d'informazione, per prevenire il rischio di diffusione di notizie false o fuorvianti riguardanti EIH.

2.3.2 Compiti dell'Organismo di Vigilanza

L'OdV vigila:

- sul funzionamento e sull'osservanza del Modello e ne cura l'aggiornamento per assicurarne l'idoneità e l'efficacia a prevenire i reati di cui alla presente parte;
- sull'evoluzione verso un modello di lavoro agile, compatibile con l'attuale organizzazione aziendale, in relazione alle nuove modalità lavorative.

L'OdV indica integrazioni ai sistemi di gestione al fine di rilevare l'esistenza di eventuali situazioni atipiche e soggette a margini di discrezionalità.
In tale contesto, devono intendersi qui integralmente richiamati i compiti attribuiti all'Organismo già dettagliati nella Parte Generale del Modello.

2.4 REATI IN VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

Il presente Modello costituisce parte integrante del sistema di gestione della salute e sicurezza sul lavoro di EIH, al quale fa riferimento.

EIH è tenuta (art. 2087 c.c. e D. Lgs. 81/2008) ad adottare le misure necessarie per tutelare la salute fisica e psichica dei lavoratori in base alla particolarità del lavoro, all'esperienza e alla tecnologia, con l'obiettivo di prevenire e limitare eventi lesivi che possono verificarsi. In tale ottica, EIH s'impegna:

- al rispetto delle normative vigenti in materia di salute e sicurezza sul lavoro;
- a coinvolgere l'intera organizzazione nella gestione attiva della salute e sicurezza sul lavoro;
- a fornire le risorse umane ed economiche necessarie;
- a sensibilizzare e formare i lavoratori per svolgere i loro compiti e assumere le loro responsabilità in materia di salute e sicurezza sul lavoro;
- a diffondere all'interno gli obiettivi di salute e sicurezza sul lavoro e i relativi programmi d'implementazione;
- a monitorare costantemente la salute e sicurezza sul lavoro attraverso la verifica degli obiettivi e del funzionamento del sistema;
- al riesame periodico e al miglioramento continuo del sistema di gestione della salute e sicurezza sul lavoro.

Il Decreto all'articolo 25 septies, primo, secondo e terzo comma, prevede la responsabilità della Società in relazione ai reati di:

- omicidio colposo,
- lesioni personali colpose,

commessi in violazione della normativa in tema di salute e sicurezza sul lavoro.

2.4.1 Aree a rischio reato in tema di salute e sicurezza sul lavoro

Con riferimento ai reati in violazione delle norme sulla tutela della salute e sicurezza sul lavoro, non si può escludere aprioristicamente alcun ambito di attività, perché possono interessare tutte le componenti aziendali e configurarsi trasversali alle varie aree operative. Si ritiene pertanto di valutare tale rischio come **rischio diffuso** nelle sedi di Roma e Catania.

Si considerano le seguenti aree di attività in ordine di rischio violazione delle norme:

- locali tecnici,
- uffici,

affidate alla responsabilità e al controllo di delegati e preposti.

2.4.2 Sistema aziendale per la tutela della salute e sicurezza sul lavoro

EIH ha individuato e implementato un sistema per la tutela della salute e sicurezza sul lavoro, che prevede:

- definizione dei ruoli e delle responsabilità, della formazione, del sistema documentale e delle modalità di controllo operativo delle attività connesse alla tutela della salute e sicurezza sul lavoro;
- definizione e assegnazione delle risorse;
- gestione delle emergenze;
- monitoraggio degli infortuni e degli incidenti;
- riesame periodico della Direzione per valutare se il sistema di tutela della salute e sicurezza sul lavoro è stato completamente realizzato e se è adeguato alla politica e agli obiettivi della Società.

EIH ha articolato la propria organizzazione per la tutela della salute e sicurezza sul lavoro con le figure di seguito indicate, accogliendo quanto previsto dal D. Lgs. 81/2008 e successive modifiche e integrazioni:

- Datore di Lavoro, che approva la politica di salute e sicurezza sul lavoro e i relativi obiettivi, nomina il Responsabile del Servizio Prevenzione e Protezione (RSPP) ed elabora il Documento per la Valutazione dei Rischi (DVR);
- Eventuali Delegati del Datore di Lavoro, quest'ultimo infatti può delegare, con atto formale, parte delle attività a lui attribuite dal D. Lgs. 81/2008 per adottare i provvedimenti di carattere organizzativo, gestionale ed economico per l'applicazione della normativa sulla salute e sicurezza sul lavoro;
- Responsabile del Servizio Prevenzione e Protezione, che fornisce supporto tecnico e normativo in materia di salute e sicurezza sul lavoro e supporta il Datore di Lavoro nella redazione del Documento per la Valutazione dei Rischi;
- Preposti, che verificano che i comportamenti dei Lavoratori siano conformi alle direttive aziendali in materia di salute e sicurezza sul lavoro e segnalano tempestivamente al Datore di Lavoro o al suo Delegato ogni altra condizione di pericolo che si verifichi durante il lavoro, della quale vengano a conoscenza sulla base della formazione ricevuta;
- Medico Competente, che collabora alla valutazione dei rischi ed effettua la sorveglianza sanitaria, a tutela dello stato di salute e della sicurezza dei lavoratori;
- Rappresentante dei Lavoratori per la Sicurezza, è la persona designata a rappresentare i lavoratori per gli aspetti di salute e sicurezza sul lavoro, è consultato preventivamente in merito alla valutazione dei rischi, alla programmazione, realizzazione e verifica della prevenzione;
- Incaricati per la Gestione delle Emergenze, lavoratori addestrati a gestire le situazioni di emergenza quali incendio, evacuazione in caso di pericolo grave e immediato e primo soccorso;
- Lavoratori.

2.4.3 Documento di Valutazione dei Rischi

Il Documento di Valutazione dei Rischi, al quale il presente Modello fa pienamente riferimento, individua e analizza i rischi potenziali in base alla normativa in vigore (D. Lgs. 81/2008) e contiene:

- il procedimento di valutazione dei rischi;
- i rischi riguardanti i luoghi e l'ambiente di lavoro;
- i rischi riguardanti la sicurezza in presenza di attrezzature e impianti;
- i rischi trasversali dovuti a organizzazione del lavoro, fattori psicologici ed ergonomici, condizioni di lavoro difficile;
- l'individuazione delle misure di prevenzione e protezione e dei Dispositivi di Protezione Individuale conseguenti alla valutazione;
- le misure per garantire il miglioramento nel tempo dei livelli di sicurezza.

Particolare attenzione va dedicata a gruppi di lavoratori, non sempre presenti, potenzialmente esposti a rischi particolari indipendentemente dalle mansioni svolte:

- lavoratrici in stato di gravidanza,
- lavoratori portatori di handicap,
- lavoratori temporanei, stagisti o tirocinanti.

Inoltre, EIH s'impegna a prevenire e reprimere comportamenti che possano avere come effetto la mortificazione del dipendente nelle sue capacità e aspettative professionali, ovvero che ne determinino l'emarginazione nell'ambiente di lavoro, il discredito o la lesione dell'immagine.

