MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI ICTS ITALIA S.R.L. A SOCIO UNICO.

Ai sensi del D.Lgs 231/2001 e ss.mm.ii.

"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica"

DEFINIZIONI

DECRETO: Il Decreto legislativo 8 giugno 2001 n. 231 e ss.mm.ii

DIPENDENTI: Persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali; quindi, ma non solo, tutti i soggetti – compresi i dirigenti – che intrattengono un rapporto di lavoro subordinato, di qualsivoglia natura, con la Società nonché i lavoratori in distacco o in forza con contratti di lavoro parasubordinato

DOCUMENTO INFORMATICO: Qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati a rielaborarli

ILLECITI AMMINISTRATIVI: Gli illeciti amministrativi di cui all'art. 187 – quinques del Testo Unico delle disposizioni in materia di intermediazione finanziaria;

MODELLO DI ORGANIZZAZIONE E DI GESTIONE: Il presente Modello di organizzazione, gestione e controllo così come previsto ex D.Lgs 231/2001 e ss.mm.ii

ORGANISMO DI VIGILANZA: L'Organismo di vigilanza previsto dal D.Lgs 231/2001 e ss.mm.ii

REATI: I reati di cui al D.Lgs 231/2001 e ss.mm.ii

S0OCIETÀ: ICTS ITALIA S.R.L. A SOCIO UNICO

SOGGETTI APICALI: Persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua Unità dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione o il controllo della Società

PARTE GENERALE

SEZIONE PRIMA

1 Il Decreto Legislativo 231/2001

1.1. La Responsabilità Amministrativa degli Enti

In data 8 giugno 2001 è stato emanato – in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 – il Decreto legislativo n. 231 (di seguito denominato il "Decreto"), entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa italiana in materia di responsabilità delle persone giuridiche alle Convenzioni Internazionali a cui l'Italia ha aderito ed in particolare:

- la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità europee;
- La Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità europea o degli Stati Membri;
- La Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

Con tale Decreto, rubricato "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", è stato introdotto nell'ordinamento italiano un regime di responsabilità amministrativa a carico di enti (società, associazioni etc.) per alcuni reati commessi nell'interesse o a vantaggio degli stessi da:

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

La responsabilità amministrativa degli Enti si aggiunge a quella della persona fisica che ha materialmente commesso il reato e sono entrambe oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale. Peraltro, la responsabilità dell'Ente permane anche nel caso in cui la persona fisica autrice del reato non sia identificata o punibile.

1.2 I reati previsti dal Decreto

I reati, dal cui compimento è fatta derivare la responsabilità amministrativa dell'Ente, sono quelli espressamente e tassativamente richiamati dal Decreto e ss.mm.ii.

1.3. Le sanzioni previste dal Decreto

Il sistema sanzionatorio, a fronte del compimento dei reati indicati, prevede l'applicazione delle seguenti sanzioni amministrative:

- Sanzioni pecuniarie;
- Sanzioni interdittive;
- Confisca;
- Pubblicazione della sentenza.

La sanzione pecuniaria è ridotta della metà e non può comunque essere superiore a € 103.291,00 nel caso in cui: a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo; b) il danno patrimoniale cagionato è di particolare tenuità.
La sanzione è ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado: a) l'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; b) è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.
Le sanzioni interdittive si applicano in relazione ai reati per i quali sono espressamente previste, quando ricorre almeno una delle seguenti condizioni: a) l'Ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative; b) in caso di reiterazione degli illeciti.
Le sanzioni interdittive hanno una durata non inferiore a 3 mesi e non superiore a 2 anni.
Il Decreto prevede le seguenti sanzioni interdittive:

- Interdizione dall'esercizio dell'attività;
- Sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- Divieto di contrattare con la Pubblica Amministrazione;
- Esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o revoca di quelli eventualmente già concessi;
- Divieto di pubblicizzare beni o servizi.

Ai sensi della normativa vigente, le sanzioni interdittive non si applicano in caso di commissione dei reati societari e di market abuse. Si precisa, infatti che, per tali reati, sono previste le sole sanzioni pecuniarie, raddoppiate nel loro ammontare dall'art. 39, comma 5, della L. 262/2005 ("Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari").
Il Decreto prevede, inoltre, che, qualora vi siano i presupposti, per l'applicazione di una sanzione interdittiva che disponga l'interruzione dell'attività della società, il giudice, in luogo dell'applicazione della sanzione interdittiva, possa disporre la prosecuzione dell'attività da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando ricorre almeno una delle seguenti condizioni:

- La società svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;
- L'interruzione dell'attività può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

1.4 Condizione esimente della Responsabilità Amministrativa

Gli artt. 6 e 7 del Decreto prevedono forme specifiche di esonero dalla responsabilità amministrativa dell'Ente per i reati commessi nell'interesse o a vantaggio dell'Ente sia da soggetti apicali sia da dipendenti.
In particolare, nel caso di reati commessi da soggetti in posizione apicale, l'art. 6 prevede l'esonero qualora l'Ente stesso dimostri che:

- L'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione e di gestione idoneo a prevenire reati della fattispecie di quello verificatosi;
- Il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di proporne l'aggiornamento sia affidato ad un organismo dell'Ente ("Organismo di Vigilanza") dotato di autonomi poteri di iniziativa e controllo;
- Le persone che hanno commesso il reato abbiano agito eludendo fraudolentemente il suddetto Modello;
- Non via stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Per quanto concerne i dipendenti, l'art. 7 prevede l'esonero nel caso in cui l'Ente abbia adottato ed efficacemente attuato prima della commissione del reato un Modello idoneo a prevenire reati della specie di quello verificatosi.
Il Decreto prevede, inoltre, che il Modello debba rispondere alle seguenti esigenze:

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

Lo stesso Decreto prevede che i Modelli possano essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministri competenti, può formulare entro 30 giorni, osservazioni sull'idoneità del Modello a prevenire i reati. Con riferimento ai reati ed illeciti amministrativi in materia di market abuse, tale valutazione di idoneità viene compiuta dal Ministero della Giustizia, sentita la CONSOB.
E' infine previsto che, negli Enti di piccole dimensioni, il compito di vigilanza possa essere svolto direttamente dall'organo dirigente.
Con riferimento all'effettiva applicazione del Modello il Decreto richiede:

- Una verifica periodica, e, nel caso in cui siano scoperte significative violazioni delle prescrizioni imposte dal Modello o intervengano mutamenti nella organizzazione o nella attività dell'ente ovvero modifiche legislative, la modificazione del Modello;
- L'irrogazione di sanzioni in caso di violazione delle prescrizioni imposte dal Modello.

1.5 Delitti tentati e delitti commessi all'estero

L'Ente risponde anche degli illeciti dipendenti da delitti tentati e da reati commessi all'estero.
Nelle ipotesi di commissione nella forma del tentativo dei delitti previsti dal Decreto, le sanzioni pecuniarie e le sanzioni interdittive sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'Ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento. L'esclusione di sanzioni si giustifica, in tal caso, in forza della interruzione di ogni rapporto di immedesimazione tra Ente e soggetti che assumono di agire in suo nome e per suo conto.
In base al disposto dell'art. 4 del Decreto, l'Ente che abbia sede in Italia può essere chiamato a rispondere, in relazione a reati – contemplati dallo stesso Decreto – commessi all'estero, al fine di non lasciare sfornita di sanzione una condotta criminosa di frequente verificazione, nonché al fine di evitare facili elusioni dell'intero impianto normativo in oggetto.
I presupposti su cui si fonda la responsabilità dell'Ente per reati commessi all'estero sono:

- Il reato deve essere commesso all'estero da un soggetto funzionalmente legato all'Ente, ai sensi dell'art. 5, comma 1 del Decreto;
- L'Ente deve avere la propria sede principale nel territorio dello Stato italiano;
- Le condizioni previste dagli artt. 7, 8, 9, 10 codice penale, con riferimento alla punibilità dei reati commessi all'estero, si devono essere verificate;
- Non si procede nei confronti dell'Ente nello Stato in cui è stato commesso il fatto.