2.4.4 Rapporti con i fornitori: qualifica, informazione, coordinamento e clausole contrattuali

EIH definisce:

- l'informazione riguardante la tutela della salute e sicurezza sul lavoro che un'impresa appaltatrice aggiudicataria di un ordine deve conoscere e s'impegna a rispettare e a far rispettare ai propri dipendenti;
- le misure per eliminare i rischi dovuti alle interferenze tra i lavoratori appartenenti a diverse imprese coinvolte nell'esecuzione di un'opera;
- le modalità di qualifica dei fornitori, che tiene conto della verifica dei requisiti tecnico-professionali prevista ai sensi dell'art. 90, comma 9, del D. Lgs. 81/2008 e della rispondenza di quanto fornito alle migliori tecnologie disponibili in tema di tutela di salute, sicurezza sul lavoro e alle specifiche di acquisto.

2.4.5 Monitoraggio degli infortuni e incidenti

EIH rileva, traccia e analizza gli infortuni e gli incidenti occorsi[1] e i mancati incidenti[2], che sono comunicati al Datore di Lavoro e al Responsabile del Servizio Prevenzione e Protezione.

2.4.6 Audit

EIH predispone attività di audit e verifica periodica dell'efficienza ed efficacia del sistema di tutela della salute e sicurezza sul lavoro, in particolare definisce:

- l'indipendenza dell'auditor rispetto all'attività che dev'essere auditata;

[1] Eventi che hanno provocato un danno (se il danno prodotto riguarda l'integrità fisica di una persona si parla d'infortunio).
[2] Incidenti che, pur caratterizzati da un elevato potenziale di rischio, non hanno provocato nessun danno o soltanto un danno marginale.

- l'applicazione di azioni correttive nel caso siano rilevati scostamenti rispetto a quanto prescritto dal sistema di tutela della salute e sicurezza sul lavoro o dalle normative applicabili;
- la verifica dell'attuazione e dell'efficacia delle suddette azioni correttive;
- la comunicazione dei risultati dell'audit al Consiglio di Amministrazione e all'Organismo di Vigilanza.

2.4.7 Riesame della Direzione

La Direzione fa periodicamente un riesame dell'efficienza e dell'efficacia del sistema di tutela della salute e sicurezza sul lavoro, che prevede le seguenti attività:

- analisi degli infortuni e incidenti occorsi e dei mancati incidenti;
- analisi degli eventuali scostamenti tra i risultati ottenuti e gli obiettivi programmati;
- analisi dei risultati degli audit;
- stato di avanzamento di eventuali azioni di miglioramento definite nel precedente riesame;
- individuazione degli obiettivi di miglioramento per il periodo successivo e di eventuali modifiche a elementi del sistema di tutela della salute e sicurezza sul lavoro.

2.4.8 Compiti dell'Organismo di Vigilanza

Per quanto concerne la salute e sicurezza sul lavoro, oltre ai compiti già attribuiti ed esposti nella Parte Generale del Modello che devono intendersi qui integralmente richiamati, l'OdV monitora le procedure interne per la prevenzione dei reati in tema di salute e sicurezza sul lavoro come organismo imparziale e indipendente dal settore sottoposto a verifica, tenendo conto dei seguenti flussi informativi:

- segnalazioni di eventuali infortuni e incidenti sul lavoro;
- provvedimenti assunti dall'Autorità Giudiziaria o da altre Autorità in tema di tutela della salute e sicurezza sul lavoro;
- eventuali segnalazioni di qualsiasi dipendente di carenze o inadeguatezze dei luoghi e delle attrezzature di lavoro e di ogni altra situazione di pericolo;
- comunicazioni del Responsabile del Servizio Prevenzione e Protezione sulla pianificazione delle norme antinfortunistiche, su ogni modifica e aggiornamento del Documento di Valutazione dei Rischi e sulle riunioni periodiche di prevenzione e protezione dai rischi (art. 35 D. Lgs. 81/2008);
- comunicazioni su ogni aggiornamento relativo a variazioni organizzative e di responsabilità conferite ai sensi del D. Lgs. 81/2008;
- segnalazioni sulle clausole contrattuali riguardanti la sicurezza nei contratti di appalto e subappalto.

2.5 REATI INFORMATICI - VIOLAZIONE DEL DIRITTO D'AUTORE

L'art. 24 bis del Decreto disciplina la responsabilità amministrativa delle persone giuridiche e fa riferimento ai reati informatici e al trattamento illecito dei dati:

- reati che comportano un danneggiamento informatico (art. 24 bis, comma 1):
  - accesso abusivo a un sistema informatico o telematico,
  - intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche,
  - installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche,
  - danneggiamento di sistemi informatici o telematici, ovvero di informazioni, dati e programmi informatici;
- reati derivanti dalla detenzione o diffusione di codici o programmi atti al danneggiamento informatico (art. 24 bis, comma 2):
  - detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici,
  - diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- reati riguardanti il falso in documenti informatici e frode del soggetto che presta servizi di certificazione di firma elettronica (art. 24 bis, comma 3).

L'art. 25 novies prevede la responsabilità degli enti riguardo ai reati in materia di violazione del diritto d'autore e altri illeciti connessi al suo esercizio.

Con il ricorso al lavoro da remoto a seguito della pandemia da COVID 19 le società potrebbero perdere il controllo dei propri perimetri e assistere, di conseguenza, a un innalzamento del rischio dei reati informatici nelle fattispecie contemplate dal D. Lgs. 231/2001, estese col tempo includendo anche:

- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
- violazione delle norme in materia di protezione del perimetro di sicurezza nazionale cibernetica.

Seguono, a titolo di esempio, alcuni casi tipici di come i reati in argomento potrebbero essere consumati.

- Accesso abusivo a un sistema informatico:
  - della Pubblica Amministrazione o di una banca per modificare i dati relativi alla Società,
  - di un cliente per modificare i dati relativi a una commessa,
  - di potenziali clienti per implementare la propria offerta commerciale o falsare l'esito di una gara,
  - di un qualsiasi ente esterno per acquisire informazioni utili alla propria attività,
  - della Società per effettuare manipolazioni di dati destinati al bilancio.

- Impedimento o interruzione di una comunicazione per ostacolare un concorrente nell'invio della documentazione di una gara in modo da determinarne l'inadempienza.
- Danneggiamento del sistema informatico di un concorrente al fine di impedirne l'attività o comprometterne l'immagine per dimostrarne l'inaffidabilità.
- Danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria nell'interesse della Società.
- Utilizzo abusivo di file tutelati da diritto d'autore per agevolare l'operatività della Società.
- Duplicazione abusiva di un programma informatico per utilizzo nell'operatività corrente.
- Utilizzo abusivo di immagini attinte da fonti esterne per utilizzo in pubblicazioni aziendali o nell'organizzazione di eventi istituzionali.