SEZIONE SECONDA

2 Il Modello di Organizzazione, gestione e controllo della ICTS ITALIA S.R.L. A SOCIO UNICO

2.1 Descrizione delle attività della ICTS ITALIA S.R.L. A SOCIO UNICO

La ICTS ITALIA S.R.L. A SOCIO UNICO è una società attiva nel settore della effettuazione, con ogni strumento e/o mezzo, anche in zona doganale, di servizi di sicurezza in ambito aeroportuale, portuale, ferroviario o in ogni altro diverso ambito per conto, anche, di compagnie aeree, marittime, ferroviarie e società di gestione di aeroporti, porti o stazioni ferroviarie, anche con assistenza ai viaggiatori ed anche al di fuori dei suddetti siti, allo scopo di ottimizzare le condizioni di viaggio; ogni diverso servizio di assistenza a terra, anche in zona doganale, anche alle compagnie aeree, marittime o ferroviarie e/o alle società di gestione di aeroporti, porti o stazioni ferroviarie; la verifica, con ogni strumento e mezzo, anche su incarico di compagnie di volo, di navigazione o ferroviarie, dell'adeguatezza dei sistemi di controllo in aziende, nei porti, aeroporti, stazioni ferroviarie e/o altri siti, anche in zone doganali, con assistenza ai viaggiatori e/o committenti, anche al di fuori dei suddetti siti, allo scopo di ottimizzare le condizioni di viaggio; ogni altra attività rientrante in genere nel settore della vigilanza e dei controlli dei trasporti di persone e cose; tenuta di corsi interni e presso le aziende committenti; preparazione di manuali di procedure studiati per la committenza e personalizzati; attività di traino e formazione del personale; effettuazione di studi di mercato, surveys, studi di fattibilità; attività di sorveglianza , di scorta e di protezione, trasporto valori, pattugliamento, vigilanza e sorveglianza di fabbricati pubblici e privati; attività di vigilanza ai sensi dell'art. 134 TULPS; consulenza in materia di sicurezza industriale, delle famiglie e dei servizi pubblici in connessione con il servizio di vigilanza; servizi di portineria, reception e sorveglianza; svolgimento di attività di ricerca e di individuazione per conto terzi di aziende di vigilanza privata per lo svolgimento dei servizi in campo della vigilanza privata anche ai sensi dell'art. 115 TULPS;

allevamento, istruzione, addestramento, cura, alloggio, compravendita, prestito d'uso e noleggio di cani da destinare ai controlli di sicurezza, nonché di formazione di istruttori ed allevatori, mediante la tenuta di corsi, la diffusione di pubblicazioni, la realizzazione o compravendita di software, nonché attraverso ogni altro più diverso mezzo e/o strumento atto allo scopo; commercializzare in ogni forma e con ogni strumento , anche elettronico, il proprio know how relativo all'addestramento e formazione dei cani ed all'espletamento dei controlli di sicurezza.

Ai fini del perseguimento dell'oggetto sociale, la ICTS ITALIA S.R.L. A SOCIO UNICO è titolare di licenza, emessa ai sensi dell'art. 134 TULPS, dalla Prefettura di Roma, licenza prot. n. 79472/Area I Ter O.S.P. rilasciata in data 28.02.2019 aggiornata con licenza prot. n. 204190/Area I Ter O.S.P..

È altresì autorizzata all'esercizio dell'attività di intermediazione di cui all'art. 115 TULPS.

Leader mondiale nella consulenza sulla sicurezza, ICTS ITALIA S.R.L., è stata fondata in Italia nel 1987.

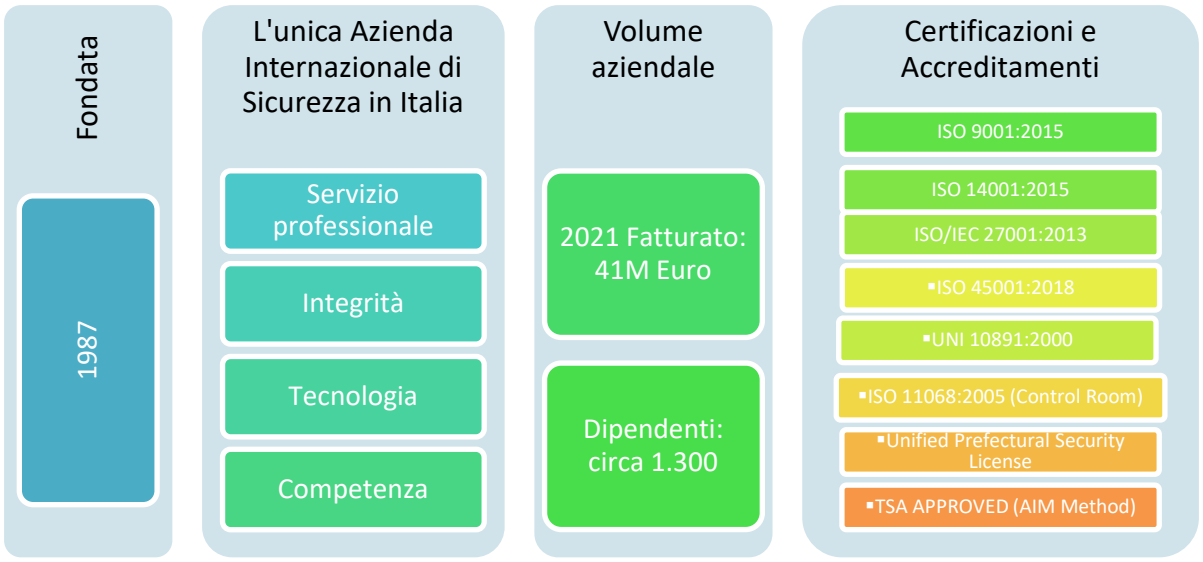
Con l'avvento dei dirottamenti di aeromobili su larga scala alla fine degli anni '60, sono emerse le necessità di protezione degli aeroporti e le compagnie aeree, principalmente a causa della loro vulnerabilità e della relativa facilità di attacco. Negli anni '70 e '80 l'attività terroristica si espanse per includere attacchi a terra, sulle piste aeroportuali o all'interno di terminal, e l'uso di ordigni esplosivi per distruggere gli aerei in volo.

Fino all'11 settembre 2001, gli incidenti più noti di questo tipo hanno riguardato il tentativo riuscito di terroristi di piazzare un ordigno esplosivo a bordo del volo PanAm 103, che è esploso su Lockerbie, in Scozia, nel dicembre 1988. Questo evento ha portato a un aumento mondiale dell'impegno per la sicurezza aerea. Dopo i terribili eventi dell'11 settembre, tale impegno è aumentato, accompagnato da cambiamenti significativi e di vasta portata nel concetto e nella direzione da parte delle agenzie di regolamentazione, delle autorità locali, delle compagnie aeree, degli aeroporti, ecc.

ICTS ha sviluppato competenze per contrastare l'attività terroristica dell'aviazione attraverso una combinazione di analisi e screening dei passeggeri, con l'utilizzo di apparecchiature avanzate per il rilevamento di esplosivi e ordigni esplosivi sui passeggeri e nel bagaglio.

Fin dall'inizio, ICTS ha sviluppato e adattato le sue tecniche e metodologie alle mutevoli esigenze del settore aereo. Molti dei servizi forniti da ICTS sono progettati per consentire alle compagnie aeree e ai clienti aeroportuali di soddisfare i requisiti di sicurezza loro imposti dalle autorità.

Negli anni successivi, ICTS è cresciuta fino a diventare un fornitore leader di soluzioni di sicurezza per un'ampia base di clienti di compagnie aeree, aeroporti, porti marittimi, operatori cargo, clienti corporate e marchi di lusso.



Nel 2010 la ICTS ITALIA S.R.L. A SOCIO UNICO ha sviluppato anche specifiche competenze in materia di sicurezza armata, organizzando uno specifico ramo d'azienda.

Socio unico della ICTS ITALIA è la ICTS Europe, fondata nell'aprile 2000, a seguito di un'analisi completa e approfondita delle tendenze e degli sviluppi economici e globali, sia di natura generale che relativi specificamente all'industria aeronautica. Tra le principali conclusioni tratte si è evidenziata la necessità di una gestione centrale delle attività europee, ovvero la gestione totale di ICTS Europe come un'unità omogenea e autonoma su tutte le società da essa partecipate.

Attraverso le sue partecipate, la ICTS Europe fornisce servizi di sicurezza aerea avanzati (principalmente l'implementazione di procedure di valutazione e classificazione dei rischi dei passeggeri, generalmente descritte come "screening dei passeggeri"). ICTS Europe fornisce, altresì, anche servizi di sicurezza dell'aviazione generale, alcuni servizi di assistenza ai passeggeri dell'aviazione, servizi di sicurezza generale, e servizi specializzati di sicurezza del cargo (svolti mediante unità cinofile).

L'obiettivo principale di ICTS Italia e ICTS Europe è assistere organizzazioni, società, compagnie aeree, Enti aeroportuali, Ambasciate, Enti pubblici etc.. nel contrastare un elenco sempre più lungo di minacce alla loro sicurezza, inclusi terrorismo, furto con scasso, distruzione di proprietà, minacce interne e uso improprio delle informazioni.

2.2 Modello di governance

La Corporate governance di ICTS ITALIA S.R.L. A SOCIO UNICO, basato sul modello tradizionale, è così articolata:

Assemblea dei soci competente a deliberare in sede ordinaria e straordinaria sulle materie alla stessa riservate dalla legge o dallo statuto.

Consiglio di Amministrazione, il cui Presidente è **investito** dei più ampi poteri per l'amministrazione della Società, con facoltà di compiere tutti gli atti opportuni per il raggiungimento degli scopi sociali, ad esclusione degli atti – riservati dalla legge – all'Assemblea dei soci.

AMMINISTRATORE DELEGATO, investito dei poteri ad esso delegati dal Consiglio di Amministrazione, comprensivi della legale rappresentanza della Società, nonché titolare e intestatario della licenza prefettizia, con tutti i poteri di controllo e di supervisione in essa previsti.

SINDACO UNICO che vigila sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento

2.3 Modello organizzativo

Di seguito sono dettagliate le descrizioni delle posizioni per le funzioni di management all'interno dell'azienda responsabili del controllo e della manutenzione del sistema di gestione.

2.3.1 **Amministratore Delegato:**

Ha tutti i poteri e le funzioni attribuitegli dal CDA con verbale del 21/02/2019. Nello specifico ha il potere di impegnare e rappresentare la ICTS ITALIA S.R.L., nonché la Direzione Tecnica dell'impresa in forza della Licenza Prefettizia rilasciata dalla prefettura di Roma ex. Art. 134 TULPS licenza prot. n. 79472/Area I Ter O.S.P. rilasciata in data 28.02.2019 aggiornata con licenza prot. n. 204190/Area I Ter O.S.P.

2.3.2 **Direttore Tecnico**

Il Direttore Tecnico d'Istituto riporta all'Amministratore Delegato e ha le seguenti responsabilità:

a) è responsabile della conduzione tecnica dell'Istituto;
b) sovrintende alle attività della Centrale Operativa;
c) compie tutti gli adempimenti di carattere tecnico e organizzativo necessari per la realizzazione dei servizi;
d) provvede alla gestione degli adempimenti di carattere tecnico operativo;
e) mantiene i contatti con i clienti.
f) mantiene i contatti con le autorità di regolamentazione nazionali e locali;
g) contribuisce efficacemente al Sistema di Gestione Integrato;
h) contribuisce efficacemente al Sistema di Gestione della Sicurezza delle Informazioni;

2.3.3 **Financial Manager**

Il Finance manager riporta all'Amministratore Delegato. Responsabilità:

a) monitoraggio dell'andamento dei parametri economico-finanziari;
b) redazione dei report periodici;
c) coordinamento e gestione dell'area finanziaria;
d) analisi della contabilità reddituale e finanziaria;
e) supervisione degli adempimenti fiscali;
f) gestione del portafoglio e del credit risk;
g) coordinamento della cassa e della tesoreria;
h) collaborazione a progetti in ambito finanziario;

i) analisi delle tendenze del mercato per massimizzare i profitti;
j) supervisione dei dipendenti che si occupano di rendicontazione finanziaria;
k) pianificazione finanziaria d'impresa;
l) controllo di gestione;
m) valutazione degli investimenti e capital budgeting;
n) misurazione delle performance;
o) conoscenza dei sistemi informativi a supporto dell'attività finanziaria.

2.3.4 Data Protection Officer (DPO)

Riporta direttamente all'Amministratore Delegato. Responsabilità:

a) fungere da punto di contatto con le autorità di vigilanza e i team interni;
b) identificare e valutare le attività di trattamento dei dati della società;
c) Fornire consigli e istruzioni su come condurre le valutazioni dell'impatto sulla protezione dei dati (DPIA)
d) monitorare le procedure di gestione dei dati e la conformità all'interno dell'azienda;
e) Partecipare agli incontri con i responsabili per garantire la privacy by design a tutti i livelli;
f) Conservare e garantire l'aggiornamento dei registri delle operazioni di trattamento
g) Garantire il corretto adempimento dei diritti degli interessati entro i termini di legge (ad es. eliminare le loro informazioni dai nostri database);
h) Collaborare con altre organizzazioni che elaborano dati per nostro conto;
i) Scrivere e aggiornare guide dettagliate sulle politiche di protezione dei dati;
j) eseguire audit e determinare se è necessario modificare le procedure aziendali per conformarsi alle normative;
k) offrire consulenza su come affrontare le violazioni della privacy;
l) organizzare una formazione sulla compliance al GDPR per i dipendenti;
m) dare seguito alle modifiche della legge ed emettere raccomandazioni per garantire la conformità.

2.4 Finalità del Modello 231

ICTS ITALIA S.R.L. A SOCIO UNICO è sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione e immagine, delle aspettative dei propri soci e del lavoro dei propri dipendenti ed è consapevole dell'importanza di dotarsi di un sistema di controllo interno aggiornato ed idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri amministratori, dipendenti, rappresentanti e partner d'affari.

A tal fine ICTS ITALIA S.R.L. A SOCIO UNICO ha avviato un progetto di analisi dei propri strumenti organizzativi, di gestione e di controllo, volto a verificare la corrispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto ed implementare il Modello di Organizzazione, Gestione e controllo ex D.Lgs 231/2001 e ss.mm.ii.

Attraverso l'adozione del Modello, la ICTS ITALIA S.R.L. A SOCIO UNICO intende perseguire i seguenti obiettivi:

- Vietare comportamenti che possano integrare le fattispecie di reato di cui al Decreto;
- Diffondere la consapevolezza che dalla violazione del Decreto, delle prescrizioni contenute nel Modello e dei principi del Codice Etico, possa derivare l'applicazione di misure sanzionatorie (di natura pecuniaria e interdittiva) anche a carico della Società;
- Consentire alla Società, grazie ad un sistema strutturato di procedure e ad una costante azione di monitoraggio sulla corretta attuazione di tale sistema, di prevenire e/o contrastare tempestivamente la commissione di reati rilevanti ai sensi del Decreto.