2.5.1 Aree a rischio reato, principi generali di comportamento e controlli preventivi

I reati sopra considerati hanno come presupposto l'impiego di sistemi e programmi informatici o di opere protette dalle norme sul diritto d'autore. È evidente che tutti i dipendenti EIH utilizzano ordinariamente sistemi e programmi informatici e hanno ampia possibilità di accesso a strumenti e dati informatici e telematici nella loro attività lavorativa. Pertanto, anche in questo caso, si ritiene di non localizzare in specifiche aree il rischio di commissione di detti reati, ma di valutarlo come **rischio diffuso**, in considerazione del fatto che essi potrebbero essere astrattamente posti in essere in qualsiasi ambito di attività, con particolare riferimento a:

- gestione e protezione delle risorse informatiche assegnate ai dipendenti,
- sicurezza fisica, inclusi i cablaggi, i dispositivi di rete, ecc.
- gestione dei profili utente e del processo di autenticazione,
- gestione degli accessi da e verso l'esterno,
- gestione e protezione delle reti,
- gestione degli output di sistema.

Inoltre, non si può escludere l'astratto rischio di duplicazione abusiva e messa a disposizione di programmi per elaboratore a scopo di profitto.

Principi generali di comportamento

In conformità alle normative vigenti, ai principi espressi dal Codice Etico e alle procedure interne, per tutti i destinatari del presente Modello è fatto divieto di assumere comportamenti tali da integrare gli illeciti considerati, anche in forma di concorso o tentativo o tali da agevolarne la commissione. In particolare, è vietato:

- lasciare il proprio computer incustodito e senza protezione password;
- utilizzare password di altri utenti, anche per l'accesso ad aree protette in nome e per conto degli stessi, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi;
- introdurre e/o conservare mediante l'utilizzo di strumenti aziendali, a qualsiasi titolo, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso;

- trasferire all'esterno della Società file o qualsiasi altra documentazione riservata di proprietà della Società stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
- effettuare copie non autorizzate di informazioni riservate e di software;
- prestare o cedere a terzi qualsiasi apparecchiatura informatica di proprietà della Società;
- utilizzare le risorse informatiche a disposizione al di fuori delle prescritte autorizzazioni;
- impiegare sulle risorse della Società prodotti non ufficialmente acquisiti dalla Società stessa;
- alterare documenti elettronici, pubblici o privati, con finalità probatoria;
- aggirare o tentare di aggirare i sistemi di sicurezza aziendali (antivirus, firewall, ecc.);
- accedere abusivamente al sistema informatico aziendale per alterare o cancellare dati e informazioni;
- accedere abusivamente a un sistema informatico di altri soggetti, pubblici o privati, o trattenersi contro la volontà, espressa o tacita, di chi ha il diritto di escluderlo;
- detenere e/o utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al sistema informatico aziendale per acquisire informazioni riservate;
- detenere e/o utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico di altri soggetti, pubblici o privati, per acquisire informazioni riservate;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- installare apparecchiature per intercettare, impedire o interrompere comunicazioni di altri soggetti pubblici o privati;
- svolgere attività di danneggiamento di informazioni, dati, programmi e sistemi informatici o telematici di altri soggetti;
- detenere e/o diffondere indebitamente codici o programmi atti al danneggiamento informatico;
- utilizzare indebitamente la firma elettronica;
- utilizzare programmi software sprovvisti di licenza;
- effettuare il download e il successivo utilizzo di contenuti multimediali protetti dalla legge 633/1941 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio);
- utilizzare, sfruttare, diffondere o riprodurre a qualsiasi titolo, in qualsiasi forma, a scopo di lucro o a fini personali opere dell'ingegno di qualsiasi natura coperte dal diritto d'autore in assenza di una liberatoria e del pagamento dei diritti di proprietà;
- porre in essere comportamenti in contrasto con leggi e regolamenti in materia di protezione e sicurezza di dati personali (in particolare Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e seguente D. Lgs. del 10 agosto 2018, n. 101,

provvedimenti del Garante della Privacy, regolamenti Consob, ecc.), nonché di tutela del diritto d'autore (legge 633/1941 e successive modifiche e integrazioni).

Inoltre, con riguardo all'utilizzo e gestione dei sistemi, strumenti, documenti o dati informatici ovvero di opere di qualsiasi natura coperte dal diritto d'autore, tutti coloro che operano per conto di EIH sono tenuti a:

- utilizzare le risorse informatiche loro assegnate per l'espletamento della propria attività lavorativa;
- custodire con cura le proprie credenziali d'accesso ai Sistemi Informativi evitando che altri soggetti possano venirne a conoscenza;
- garantire la tracciabilità dei documenti prodotti;
- segnalare il furto o lo smarrimento delle risorse informatiche e far pervenire alla Società l'originale della denuncia all'Autorità di Pubblica Sicurezza senza ingiustificato ritardo;
- segnalare ai Sistemi Informativi eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche senza ingiustificato ritardo;
- utilizzare unicamente materiale pubblicitario autorizzato;
- osservare scrupolosamente quanto previsto dalle politiche e procedure di sicurezza aziendali per la protezione e il controllo delle risorse informatiche, per la tutela del diritto d'autore e per la protezione e sicurezza di dati personali.

Controlli preventivi

Ai fini dell'attuazione dei comportamenti di cui sopra:

- è attuato il monitoraggio affinché la gestione della ICT Security e Governance sia adeguata e corretta, al fine di individuare tempestivamente l'esistenza di attività che potrebbero determinare il mancato rispetto delle regole aziendali e la presenza di accessi e dispositivi non autorizzati;
- sono previsti controlli atti a prevenire e/o impedire la realizzazione di illeciti informatici, per esempio attraverso l'installazione di software non previsto o non autorizzato;
- sono previsti controlli per rilevare situazioni anomale;
- i dipendenti, salvo i casi autorizzati, non hanno i diritti di amministratori delle risorse loro affidate allo scopo di prevenire l'istallazione di software non autorizzato;
- sono previsti sistemi di web-filtering per prevenire un uso non autorizzato di internet e non rendere accessibili i contenuti che rientrano automaticamente nelle categorie contrarie ai principi espressi nel Codice Etico;
- sono adottate misure per garantire la sicurezza delle informazioni attraverso la restrizione degli accessi in lettura/scrittura sulla base delle liste di distribuzione, la corretta conservazione dei file, la crittografia;

- i fabbisogni di materiale ICT sono dettagliati nel budget annuale, le esigenze di acquisto contingenti sono valutate dal Responsabile di ciascuna unità organizzativa;
- sono censite le licenze software autorizzate e i fabbisogni di nuove licenze sono dettagliati nel budget annuale, le esigenze di acquisto contingenti sono valutate dal Responsabile di ciascuna unità organizzativa;
- è effettuata l'analisi dei requisiti di sicurezza in fase di modifica dei Sistemi Informativi;
- sono previsti specifici controlli per l'individuazione, prevenzione e ripristino dei sistemi rispetto a virus e vulnerabilità;
- è effettuata la protezione del software critico;
- è regolarmente effettuato il backup di informazioni e software;
- è regolarmente effettuata l'attività di manutenzione dei sistemi;
- sono adottate linee guida sulla protezione dei dati e i criteri per la classificazione delle informazioni (pubbliche, interne, riservate);
- sono previsti programmi di informazione, formazione e sensibilizzazione per il personale al fine di diffondere la consapevolezza dei rischi derivanti da un utilizzo improprio e non responsabile delle risorse informatiche aziendali.

2.5.2 Protocolli a presidio dei reati in oggetto

Policy

Oltre al Codice Etico, EIH ha adottato e pubblicato nella rete interna ERP (Enterprise Resource Planning, raccolta di documenti e servizi interni) il **Disciplinare delle Risorse Informatiche per i Dipendenti e i Collaboratori degli Enti che Aderiscono al Manifesto ELIS**, guida per un utilizzo responsabile delle risorse informatiche aziendali, per prevenire i rischi di tipo informatico e per tutelare i dati personali, al quale il presente Modello fa pienamente riferimento. Tutti i dipendenti e collaboratori titolari di un account sono tenuti a conoscerlo e accettarlo. Ogni revisione richiede una nuova accettazione. È compito di Sistemi Informativi diffonderne la conoscenza e di Risorse Umane farlo rispettare.

Classificazione e controllo dei beni

Sono identificati e classificati gli asset aziendali, ivi inclusi dati e informazioni.

Sicurezza fisica

I locali dove sono ospitati i beni e le apparecchiature informatiche sono messi in sicurezza per prevenire accessi non autorizzati, interferenze e danni.

Controllo degli accessi

Sono disciplinati gli accessi ai Sistemi Informativi, alla rete, ai sistemi operativi, alle applicazioni e alle informazioni. In particolare, sono previsti:

- le liste del personale abilitato all'accesso e le autorizzazioni specifiche dei diversi utenti o categorie di utenti;

- una procedura per accordare e revocare i diritti di accesso a tutti i sistemi e servizi informativi;
- l'autenticazione degli utenti tramite credenziali personali di accesso (user id e password);
- l'accesso ai servizi di rete esclusivamente da parte degli utenti autorizzati;
- la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti;
- la revoca dei diritti di accesso in caso di cessazione del rapporto di lavoro o cambiamento del tipo di rapporto che attribuiva tali diritti;
- il controllo e la tracciabilità degli accessi;
- la chiusura di sessioni inattive dopo un periodo di tempo predefinito;
- la segmentazione della rete per prevenire la violazione delle norme di controllo degli accessi alle applicazioni aziendali.

Crittografia

È adottato un sistema che prevede:

- controlli crittografici per la protezione delle informazioni e gestione delle chiavi crittografiche;
- la tracciatura delle attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
- la gestione dei log che registrano le attività degli utilizzatori e gli eventi concernenti la sicurezza;
- il controllo sui cambiamenti degli elaboratori e dei sistemi.

Gestione degli incidenti e dei problemi di sicurezza informatica

Il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica prevede in particolare:

- appropriati canali per la comunicazione di problemi, incidenti e di ogni debolezza e vulnerabilità dei sistemi e servizi, osservata o potenziale;
- l'analisi della documentazione disponibile e l'individuazione di debolezze e vulnerabilità che potrebbero generare problemi in futuro;
- l'analisi di basi dati contenenti informazioni su errori noti e le soluzioni identificate o implementate per supportare la gestione degli incidenti di sicurezza informatica;
- l'analisi di tutti gli incidenti, singoli e ricorrenti, e l'individuazione delle cause;
- la gestione dei problemi che hanno generato gli incidenti fino alla loro soluzione definitiva;
- l'analisi di report e trend di problemi e incidenti e l'individuazione di azioni preventive.

Comunicazione Istituzionale

La struttura provvede:

- a verificare e raccogliere il materiale promozionale, brochure, cataloghi e presentazioni;
- a mettere a disposizione presentazioni istituzionali ai dipendenti chiamati a partecipare a seminari, convegni o altre iniziative in qualità di relatori;
- a pubblicare notizie e aggiornamenti su tematiche di interesse collettivo sulla rete interna e sul sito.

Risorse Umane

La struttura provvede:

- a valutare l'esperienza delle persone destinate a svolgere attività di ICT, con particolare riferimento alla sicurezza, tenendo conto dei principi etici, della normativa applicabile in materia e della classificazione delle informazioni alle quali i menzionati soggetti avranno accesso;
- a promuovere interventi di formazione e aggiornamento periodici sui comportamenti, sull'uso responsabile delle risorse informatiche e sulla prevenzione in fatto di sicurezza informatica per tutti i dipendenti;
- a rammentare l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (computer, telefoni cellulari, token di autenticazione, ecc.) a tutti i dipendenti e ai terzi al momento della conclusione del rapporto di lavoro e/o del contratto di collaborazione;
- a far revocare i diritti di accesso alle informazioni, ai sistemi e agli applicativi a tutti i dipendenti e ai terzi al momento della conclusione del rapporto di lavoro e/o del contratto di collaborazione o in caso di cambio della mansione svolta.

Audit

Sono previste attività di verifica periodiche dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica e dell'applicazione del Disciplinare delle Risorse Informatiche.

2.5.3 Compiti dell'Organismo di Vigilanza

L'OdV vigila sul funzionamento e sull'osservanza del Modello e ne cura l'aggiornamento, al fine di assicurarne l'idoneità e l'efficacia a prevenire i reati di cui alla presente parte. In tale contesto, in aggiunta ai compiti attribuiti all'Organismo già esposti nella Parte Generale del Modello, che devono intendersi qui integralmente richiamati, l'OdV:

- valuta le informazioni rilevanti ricevute da EIH, con particolare riguardo alla reportistica sul traffico di rete in forma aggregata (fermo restando il rispetto della tutela dei dati personali dei dipendenti), alle variazioni organizzative, alla struttura preposta alla gestione della sicurezza, alle variazioni sulle procedure di sicurezza, alla funzionalità ed efficienza del sito internet;
- verifica l'adeguatezza e l'aggiornamento della documentazione e delle procedure predisposte alla prevenzione degli illeciti informatici e alla tutela del diritto d'autore.

2.6 TRATTAMENTO ILLECITO DEI DATI PERSONALI

EIH, nel rispetto del D. Lgs. 231/2001, s'impegna a creare un ambiente di lavoro che garantisca a tutti, in particolare ai dipendenti e collaboratori, condizioni rispettose della dignità personale e della sicurezza declinata in tutti i suoi aspetti.

In ossequio al rispetto della persona e ai precetti di legge di volta in volta vincolanti, EIH s'impegna alla protezione delle persone fisiche anche con riguardo al trattamento dei dati personali e delle informazioni attinenti alla sfera privata. Allo stesso modo s'impegna a proteggere le opinioni dei propri dipendenti e di quanti interagiscono con essa, adottando regole per vietare l'indebita comunicazione e/o diffusione dei dati in assenza del consenso dell'interessato o comunque delle condizioni di liceità.