Scopo del Modello è la definizione di un sistema strutturato ed organico di procedure ed attività di controllo (preventivo ed ex post) con l'obiettivo di ridurre il rischio di commissione dei reati mediante la individuazione delle "Aree di attività a rischio" e dei "Processi strumentali/funzionali" alla commissione e la proceduralizzazione delle principali aree di attività a rischio e dei principali processi strumentali.
I principi contenuti nel presente Modello devono condurre, da un lato, a determinare una piena consapevolezza nel potenziale autore del reato di commettere un illecito (la cui commissione è fortemente condannata e contraria agli interessi della ICTS ITALIA S.R.L. A SOCIO UNICO anche quando apparentemente essa potrebbe trarne un vantaggio), dall'altro, grazie ad un monitoraggio costante dell'attività, a consentire a ICTS ITALIA S.R.L. A SOCIO UNICO di reagire tempestivamente nel prevenire od impedire la commissione del reato stesso.
Tra le finalità del Modello c'è, quindi, quella di sviluppare la consapevolezza nei dipendenti, organi sociali, consulenti e partner, genericamente "soggetti terzi" che operino per conto o nell'interesse della società, di poter incorrere – in caso di comportamenti non conformi alle prescrizioni del Codice Etico e alle altre norme e procedure aziendali – in illeciti passibili di conseguenze penalmente rilevanti non solo per se stessi, ma anche per la società.
Gli elementi che caratterizzano il presente Modello sono: l'efficacia, la specificità e l'attualità.

L'efficacia.

L'efficacia del Modello dipende dalla sua idoneità in concreto ad elaborare meccanismi di decisione e di controllo tali da eliminare – o quantomeno ridurre significativamente – l'area di rischio da responsabilità. Tale idoneità è garantita dall'esistenza di meccanismi di controllo, preventivo e successivo, idonei ad identificare le operazioni che possiedono caratteristiche anomale, tali da segnalare condotte critiche rientranti nelle aree di rischio e strumenti di tempestivo intervento nel caso di individuazione di siffatte anomalie.

La specificità

La specificità del Modello è uno degli elementi che ne connota l'efficacia. È necessaria una specificità connessa alle aree di rischio, così come richiamata dall'art. 6, comma 2 lett. a) del Decreto, che impone un censimento delle attività della Società nel cui ambito possono essere commessi i reati.
Ai sensi dell'art. 6, comma 2 lett. b) del Decreto è altrettanto necessario che il Modello preveda specifici protocolli diretti a regolamentare la formazione e l'attuazione delle decisioni della Società nell'ambito delle Aree di attività a rischio e dei processi strumentali individuati in sede di mappatura delle attività.
Analogamente, la individuazione delle modalità di gestione delle risorse finanziarie, la definizione di un sistema di flussi informativi verso l'organo di vigilanza e la introduzione di un adeguato sistema disciplinare sono obblighi che richiedono la specificità delle singole componenti del Modello.

Il Modello, ancora, deve tener conto delle caratteristiche proprie, delle dimensioni della Società e del tipo di attività svolte, nonché della storia della Società.

L'attualità

Un Modello è idoneo a ridurre i rischi da reato qualora sia costantemente aggiornato e adeguato nel tempo alle caratteristiche della struttura e dell'attività di impresa.

In tal senso, l'art. 6 del Decreto prevede che l'Organismo di vigilanza, titolare di autonomi poteri di iniziativa e controllo, abbia la funzione di curare l'aggiornamento del Modello in maniera tale da poter mantenere nel tempo i requisiti di funzionalità ed efficacia che lo caratterizzano.

Come previsto nella Circolare della Guardia di Finanza n. 83607/2012 " Attività della Guardia di Finanza a tutela del mercato dei capitali – volume III Responsabilità amministrativa degli enti dipendente da reato", tale attività si concretizza nella predisposizione e presentazione, a cura dell'Organismo di vigilanza, di apposite note di adeguamento per gli organo aziendali che si adopereranno per assicurarne il recepimento.

L'art. 7 del Decreto stabilisce che l'efficace attuazione del Modello contempli una verifica periodica, nonché l'eventuale modifica dello stesso allorquando siano scoperte eventuali violazioni significative delle prescrizioni oppure intervengano modifiche nell'attività o nella struttura organizzativa della Società.

2.5 Destinatari

Le regole contenute nel Modello si applicano:

- A coloro i quali siano titolari, all'interno della Società, di qualifiche formali, come quella di rappresentante legale, amministratore, sindaco;
- A coloro i quali svolgano funzioni di direzione in veste di responsabili di specifiche Unità Organizzative;
- A coloro i quali, seppure sprovvisti di una formale investitura, esercitino nei fatti attività di gestione e controllo della Società. La previsione, di portata residuale, è finalizzata a conferire rilevanza al dato fattuale, in modo da ricomprendere, tra gli autori dei reati anche coloro che, compiendo determinate operazioni, agiscono concretamente sulla gestione della società;
- Ai lavoratori subordinati della Società, di qualsiasi grado e in forza di qualsiasi tipo di rapporto contrattuale, nonché ai dipendenti distaccati;
- A chi, pur non appartenendo alla Società, opera su mandato o nell'interesse della medesima (consulenti, collaboratori, partner, fornitori ecc..).

Il Modello costituisce un riferimento indispensabile per tutti coloro che contribuiscono allo sviluppo delle varie attività, in qualità di fornitori di beni, servizi e lavori, consulenti, partners nelle associazioni temporanee o società con cui ICTS ITALIA opera.

2.6 Struttura del Modello

Il presente Modello è costituito da una "Parte Generale" e da singole "Parti Speciali" predisposte per le diverse tipologie di reato contemplate nel Decreto.

Si evidenza che nelle Parti Speciali sono state riportate le tipologie di reato presupposto, identificate nell'ambito di un'attività di mappatura delle "Aree a rischio reato" e per le quali è stato ritenuto che ICTS ITALIA possa essere esposta, in via potenziale ed eventuale, al rischio di commissione degli illeciti in considerazione delle attività svolte.

È demandato all'Amministratore Delegato di mantenere il Modello costantemente aggiornato ed in particolare di integrarlo, ove necessario e/o opportuno, mediante apposite delibere, anche con ulteriori Parti Speciali relative ad altre tipologie di reato che, per effetto di sopravvenute normative, risultino inserite o comunque collegate all'ambito di applicazione del Decreto.

2.7 Elementi fondamentali del Modello

In linea con le esigenze definite all'art. 6, comma 2, del Decreto, gli elementi fondamentali sviluppati dalla ICTS ITALIA nella definizione del Modello, possono essere così riassunti:

- Mappatura delle attività sensibili, con la descrizione di possibili modalità di realizzazione dei reati, nonché dei processi strumentali/funzionali potenzialmente associabili alla commissione dei reati richiamati nel Decreto, da sottoporre ad analisi e monitoraggio periodico;
- Previsione di specifiche procedure operative dirette a regolamentare la formazione e l'attuazione delle decisioni della Società, nonché la gestione delle risorse finanziarie;
- Identificazione dei principi etici e delle regole comportamentali volte alla prevenzione di condotte che possano integrare le fattispecie di reato previste dal Decreto, sanciti nel Codice Etico adottato dalla Società e, più in dettaglio, nel presente Modello;
- Nomina di un Organismo di Vigilanza al quale sono attribuiti specifici compiti di vigilanza sull'efficace attuazione ed effettiva applicazione del Modello ai sensi dell'art. 6 punto b) del Decreto;
- Adozione di un sistema sanzionatorio idoneo a garantire l'efficace attuazione del Modello, contenente le disposizioni disciplinari applicabili in caso di mancato rispetto delle misure indicate nel Modello medesimo;
- Svolgimento di un'attività di informazione, sensibilizzazione e divulgazione sulle previsioni del Decreto e sui contenuti del Modello ai destinatari del Modello stesso;
- Definizione delle modalità per l'adozione e l'effettiva applicazione del Modello nonché per le necessarie modifiche o integrazioni dello stesso.