Questa parte del Modello è finalizzata alla prevenzione degli illeciti contemplati nel Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (Protezione delle Persone Fisiche con Riguardo al Trattamento dei Dati Personali), d'ora in avanti "Regolamento", e nel D. Lgs. del 10 agosto 2018, n. 101 (Disposizioni per l'adeguamento della normativa nazionale al citato Regolamento Europeo, Modifiche al codice di protezione dei dati personali di cui al D. Lgs. del 30 giugno 2003, n. 196). In particolare, gli illeciti che questa parte intende prevenire sono:

- violazione del diritto alla protezione (pretesa che il trattamento dei propri dati personali avvenga nel rispetto dei diritti, con particolare riferimento alla riservatezza);
- violazione del principio di necessità (la raccolta e il trattamento dei dati personali devono essere limitati ai soli dati necessari e sufficienti);
- violazione del principio di finalità (obbligo per chi effettua la raccolta di far conoscere all'interessato la finalità per la quale i suoi dati personali sono raccolti e trattati);
- violazione del principio di autodeterminazioni informativa (consenso dell'interessato al fatto che i suoi dati personali possano essere oggetto di trattamento e quindi diffusi e conosciuti da altri, l'interessato ha il diritto di consentire o no quel trattamento secondo quanto prevede l'Art. 6 del Regolamento - Liceità del Trattamento);
- violazione dei principi di liceità, correttezza e trasparenza (il trattamento è lecito quando è conforme alla legge, è corretto quando la raccolta dei dati personali avviene in modo trasparente e non mediante artifici o raggiri);
- violazione del principio di precauzione (prevenzione di ogni forma di utilizzo illecito o non corretto dei dati personali, anche per negligenza o imperizia);
- inosservanza delle sanzioni interdittive (provvedimenti dell'Autorità di Controllo, art. 51 del Regolamento);
- traffico di influenze illecite (nei confronti di terzi);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità competente.

I dati personali trattati in violazione della disciplina in materia non possono essere utilizzati. Pertanto, EIH s'impegna ad adottare procedure e misure di sicurezza di tipo organizzativo, fisico e logico adeguate e proporzionate per prevenire ogni trattamento illecito o non corretto dei dati personali ed evitare possibili abusi e violazioni. Non sussistono obblighi generalizzati di adozione di misure minime di sicurezza poiché tale valutazione è rimessa al Titolare in rapporto ai rischi individuati (Art. 32 del Regolamento). EIH deve anche promuovere la consapevolezza dei rischi di

violazione dei dati personali e l'assunzione di comportamenti responsabili in tutti i dipendenti e collaboratori. Di tutto ciò EIH s'impegna a dare informativa all'OdV.

2.6.1 Aree a rischio reato, principi generali di comportamento e controlli preventivi

Le aree di attività considerate a rischio in relazione al trattamento illecito o non corretto dei dati personali sono ritenute le seguenti.

1. Gestione della tipologia dei dati personali trattati.
2. Incaricati del Trattamento dei dati personali.
3. Gestione dell'informativa e del consenso dell'interessato.
4. Misure di sicurezza.
5. Gestione degli incidenti per violazione dei dati personali.

Principi generali di comportamento

In conformità alle normative vigenti, ai principi contenuti nel Codice Etico e alle procedure interne, per tutti i destinatari del presente Modello che si trovano a operare nelle suddette aree è fatto divieto di assumere comportamenti tali da integrare gli illeciti considerati, anche in forma di concorso o tentativo o tali da agevolarne la commissione. In particolare, è vietato:

- trattare dati personali senza rispettare i diritti dell'interessato;
- trattare dati personali senza limitare la raccolta e il trattamento a quelli necessari e sufficienti;
- trattare dati personali senza far conoscere all'interessato la finalità per la quale sono raccolti, che deve essere determinata, esplicita e legittima;
- trattare dati personali in assenza del consenso dell'interessato, eccettuati i casi previsti nei punti b), c), e) ed f) dell'Art. 6 comma 1 del Regolamento;
- trattare dati personali senza garantire la liceità, la correttezza e la trasparenza del trattamento, sia durante la raccolta sia durante l'elaborazione;
- trattare dati personali senza prevenire ogni forma di utilizzo illecito o non corretto;
- fornire, in qualsiasi forma, informazioni non veritiere o incomplete all'Autorità competente;
- condizionare in qualsiasi forma e con qualsiasi mezzo soggetti chiamati a rendere dichiarazioni all'Autorità competente.

Facendo riferimento alle suddette aree sensibili, a titolo esemplificativo, sono di seguito commentate le modalità attraverso le quali possono essere commessi gli illeciti per ottenere indebiti vantaggi e i principi generali di controllo preventivo.

Area a rischio 1

Gestione della tipologia dei dati personali trattati

Attività sensibili/modalità di commissione degli illeciti

Coloro che si trovano a operare in quest'area sensibile potrebbero offrire o promettere informazioni sui dati personali di persone fisiche in loro possesso, siano essi o no oggetto di profilazione.

Controlli preventivi

- Individuazione delle categorie di interessati (clienti, fornitori, dipendenti, collaboratori, candidati, ecc.);
- individuazione delle categorie di destinatari ai quali i dati sono o saranno comunicati;
- individuazione dei dati sensibili comunicati dagli interessati per dare seguito a eventuali incombenze (convinzioni religiose o di altra natura, adesione a partiti, sindacati o associazioni, stato di salute);
- individuazione dei dati giudiziari (dati idonei a rivelare provvedimenti iscritti nel casellario giudiziario o relativi alla qualità di imputato o indagato di una persona - artt. 60 e 61 del codice di procedura penale);
- esplicitazione delle finalità dei trattamenti effettuati;
- esplicitazione del termine di conservazione dei dati;
- esplicitazione dell'eventuale attività di profilazione (qualsiasi forma di trattamento automatizzato dei dati consistente nel loro utilizzo per valutare determinati aspetti personali relativi a una persona fisica);
- individuazione dell'elenco degli archivi che contengono i dati personali e loro dislocazione;
- conoscenza e applicazione delle regole (autorizzazione e autenticazione) per l'accesso ai dati personali da parte degli Incaricati del Trattamento;
- custodia dei dati cartacei personali o sensibili in armadi con serratura.

Area a rischio 2

Incaricati del Trattamento dei dati personali

Attività sensibili/modalità di commissione degli illeciti

EIH deve predisporre un'adeguata organizzazione di sicurezza finalizzata al trattamento dei dati personali, misura da non ignorare neanche per semplice negligenza o imperizia.

Controlli preventivi

- Predisposizione di una lista degli Incaricati del Trattamento dei dati personali delle persone fisiche;
- designazione formale dei componenti della lista di cui al punto precedente;
- previsione di interventi formativi per gli Incaricati del Trattamento dei dati personali;
- predisposizione dell'elenco degli archivi che contengono i dati personali con i relativi Incaricati del Trattamento;
- predisposizione di una lista degli Amministratori di Sistema (tecnici interni o esterni che possono accedere ai dati personali al di fuori delle normali procedure);
- designazione formale degli Amministratori di Sistema;

- sistema di registrazione degli accessi da parte degli Amministratori di Sistema ("log" degli Amministratori di Sistema).