2.8 Codice Etico e Modello 231

Le regole di comportamento contenute nel presente Modello si integrano con quelle del Codice Etico che ne costituisce parte integrante, pur presentando il Modello, per le finalità che esso intende perseguire in attuazione della disposizione del Decreto, una portata diversa rispetto al Codice stesso. Sotto tale profilo infatti:

- il Codice Etico rappresenta uno strumento adottato in via autonoma e suscettibile di applicazione sul piano generale allo scopo di esprimere dei principi di "deontologia aziendale" che la Società riconosce come propri e sui quali richiama l'osservanza da parte di tutti i Dipendenti e dei diversi portatori di interesse della Società (p.e. fornitori, partners, clienti ecc..);
- il Modello risponde invece a specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati.

2.9 Presupposti del Modello

Nella predisposizione del Modello, ICTS ITALIA ha tenuto conto della propria organizzazione aziendale, al fine di identificare le aree di attività più esposte al rischio di potenziale commissione dei reati contemplati nel Decreto.

La Società ha tenuto altresì conto del proprio sistema di controllo interno al fine di valutarne la capacità a prevenire le fattispecie di reato previste dal Decreto nelle aree di attività identificate a rischi.

Il sistema di controllo interno di ICTS ITALIA deve garantire, con ragionevole certezza, il raggiungimento dei seguenti obiettivi:

- obiettivo operativo, che riguarda l'efficacia e l'efficienza della Società nell'impiegare le risorse, nel proteggersi dalle perdite e nel salvaguardare il patrimonio aziendale;
- obiettivo di informazione completa, corretta e veritiera che si traduce nella predisposizione di rapporti completi, tempestivi ed affidabili a supporto del processo decisionale all'interno e all'esterno dell'organizzazione aziendale;
- obiettivo di conformità a leggi e regolamenti, al fine di garantire che tutte le operazioni ed azioni siano condotte nel rispetto delle leggi e dei regolamenti applicabili, dei requisiti prudenziali e delle procedure aziendali interne.

Il sistema di controllo interno di ICTS ITALIA si basa sui seguenti elementi:

- sistema organizzativo formalizzato e chiaro nella attribuzione delle responsabilità;
- sistema di controllo di gestione e reporting;
- poteri autorizzativi e di firma assegnati in coerenza con le responsabilità attribuite ai Responsabili di Area;
- sistema di comunicazione interna e formazione del personale sui presupposti della normativa e sui contenuti del Modello;
- procedure operative interne relative ai principali processi aziendali.

Alla base del sistema di controllo interno di ICTS ITALIA vi sono i seguenti principi:

- ogni operazione, transazione e azione deve essere veritiera, verificabile, coerente e documentata;
- nessuno deve poter gestire un intero processo in autonomia;
- il sistema di controllo interno deve poter documentare l'effettuazione dei controlli, anche di supervisione.

Tutto il personale, nell'ambito delle funzioni svolte, è responsabile della definizione e del corretto funzionamento del sistema di controllo attraverso i controlli di linea, costituiti dall'insieme delle attività di controllo che le singole unità operative svolgono sui loro processi.

2.10 Individuazione delle attività "a rischio"

Il Decreto prevede espressamente, all'art. 6 comma 2 lett. a), che il Modello dell'Ente individui le attività aziendali, nel cui ambito possano essere potenzialmente commessi i reati di cui al medesimo Decreto.
È stata dunque condotta l'analisi delle attività aziendali di ICTS ITALIA e delle relative strutture organizzative, allo specifico scopo di identificare le aree di attività aziendale a rischio, ossia quelle nel cui ambito possono essere commessi i reati previsti nel Decreto, le attività sensibili, le esemplificazioni di

possibili modalità di realizzazione dei reati, nonché i processi nel cui svolgimento, sempre in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato (c.d. processi strumentali/funzionali).
La valutazione del grado di rischio, cui è esposta la Società, è stata effettuata in sede di mappatura delle attività aziendali, con riguardo a ciascuna attività sensibile e processo strumentale/funzionale, sulla base di considerazioni di tipo quantitativo e qualitativo che hanno tenuto conto, a titolo esemplificativo dei seguenti fattori; frequenza dell'accadimento, dell'evento o dell'attività, gravità delle sanzioni potenzialmente associabili alla commissione di uno dei reati, danno di immagine derivante dalla possibile realizzazione di condotte illecite nelle attività a rischio.
In considerazione delle attività caratteristiche di ICTS ITALIA le aree a rischio rilevate hanno riguardato, in particolar modo, i reati previsti agli artt. 24, 25, 25–ter, 24-bis, 25-decies, 25-septies del Decreto. In particolare i reati di:

- Corruzione per un atto di ufficio o contrario ai doveri di ufficio (artt. 318 e 319 c.p.);
- Corruzione in atti giudiziari (art. 319-ter c.p.);
- Istigazione alla corruzione (art. 322 c.p.);
- Induzione indebita a promettere utilità (art. 319 – quater c.p.);
- Truffa in danno dello Stato, di altro Ente Pubblico o dell'Unione Europea (art. 640, comma 2, n. 1 c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 c.p.);
- Malversazione a danno dello Stato o dell'Unione Europea (art. 316-bis c.p.);
- Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (art. 316-ter c.p.);
- Frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640-ter c.p.);
- Concussione (art. 317 c.p.);
- Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e degli Stati Esteri (art. 322 –bis c.p.);
- False comunicazioni sociali e comunicazioni sociali in danno della Società, dei soci e dei creditori (art. 2621 e 2622 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Impedito controllo (art. 2625 c.c.);
- Formazione fittizia del capitale (art. 2632 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità Pubbliche di Vigilanza (art. 2638 c.c.);
- Illegale ripartizione degli utili o delle riserve (art, 2627 c.c.);
- Corruzione tra privati (art. 2635 c.c.);
- Indebita restituzione dei conferimenti (art. 2626 c.c.);
- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Indebita ripartizione dei ben sociali da parte dei liquidatori (art. 2633 c.c.);
- Omessa comunicazione del conflitto di interesse (art. 2629 c.c.);
- Estensione delle qualifiche soggettive (art. 2639 c.c.);
- Falsità in documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.);
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinques c.p.);
- Frode informatica del certificatore di firma elettronica (art. 640-quinques c.p.);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-ter c.p.);

- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinques c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 – quater c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinques c.p.);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
- Indebito utilizzo, falsificazioni, alterazione e ricezione di carte di credito o di pagamento (art. 55, comma 5, D.lgs 231/2007);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.);
- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose (art. 590 c.p.).

Nello specifico è stato riscontrato il rischio di possibile commissione dei reati previsti dal Decreto nelle seguenti aree di attività aziendale:

1) GESTIONE DI RAPPORTI DI PROFILO ISTITUZIONALE CON SOGGETTI APPARTENENTI ALLA PUBBLICA AMMINISTRAZIONE

Gestione dei rapporti di "alto profilo" con soggetti istituzionali e/o altri soggetti appartenenti a Enti pubblici di rilevanza nazionale e internazionale

2) GESTIONE DEL SISTEMA DI SICUREZZA AI SENSI DEL D.LGS 81/2008 E SS.MM.II

- Espletamento e gestione degli adempimenti in materia di tutela della salute e della sicurezza nei luoghi di lavoro ai sensi del D.Lgs 81/2008 e ss.mm.ii;

- Gestione dei rapporti con le Autorità di controllo in materia di tutela della salute e della sicurezza nei luoghi di lavoro, anche in occasione di verifiche e ispezioni (es. ASL, Vigili del Foco, Ispettorato del Lavoro etc..)

3) GESTIONE DEGLI ADEMPIMENTI IN MATERIA DI ASSUNZIONI, CESSAZIONE DEL RAPPORTO DI LAVORO, RETRIBUZIONI, RITENUTE FISCALI E CONTRIBUTI PREVIDENZIALI E ASSISTENZIALI, RELATIVI A DIPENDENTI E COLLABORATORI

- Gestione dei rapporti con Funzionari competenti (INPS, INAIL, ASL, Direzione Provinciali del Lavoro ec.), anche tramite il supporto di consulenti esterni, per l'osservanza degli obblighi previsti dalla normativa di riferimento:

- predisposizione delle denunce relative a costituzione, modifica ed estinzione del rapporto di lavoro;
- comunicazione elenchi del personale attivo, assunto e cessato presso l'INAIL;
- controlli e verifiche circa il rispetto dei presupposti e delle condizioni previste dalla normativa vigente;
- predisposizione ed esecuzione dei pagamenti verso gli Enti pubblici competenti.

- Gestione dei rapporti con i Funzionari Pubblici nell'ambito del rispetto dei presupposti e delle condizioni richieste dalla normativa vigente per le assunzioni agevolate, anche in occasione di verifiche ispettive:
  - Stipula di una Convenzione Ordinaria o di una Integrazione Lavorativa al fine di assolvere l'obbligo di assunzione dei disabili in maniera graduale e programmata;
  - Presentazione del prospetto informativo riportante la situazione occupazionale dell'azienda ai competenti uffici istituiti presso i Centri per l'Impiego di ciascuna Provincia;
  - Definizione del piano formativo, durata, rispetto dei limiti di età etc

4) GESTIONE DEI CONTENZIOSI GIUDIZIALI E DELLE PROBLEMATICHE CONNESSE

- Gestione dei rapporti con i Giudici, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito di procedimenti giudiziari (civili, penali, amministrativi) con particolare riferimento alla nomina dei legali e dei consulenti tecnici e di parte.
- Gestione dei rapporti con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale.

5) GESTIONE DEL SISTEMA INFORMATIVO AZIENDALE

- Utilizzo e gestione di software nell'ambito dei sistemi informativi aziendali;
- Gestione delle attività connesse all'implementazione, manutenzione e aggiornamento del sito internet e della rete telematica aziendale.

6) COORDINAMENTO E GESTIONE DELLA CONTABILITÀ GENERALE E FORMAZIONE DEL BILANCIO

- Coordinamento e gestione della contabilità generale, con particolare riferimento alle attività di:
  - Rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi, finanziari ed economici;
  - Corretta tenuta dei rapporti amministrativi con terzi (es. clienti e fornitori);
  - Gestione amministrativa e contabile dei cespiti;
  - Accertamenti di tutti gli altri fatti amministrativi in corso d'anno (es. costi del personale, penalità contrattuali, finanziamenti passivi e relativi interessi etc..).
- Raccolta e aggregazione dei dati contabili necessari per la predisposizione delle bozze di bilancio civilistico e/o consolidato;
- Collaborazione e supporto all'Organo Amministrativo nello svolgimento delle attività di ripartizione degli utili di esercizio, delle riserve e restituzione dei conferimenti.

7) GESTIONE DEGLI ADEMPIMENTI SOCIETARI

- Gestione dei rapporti con i Funzionari degli Enti competenti in materia di adempimenti societari (es. CCIAA);
- Gestione dei rapporti con la Corte dei Conti, il Collegio Sindacale, la Società di Revisione e i Soci nelle attività di verifica della gestione aziendale;
- Tenuta delle scritture contabili e dei Libri Sociali;
- Predisposizione della documentazione che sarà oggetto di discussione e delibera in Assemblea e gestione dei rapporti con tale Organo Sociale.

Sono stati inoltre individuati i processi nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato (processi c.d. funzionali/strumentali):

1. acquisti di beni, servizi e consulenze;
2. Rapporti con la Pubblica Amministrazione;
3. Gestione dei flussi monetari e finanziari;
4. Selezione, assunzione e gestione del personale;
5. Gestione dei rimborsi spese e delle spese di rappresentanza;

6.Gestione sponsorizzazioni, donazioni e omaggi;
7. Gestione della sicurezza sui luoghi di lavoro;
8. Gestione della sicurezza, manutenzione e sviluppo dei sistemi informativi;
9. Formazione del bilancio e gestione dei rapporti con Soci e Organi di Controllo.

2.11 Principi generali di controllo interno

Il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di esplicita formalizzazione delle norme comportamentali; chiara, formale e conoscibile descrizione ed individuazione delle attività, dei compiti e dei poteri attribuiti a ciascuna direzione e alle diverse qualifiche e ruoli professionali; precisa descrizione delle attività di controllo e loro tracciabilità; adeguata segregazione di ruoli operativi e ruoli di controllo.

In particolare devono essere perseguiti i seguenti principi generali di controllo interno:

<u>Norme comportamentali</u>

- Adozione del Codice Etico che descrive regole comportamentali di carattere generale a presidio delle attività svolte.

<u>Definizione di ruoli e responsabilità</u>

- Adozione di un Modello organizzativo e di un Organigramma interno, regolarmente aggiornati, che individuano ruoli e responsabilità delle direzioni, delle funzioni e delle unità organizzative, descrivendo in maniera omogenea le attività proprie di ciascuna struttura. Tale documento è disponibile, diffuso e conosciuto all'interno della organizzazione.

<u>Procedure e norme interne</u>

- Le attività sensibili devono essere regolamentate attraverso strumenti normativi aziendali così che si possano identificare le modalità operative di svolgimento delle attività, dei relativi controlli e le responsabilità di chi ha operato;
- Deve essere individuato e formalizzato un Responsabile per ciascuna attività sensibile, tipicamente coincidente con il responsabile della struttura organizzativa competente per la gestione dell'attività stessa;
- Le procedure e norme interne devono essere adeguatamente diffuse e devono essere oggetto di monitoraggio periodico ai fini di un loro aggiornamento in virtù del mutato contesto normativo e aziendale.

<u>Segregazione dei compiti</u>

- All'interno di ogni processo aziendale rilevante devono essere separati i soggetti incaricati della decisione e della sua attuazione rispetto a chi la registra e chi la controlla;
- Non deve esservi identità soggettiva tra coloro che assumono o attuano le decisioni, coloro che elaborano evidenze contabili delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- Deve esistere una chiara separazione dei compiti tra chi esegue, chi controlla e chi autorizza almeno in relazione agli aspetti più critici di ciascun processo;

- La segregazione dei compiti deve essere evidenziata nell'ambito delle procedure aziendali adottate.

Poteri di firma e poteri autorizzativi interni

- Deve essere definito un sistema di deleghe all'interno del quale vi sia una chiara identificazione ed una specifica assegnazione dei poteri di firma e autorizzativi interni e dei relativi limiti;
- I poteri autorizzativi e di firma (deleghe, procure e connessi limiti di spesa) devono essere coerenti con le responsabilità organizzative assegnate;
- Le procure devono essere coerenti con il sistema interno delle deleghe;
- Devono essere previsti meccanismi di pubblicità delle procure verso gli interlocutori esterni;
- Il sistema di deleghe deve identificare, tra l'altro:
    - I requisiti e le competenze professionali che il delegato deve possedere in ragione dello specifico ambito di operatività della delega;
    - L'accettazione espressa da parte del delegato o del subdelegato delle funzioni delegate e la conseguente assunzione degli obblighi conferiti;
    - Le modalità operative di gestione degli impegni di spesa.
- Le deleghe sono attribuite secondo i principi di:
    - Autonomia decisionale e finanziaria del delegato;
    - Idoneità tecnico-professionale del delegato;
    - Disponibilità di risorse adeguate al compito e continuità delle prestazioni.
- L'assunzione di impegni e la gestione dei rapporti di qualsivoglia natura con la Pubblica amministrazione sono riservate esclusivamente alle Aree aziendali a ciò preposte ed al personale autorizzato.