Area a rischio 3

Gestione dell'informativa e del consenso dell'interessato

Attività sensibili/modalità di commissione degli illeciti

Il consenso al trattamento dei dati personali di persone fisiche potrebbe essere ottenuto in modo non lecito, cioè non conforme alla legge, o non corretto, cioè non in modo chiaro e trasparente ma con artifizi e raggiri.

Controlli preventivi

- Predisposizione di un'adeguata informativa per clienti, fornitori, dipendenti, collaboratori, candidati, ecc.;
- indicazione del periodo di conservazione dei dati personali;
- firma del consenso dell'interessato soprattutto nel caso di trattamento dei dati sensibili;
- firma dei genitori o tutori nel caso di trattamento dei dati relativi ai minori;
- predisposizione di una procedura per gestire le eventuali richieste legittime dell'interessato.

Area a rischio 4

Misure di sicurezza

Attività sensibili/modalità di commissione degli illeciti

I dipendenti e collaboratori a qualsiasi titolo devono conoscere e applicare le procedure e istruzioni operative predisposte da EIH che, a sua volta, deve dedicare le risorse, sia umane che materiali, adeguate a gestire in sicurezza i dati personali delle persone fisiche, garantendone riservatezza, integrità e disponibilità.

Controlli preventivi

- Accesso al sistema da parte degli Incaricati del Trattamento tramite credenziali personali costituite da user id e password, secondo quanto prescrive il Disciplinare delle Risorse Informatiche per i Dipendenti e i Collaboratori degli Enti che Aderiscono al Manifesto ELIS;
- modifica della password, secondo quanto prescrive il Disciplinare;
- protezione con password dei dispositivi portatili assegnati al personale (notebook, tablet, ecc.);
- predisposizione di una procedura di copia e cancellazione/dismissione dei dati;
- protezione dei sistemi con software antivirus e anti-malware;

- predisposizione di un'analisi dei rischi (furto, incendio, comportamenti fraudolenti, errori degli operatori, intrusioni interne o esterne, ecc.) con l'elenco delle misure da adottare;
- predisposizione del Registro delle attività di trattamento effettuate nel caso si trattino dati con rischi per i diritti e le libertà degli interessati e/o in maniera non occasionale.

Area a rischio 5

Gestione degli incidenti per violazione dei dati personali

Attività sensibili/modalità di commissione degli illeciti

In caso di violazione dei dati personali EIH deve informare l'Autorità di Controllo e l'interessato senza ingiustificato ritardo, pensando o tentando di evitare problemi.

Controlli preventivi

Predisposizione di una procedura di raccolta d'informazioni in caso di violazione di sicurezza che comporti, anche accidentalmente, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati al fine di gestire l'incidente, arginare e limitare le conseguenze e prevenire il ripetersi.

2.6.2 Compiti dell'Organismo di Vigilanza

L'OdV vigila sul funzionamento e sull'osservanza del Modello e ne cura l'aggiornamento, al fine di assicurarne l'idoneità e l'efficacia a prevenire gli illeciti di cui alla presente parte. In tale contesto, in aggiunta ai compiti attribuiti all'Organismo già esposti nella Parte Generale del Modello, che devono intendersi qui integralmente richiamati, l'OdV dovrà altresì monitorare le procedure interne per la prevenzione degli illeciti in tema di protezione dei dati personali come organismo imparziale e indipendente dal settore sottoposto a verifica; tale compito sarà svolto anche tenendo conto dei seguenti flussi informativi:

- segnalazioni di eventuali incidenti per violazioni di dati personali,
- provvedimenti assunti dall'Autorità di Controllo,
- eventuali segnalazioni pervenute da qualsiasi dipendente o collaboratore di carenze o inadeguatezze e di ogni altra situazione di rischio,
- comunicazioni di EIH su ogni aggiornamento relativo a variazioni organizzative e di responsabilità conferite in tema di protezione dei dati personali.

2.7 REATI TRIBUTARI

La presente trattazione dei Reati Tributari viene considerata, nell'ambito del Modello di Organizzazione, Gestione e Controllo, come parte a sé stante e autonoma, per la specificità e rilevanza della materia, anziché farla rientrare nel paragrafo 2.1, ove vengono analizzati i Reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia, di cui comunque alcuni punti risultano contigui e compatibili con quelli che vengono di seguito riportati.

Inoltre, si ritiene opportuno evidenziare che questo argomento è novellato da alcune norme recate dal D. L. 26 ottobre 2019, n. 124 (Disposizioni urgenti in materia fiscale e per esigenze indifferibili), convertito dalla Legge 19 dicembre 2019, n. 157, e dal D. Lgs. 14 luglio 2020, n. 75, diretto ad armonizzare la disciplina penale italiana alla direttiva del Parlamento Europeo e del Consiglio del 5 luglio 2017, n. 1371, in tema di lotta contro la frode che leda gli interessi finanziari dell'Unione (cosiddetta "direttiva PIF" - direttiva per la protezione degli interessi finanziari).

In particolare, il predetto D. Lgs. n. 75:

- inasprisce le pene per una serie di reati quando dalla commissione degli stessi derivi una lesione degli interessi finanziari dell'U.E.;
- in materia di imposte sui redditi e sull'IVA - per i reati di dichiarazione infedele, dichiarazione fraudolenta mediante fatture e/o dichiarazione fraudolenta - inserisce la punibilità anche del solo tentativo di reato quando questo è consumato anche nel territorio di un altro Stato membro all'interno dell'U.E.;
- interviene in tema di elusione dei diritti doganali, ripristinando le sanzioni penali per il reato di contrabbando;
- modifica il D. Lgs. 231 del 2001, e, in particolare, con l'articolo 5 apporta modifiche agli artt. 24, 25, e 25 quinquiesdecies dello stesso D. Lgs. 231, ampliando significativamente il catalogo dei reati in relazione ai quali si applicano le sanzioni per la responsabilità amministrativa degli enti.

La direttiva europea è quindi volta a completare il quadro delle misure poste a tutela degli interessi finanziari dell'U.E. in diritto amministrativo e in diritto civile con quelle del diritto penale "evitando al contempo incongruenze sia all'interno di ciascuna di tali branche del diritto che tra di esse".

Più specificatamente, scopo della direttiva è quello di impegnare gli Stati membri a indicare con chiarezza ed esplicitamente quali fattispecie di reato dei rispettivi ordinamenti devono essere considerate lesive degli interessi finanziari dell'U.E., facendo conseguire a tale catalogazione misure sanzionatorie efficaci e proporzionate.