Attività di controllo e tracciabilità

- Nell'ambito delle procedure o di altra regolamentazione interna devono essere formalizzati i controlli operativi e le loro caratteristiche (responsabilità, evidenza, periodicità);
- La documentazione afferente alle attività sensibili deve essere adeguatamente formalizzata e archiviata in luogo idoneo alla conservazione, al fine di tutelare la riservatezza dei dati in essi contenuti e di evitare danni, deterioramenti e smarrimenti;
- Le fasi salienti delle attività sensibili devono essere oggetto di un'adeguata tracciabilità, finalizzata a:
    - Rendere chiaro chi ha svolto l'attività e chi ha effettuato il monitoraggio/controllo;
    - Permettere ad una terza persona di ripercorrere le fasi salienti del processo.
- Devono essere ricostruibili la formazione degli atti e i relativi livelli autorizzativi, lo sviluppo delle operazioni, materiali e di registrazione, con evidenza della loro motivazione e della loro causale, a garanzia della trasparenza delle scelte effettuate; deve essere prevista, laddove possibile, l'adozione di sistemi informatici, che garantiscano la corretta e veritiera imputazione di ogni operazione al soggetto che ne è responsabile e ai soggetti che vi partecipano. Il sistema deve prevedere l'impossibilità di modifica (non tracciata) delle registrazioni;
- Il responsabile dell'attività sensibile deve produrre e mantenere adeguati report di monitoraggio che contengano evidenza dei controlli effettuati e di eventuali anomalie; coloro che effettuano il controllo degli adempimenti connessi all'espletamento delle attività sensibili devono porre

particolare attenzione all'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità;
- La Società deve essere pertanto dotata di uno o più archivi di riferimento, disponibili in caso di controllo;
- I documenti riguardanti l'attività della Società, ed in particolare i documenti o la documentazione informatica riguardanti attività sensibili, sono archiviati e conservati, a cura della struttura organizzativa competente, con modalità tali da non permettere la modificazione successiva, se non con apposita evidenza;
- L'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate in base alle norme interne o a quanto loro delegato, al Collegio Sindacale od organo equivalente o altri organi di controllo interno, alla Società di Revisione e all'Organismo di Vigilanza;
- Nelle comunicazioni ufficiali verso la Pubblica Amministrazione deve essere assicurata la tracciabilità delle fonti e degli elementi informativi.

SEZIONE TERZA

3. Organismo di vigilanza

3.1. L'art. 6, comma 1 lett. b), del Decreto prevede che la funzione di vigilare e di curare l'aggiornamento del Modello sia affidata ad un Organismo di Vigilanza esterno dell'Ente che, dotato di autonomi poteri di iniziativa e di controllo, eserciti in via continuativa i compiti ad esso rimessi.

Non potrà essere nominato componente dell'Organismo di Vigilanza e, se nominato decade, l'interdetto, l'inabilitato, il fallito o chi è stato condannato, ancorché con condanna non definitiva, ad una pena che importi l'interdizione, anche temporanea, dai pubblici uffici o dagli uffici direttivi delle persone giuridiche ovvero sia stato condannato, anche con sentenza non definitiva o con sentenza di patteggiamento, per aver commesso uno dei reati previsti dal Decreto.

In ogni caso, il componente dell'Organismo di Vigilanza è scelto tra soggetti che non abbiano rapporti di parentela con i soci, gli Amministratori e il Management della Società, che ne possano compromettere l'indipendenza di giudizio.

In caso di nomina di un componente esterno, lo stesso non dovrà avere rapporti con la Società che possano configurare ipotesi di conflitto di interessi.

La ICTS ITALIA ha ritenuto idonea la costituzione di un Organismo di Vigilanza monocratico, funzionalmente dipendente dall'Amministratore Delegato. Il componente dell'Organismo, nominato dal Consiglio di Amministrazione previa valutazione dei requisiti di indipendenza e professionalità, è prescelto tra:

- Professionisti esterni, aventi comprovata esperienza nella materia di cui al Decreto.

Nello svolgimento delle proprie funzioni, l'Organismo di Vigilanza riferisce esclusivamente all'Amministratore Delegato o al Presidente del Consiglio di Amministrazione.

All'Organismo di Vigilanza sono attribuiti autonomi poteri di spesa che prevedono l'impiego di un budget annuo adeguato, approvato dall'Amministratore Delegato, su proposta dell'Organismo di Vigilanza. L'Organismo di Vigilanza può impegnare risorse che eccedono i propri poteri di spesa, dandone successivamente conto all'Amministratore Delegato.

In particolare, l'Organismo di Vigilanza deve avere i seguenti requisiti:

- Autonomia e indipendenza: detto requisito è assicurato dall'assenza di un rapporto gerarchico all'interno della organizzazione della Società, dalla facoltà di reporting all'Amministratore Delegato, dalla composizione dell'Organismo di Vigilanza il cui componente non si trovi in una posizione, neppure potenziale, di conflitto di interessi con la Società né è titolare all'interno della stessa di funzioni di tipo esecutivo;
- Onorabilità e professionalità: requisito questo garantito dal bagaglio di conoscenze professionali, tecniche e pratiche, di cui dispone il componente dell'Organismo di Vigilanza;
- Continuità dell'azione: con riferimento a tale requisito, l'Organismo di vigilanza è tenuto a vigilare costantemente, attraverso poteri di indagine, sul rispetto del Modello, a curarne l'attuazione e l'aggiornamento, rappresentando un riferimento costante per tutto il personale della Società.

Il componente dell'Organismo di Vigilanza resta in carica per 3 anni ed è in ogni caso rieleggibile.

3.2 Poteri e funzioni dell'Organismo di Vigilanza

All'Organismo di Vigilanza sono affidati i seguenti compiti:

- Vigilare sul funzionamento e osservanza del Modello;
- Curarne l'aggiornamento.

Tali compiti sono svolti dall'Organismo attraverso le seguenti attività:

- Vigilanza sulla diffusione nel contesto aziendale della conoscenza, della comprensione e dell'osservanza del Modello;
- Vigilanza sulla effettività del Modello, con particolare riferimento ai comportamenti riscontrati nel contesto aziendale, verificandone la coerenza rispetto ai principi di comportamento e di controllo definiti nel presente Modello;
- Disamina dell'adeguatezza del Modello, ossia della effettiva capacità del Modello di prevenire la commissione dei reati previsti dal Decreto;
- Analisi circa il mantenimento nel tempo dei requisiti di solidità e funzionalità del Modello;
- Formulazione di proposte di aggiornamento del Modello nell'ipotesi in cui si renda necessario e/o opportuno effettuare correzioni e/o adeguamenti dello stesso, in relazione alle mutate condizioni legislative e/o aziendali;
- Segnalazione, anche documentale, all'Amministratore Delegato di eventuali violazioni accertate nel modello organizzativo che possano comportare l'insorgere della responsabilità in capo alla Società.

Nello svolgimento di dette attività, l'Organismo provvederà ai seguenti adempimenti:

- Programmare ed erogare un piano periodico di formazione volto a favorire la conoscenza delle prescrizioni del Modello differenziato secondo il ruolo e la responsabilità dei destinatari;
- Documentare lo svolgimento dei suoi compiti;
- Raccogliere, elaborare, conservare e aggiornare ogni informazione rilevante ai fini della verifica dell'osservanza del Modello;
- Verificare e controllare periodicamente le aree/operazioni a rischio individuate nel Modello.