Questa parte del Modello è finalizzata alla prevenzione dei reati contemplati nell'articolo 25 quinquiesdecies del Decreto 231 e nel combinato disposto della normativa di cui sopra che estende il catalogo dei reati presupposto per la responsabilità dell'ente:

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 1, del D. Lgs. 10 marzo 2000, n. 74, come modificato dal D. L. 26 ottobre 2019, n. 124),
- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 2-bis),
- dichiarazione fraudolenta mediante altri artifici (art. 3),

- emissione di fatture o altri documenti per operazioni inesistenti (art. 8, comma 1 e comma 2-bis),
- occultamento o distruzione di documenti contabili (art. 10),
- sottrazione fraudolenta al pagamento di imposte (art. 11),
- dichiarazione infedele (art. 4),
- omessa dichiarazione (art. 5),
- indebita compensazione (art. 10-quater).

2.7.1 Aree a rischio reato, principi generali di comportamento e controlli preventivi

Le aree di attività considerate a rischio con riguardo ai reati tributari sono ritenute le seguenti:

1. Gestione dei rapporti con l'Amministrazione Finanziaria e altri Enti Pubblici.
2. Gestione degli adempimenti fiscali.
3. Contabilità e bilancio.
4. Gestione degli adempimenti societari e dei rapporti di EIH con gli altri Enti che aderiscono al Manifesto ELIS.
5. Gestione della finanza e della tesoreria.

Principi generali di comportamento

In conformità alle normative vigenti, ai principi contenuti nel Codice Etico e alle procedure aziendali, per tutti i destinatari del presente Modello che si trovano a operare nelle suddette aree è vietato:

- assumere comportamenti tali da integrare i reati considerati, anche in forma di concorso o tentativo, o tali da agevolarne la commissione;
- intraprendere iniziative e/o adottare provvedimenti formalmente e volutamente ineccepibili, che surrettiziamente conducano ad evitare l'applicazione di norme contributive o ricadenti nella materia degli adempimenti fiscali;
- inserire nel bilancio o nelle altre comunicazioni sociali previste dalla legge dati non rispondenti al vero o incompleti sulla situazione economica, patrimoniale o finanziaria di EIH;
- effettuare operazioni volte a creare disponibilità extracontabili per scopi non corretti (ad esempio ricorrendo a fatture per operazioni inesistenti o alla sovra fatturazione);
- compromettere la corretta operatività degli organi sociali, dei revisori o recare pregiudizio ai dipendenti e ai creditori;
- impedire od ostacolare in qualunque modo lo svolgimento delle attività di controllo del collegio sindacale;
- determinare o influenzare illecitamente le delibere assunte dall'assemblea dei soci.

Facendo riferimento alle suddette aree sensibili, a titolo esemplificativo, sono di seguito commentate le modalità attraverso le quali i reati stessi possono essere commessi e i principi generali di controllo preventivo.

Area a rischio 1

Gestione dei rapporti con l'Amministrazione Finanziaria e altri Enti Pubblici

Attività sensibili/modalità di commissione dei reati

- Redazione e trasmissione di documenti e dichiarazioni non complete o non veritiere per ottenere un beneficio economico derivante dal pagamento di tributi, contributi o somme in misure inferiori a quanto dovuto a danno dello Stato o di altri Enti pubblici (Regioni, Comuni, altri Enti pubblici fornitori di beni e servizi).
- Richieste di agevolazioni fiscali o decontribuzioni in base a dati, conteggi e titoli predisposti con modalità e misure apposite da essere simili alle condizioni previste da norme vigenti.
- Manifesta intenzione o promessa di corrispondere un'utilità indebita a un Pubblico Ufficiale o incaricato di Pubblico Servizio in occasione di un'ispezione o di richiesta di ulteriore documentazione per procedere alla verifica dell'ottemperanza alle prescrizioni fiscali e contributive.

Controlli preventivi

- Identificazione formale dei soggetti deputati a rappresentare la Società e a intrattenere rapporti con l'Amministrazione Finanziaria e con altri Enti Pubblici, anche in sede d'ispezioni e accertamenti;
- monitoraggio dell'evoluzione della normativa di riferimento per garantire l'adeguamento alle novità in materia fiscale e contributiva da parte di EIH e quindi alla sua puntuale applicazione;
- segregazione dei compiti tra chi predispone la documentazione da trasmettere all'Amministrazione Finanziaria e agli altri Enti Pubblici e chi la controlla e ne autorizza l'invio;
- monitoraggio delle tempistiche da rispettare per comunicazioni e adempimenti verso le suddette Amministrazioni Pubbliche;
- completa, corretta e trasparente trasmissione delle informazioni e dei dati per assolvere gli adempimenti richiesti dall'Amministrazione Finanziaria;
- autorizzazione formale, nel rispetto delle deleghe e delle procure, al corretto pagamento delle imposte e delle tasse correnti.

Area a rischio 2

Gestione degli adempimenti fiscali

Attività sensibili/modalità di commissione dei reati

- Scarsa attenzione al governo della gestione della fiscalità aziendale.

- Comportamenti orientati a contrastare e ridurre il prelievo fiscale a carico di EIH, mediante atteggiamenti fraudolenti messi in atto per pagare meno imposte e tasse o aggirare le norme fiscali.
- Metodi e azioni aventi l'obiettivo di ridurre o eliminare il prelievo fiscale (evasione fiscale) da parte dello Stato e di altre Amministrazioni Pubbliche (Regione, Comune e altri), attraverso pratiche e criteri contabili che violano leggi, regolamenti e norme fiscali, da cui derivano conseguenze sanzionabili sul piano amministrativo e di natura penale.
- Comportamenti e azioni che manifestandosi in abuso del diritto configurano operazioni prive di sostanza economica che, pur nel pedissequo rispetto formale delle norme fiscali, realizzano vantaggi fiscali indebiti (elusione fiscale). Sono irrilevanti sotto il profilo penale, ma sono soggette all'applicazione di sanzioni amministrative commisurate alla misura dell'importo eluso al fisco.

I predetti comportamenti e azioni si concentrano in particolari periodi dell'anno (scadenze contabili e di bilancio, adempimenti e presentazione di dichiarazioni, modelli e documenti fiscali e di natura previdenziale e sociale e relativi versamenti monetari) entro termini perentori, il cui mancato rispetto comporta l'irrogazione di sanzioni, pecuniarie e no.

Controlli preventivi

Il regime contabile/fiscale di EIH rappresenta la metodologia di rilevazione, l'insieme dei documenti da tenere e le formalità da osservare per essere in regola con il fisco e con le norme del Codice civile per la predisposizione del bilancio d'esercizio, al fine di pervenire al corretto calcolo del risultato d'esercizio medesimo, della compilazione della dichiarazione annuale dei redditi e della redazione di tutti gli altri documenti e modelli previsti dalla normativa vigente.

- Assicurare l'assolvimento degli obblighi fiscali, tributari e previdenziali derivanti dalla natura giuridica di EIH e dalla tipologia dell'attività sociale svolta, anche attraverso la gestione di servizi telematici.
- Documentare ogni operazione gestionale e amministrativa, anche per i risvolti fiscali connessi, in modo che sia possibile effettuare controlli in ordine alle caratteristiche e alle motivazioni delle operazioni aziendali e sia agevole individuare le corrispondenti responsabilità.
- Monitorare tutte le tempistiche da rispettare per comunicazioni, trasmissione dati e documenti all'Amministrazione Finanziaria e agli altri Enti pubblici e per i versamenti di imposte, tasse e contributi dovuti.

Area a rischio 3

Contabilità e bilancio

Attività sensibili/modalità di commissione dei reati

- Alterazione dei dati contabili e finanziari con la finalità di produrre informativa economico/patrimoniale/finanziaria non accurata o non veritiera nell'interesse di EIH (sopravalutazione di beni, fatturazioni per forniture inesistenti, contabilizzazione di costi per beni o servizi inesistenti, ecc.).

- Ostacolo allo svolgimento delle attività di controllo attraverso l'occultamento di documenti riguardanti le vicende contabili o attraverso la mancata archiviazione della documentazione.
- Esposizione in bilancio di valori inesistenti o difformi da quelli reali.

Controlli preventivi

- Rispetto dei ruoli e responsabilità definiti dall'organigramma aziendale, dal sistema autorizzativo e dalle procedure vigenti nella gestione della contabilità e del bilancio;
- Obbligo di tenuta e regolarità delle scritture contabili, ossia la rilevazione cronologica degli accadimenti amministrativi che caratterizzano lo svolgimento delle attività produttive e istituzionali, tramite le previste registrazioni e gli appositi libri e documenti contabili;
- Rispetto dei principi di compilazione dei documenti contabili ai sensi dell'art. 2423, comma 2 c.c., a norma del quale "il bilancio deve essere redatto con chiarezza e deve rappresentare in modo veritiero e corretto la situazione patrimoniale della Società e il risultato economico dell'esercizio";
- Obbligo di corretta conservazione e archiviazione di tutta la documentazione che è prodromica all'intera gestione e attività aziendale e deve essere custodita per specifici periodi di tempo espressamente previsti.

Area a rischio 4

Gestione degli adempimenti societari e dei rapporti con i vari Enti che aderiscono al Manifesto ELIS

Attività sensibili/modalità di commissione dei reati

- Esistenza di rapporti economico-finanziari e transazioni commerciali e amministrative con gli altri Enti che aderiscono al Manifesto ELIS.
- Ostacolo allo svolgimento delle attività di controllo, attraverso l'occultamento di documenti riguardanti le vicende contabili o la mancata archiviazione della documentazione.
- Realizzazione di operazioni societarie in presenza di conflitto d'interessi degli Amministratori.

Controlli preventivi

- Rispetto dei compiti, ruoli e responsabilità definiti dall'organigramma aziendale e dal sistema autorizzativo nella gestione degli adempimenti societari;
- monitoraggio periodico degli aggiornamenti normativi in materia societaria;
- definizione formale delle modalità di convocazione e svolgimento dell'assemblea;
- definizione formale delle modalità di predisposizione, approvazione e conservazione della documentazione riguardante gli atti societari;
- messa a disposizione del Collegio Sindacale e della Società di revisione dei documenti gestionali per le verifiche proprie dei due organismi;
- rispetto dei ruoli e delle modalità per l'accesso ai libri sociali (preventiva verifica della

legittimazione del richiedente, rispetto della riservatezza, integrità e disponibilità dei libri medesimi, documentazione attestante l'attività svolta con riferimento alle norme in materia di trasparenza amministrativa e di accesso agli atti);

- vigilanza sulla correttezza e regolarità contabile e amministrativa nei flussi comunicativi, nel rilascio dei titoli e documenti riguardanti i rapporti economico-finanziari e lo scambio di prestazioni e forniture di beni e servizi nell'ambito degli Enti che aderiscono al Manifesto ELIS.

Area a rischio 5

Gestione della finanza e della tesoreria

Attività sensibili/modalità di commissione dei reati

- Gestione non corretta degli incassi per alterare o non fornire l'informativa economico-finanziaria.
- Mancata o errata contabilizzazione di pagamenti o registrazione di pagamenti non corrispondenti al vero (destinatari fittizi o non coincidenti con i destinatari reali, prestazioni non ricevute), per alterare o non fornire l'informativa economico-finanziaria.
- Adeguatezza del numero dei conti correnti e delle aperture di credito presso il sistema bancario.
- Operazioni aventi contenuto finanziario stipulate con gli Enti che aderiscono al Manifesto ELIS.

Controlli preventivi

- Autorizzazione formale, nel rispetto delle deleghe e delle procure, delle operazioni sui conti correnti di EIH;
- controlli formalizzati per accertare la completezza e validità della documentazione intercorsa con l'Istituto Bancario;
- limitazione degli accessi al sistema di homebanking tramite l'assegnazione di credenziali personali di accesso (username e password) e token ai procuratori aziendali;
- monitoraggio del sistema di homebanking per accertare la corrispondenza tra incassi, pagamenti e la documentazione di supporto;
- definizione formale delle modalità di determinazione del fabbisogno finanziario, sulla base delle previsioni d'incasso e di spesa;
- monitoraggio della gestione dei conti correnti bancari e della correttezza delle transazioni dal sistema di gestione della tesoreria al sistema di contabilità generale;
- controlli atti ad accertare che i bonifici siano autorizzati dai procuratori abilitati;
- in caso di operazioni all'estero, verifica che il conto indicato dal fornitore non risieda in uno Stato considerato a rischio (sulla base delle liste stilate dalle organizzazioni sovranazionali) o con regime fiscale privilegiato; in questi casi il Responsabile Amministrativo dovrà fare le opportune valutazioni;
- riconciliazioni bancarie e di cassa eseguite periodicamente;

- definizione formale delle tipologie di spese che possono essere sostenute tramite cassa, del relativo ammontare massimo e dei soggetti abilitati ad autorizzarle;
- verifica della corrispondenza tra le spese autorizzate e i relativi giustificativi.

2.7.2 Compiti dell'Organismo di Vigilanza

L'OdV vigila sul funzionamento e sull'osservanza del Modello e ne cura l'aggiornamento, al fine di assicurarne l'idoneità e l'efficacia a prevenire i reati di cui alla presente parte. In tale contesto, oltre ai compiti presentati nella parte introduttiva del Modello, l'OdV dovrà altresì:

- verificare periodicamente i requisiti d'indipendenza della Società di revisione;
- indicare eventuali integrazioni ai sistemi di gestione finanziaria e contabile, al fine di rilevare l'esistenza di eventuali flussi finanziari atipici e/o soggetti a margini di discrezionalità;
- indicare eventuali scostamenti o sovrapposizioni di perseguimento di obiettivi nello svolgimento dei rapporti interistituzionali tra i soggetti giuridici che aderiscono al Manifesto ELIS.

L'OdV vigila sull'evoluzione verso un modello di lavoro agile, compatibile con l'organizzazione aziendale in relazione alle nuove modalità lavorative.