Al fine di consentire all'Organismo la migliore conoscenza in ordine all'attuazione del Modello, alla sua efficacia e al suo effettivo funzionamento, nonché alle esigenze di aggiornamento dello stesso, è fondamentale che l'Organismo di Vigilanza operi in stretta collaborazione con le Aree aziendali.
Ai fini dello svolgimento degli adempimenti sopra elencati, l'Organismo è dotato dei poteri di seguito indicati:

- Accedere liberamente, senza autorizzazione, a ogni documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'Organismo ai sensi del D.lgs. 231/2001;
- Disporre che i responsabili delle Direzioni Aziendali, e in ogni caso tutti i destinatari, forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare e approfondire aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso da parte delle strutture aziendali; a tal fine è facoltà dell'Organismo di eseguire interviste e raccogliere informazioni;
- Ricorrere a consulenti esterni nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello;

3.3 Reporting dell'Organismo di Vigilanza

Al fine di garantire la piena autonomia e indipendenza nello svolgimento delle relative funzioni, l'Organismo di Vigilanza comunica direttamente all'Amministratore Delegato e al Sindaco Unico, lo stato di fatto sull'attuazione del Modello, gli esiti delle attività di vigilanza svolta e gli eventuali interventi opportuni per l'implementazione del Modello. Segnatamente, l'Organismo di Vigilanza riferisce secondo le seguenti modalità:

- Almeno semestralmente nei confronti dell'Amministratore Delegato attraverso una relazione scritta in ordine all'attuazione del Modello, all'esercizio delle proprie funzioni di vigilanza nei confronti dei destinatari del Modello e, in particolare, in ordine all'osservanza, da parte di questi, del Modello stesso, nonché all'adeguatezza e all'aggiornamento del Modello;
- Almeno annualmente nei confronti del Sindaco Unico e della Società di revisione, ovvero su richiesta degli stessi, in ordine alle attività svolte.

3.4 Flussi informativi nei confronti dell'Organismo di Vigilanza

Il Decreto enuncia, tra le esigenze che il Modello deve soddisfare, l'istituzione di obblighi informativi nei confronti dell'Organismo di Vigilanza. Detti flussi riguardano tutte le informazioni e i documenti che devono essere portati a conoscenza dell'Organismo di Vigilanza.

Per ciascuna "area a rischio reato", è identificato un "Responsabile Interno" che dovrà, tra l'altro, fornire all'Organismo di Vigilanza, almeno con cadenza semestrale, i flussi informativi così come definiti dall'Organismo stesso. Anche nel caso in cui, nel periodo selezionato, non vi siano state segnalazioni

significative da comunicare all'Organismo di Vigilanza, allo stesso dovrà essere inviata una segnalazione "negativa".

Sono stati inoltre istituiti precisi obblighi gravanti sugli organi sociali e sul personale della ICTS ITALIA S.R.L., e in particolare:

- I destinatari devono riferire all'Organismo di Vigilanza ogni informazione relativa a comportamenti che possano integrare violazioni o presunte violazioni delle prescrizioni del Modello o fattispecie di reato;
- Gli organi sociali devono riferire all'Organismo di Vigilanza ogni informazione rilevante per il rispetto e il funzionamento del Modello.

Oltre alle informazioni sopraindicate, devono essere obbligatoriamente trasmesse all'Organismo di Vigilanza le seguenti informazioni:
(i) i piani di comunicazione e formazione sui principi e i contenuti del Decreto e del Modello di organizzazione gestione e controllo;
(ii) i piani e i risultati delle attività di controllo e di audit svolte all'interno della Società, in relazione a processi e attività rilevanti ai sensi del presente Modello;
(iii) le analisi di risk assessment e di mappatura delle attività e dei processi rilevanti in funzione del Modello Organizzativo;
(iv) gli eventuali procedimenti disciplinari avviati per violazione del Modello e i relativi provvedimenti sanzionatori o di archiviazione, con le relative motivazioni;
(v) i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra Autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per ipotesi di reato di cui al D.lgs 231/01, che riguardino direttamente o indirettamente la Società;
(vi) le richieste di assistenza legale inoltrate dai componenti gli organi sociali, dai dirigenti e/o dagli altri dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto, che riguardino direttamente o indirettamente la Società;
(vii) eventuali ispezioni, accertamenti e visite promossi dalla Pubblica Amministrazione o da altri Enti competenti nei confronti della Società e i relativi contenziosi in essere;
(viii) modifiche nel sistema delle deleghe e delle procure, modifiche statutarie o modifiche dell'organigramma aziendale;
(ix) segnalazione di infortuni gravi, rientrando in tale categoria quegli infortuni sul lavoro con prognosi superiore ai 40 giorni occorsi ai dipendenti, appaltatori, subappaltatori e/o collaboratori presenti nei luoghi di lavoro della Società.
I destinatari del presente Modello possono, inoltre, trasmettere all'Organismo di Vigilanza indicazioni e suggerimenti relativi all'attuazione, all'adeguatezza e all'aggiornamento del Modello Organizzativo.
L'Organismo di Vigilanza raccoglierà e valuterà tutte le informazioni e le segnalazioni pervenutegli.
È rimesso alla discrezionalità dell'Organismo di Valutazione valutare, sulla base delle segnalazioni ricevute, le iniziative da assumere. In particolare potrà convocare, qualora lo ritenga opportuno, sia il segnalante per ottenere maggiori informazioni sia l'eventuale presunto autore della violazione, dando inoltre luogo a tutti gli accertamenti e le indagini che ritenga necessarie per appurare la fondatezza della segnalazione.
Le segnalazioni dovranno essere in forma scritta e possono essere in forma anonima. Pertanto, è obbligo dell'Organismo di Vigilanza agire in modo da garantire i segnalanti contro qualsiasi forma di ritorsione,

discriminazione o penalizzazione, fatti salvi gli obblighi di legge a tutela dei diritti della Società e dei terzi, assicurando l'anonimato del segnalante e la riservatezza dei fatti dal medesimo segnalati.
Tutte le informazioni, la documentazione e le segnalazioni raccolte nell'espletamento dei compiti istituzionali devono essere archiviate e custodite, per almeno 5 anni, dall'Organismo di valutazione, avendo cura di mantenere riservati i documenti e le informazioni acquisite, anche nel rispetto della normativa sulla privacy.

SEZIONE QUARTA

4. Informazione, formazione del personale e aggiornamento del Modello

4.1 Comunicazione del Modello e formazione del personale

La comunicazione del Modello Organizzativo e di Controllo e la formazione del personale rappresentano per la Società fondamentali requisiti per l'attuazione del Modello stesso.
È obiettivo della Società garantire la corretta divulgazione e conoscenza del Modello Organizzativo e di Controllo nei confronti delle risorse già presenti in azienda, di quelle da inserire, nonché dei collaboratori, partner e terzi che intrattengono rapporti con ICTS ITALIA.
Il Modello Organizzativo e di controllo è comunicato mediante consegna e sottoscrizione della dichiarazione di ricezione, presa d'atto ed accettazione dei suddetti documenti.
Inoltre, in relazione alle controparti con cui ICTS ITALIA instaura rapporti contrattuali, la Società informa le stesse circa l'adozione e l'attuazione del Codice Etico e del Modello Organizzativo e di controllo, ai sensi del D.lgs. 231/2001, mediante inserimento nei contratti di specifica clausola con cui la Società richiede alle controparti di uniformarsi, nell'ambito dei rapporti commerciali con la Società, ai principi di comportamento di cui al Codice Etico di ICTS ITALIA, pubblicato sul sito internet della Società.
ICTS ITALIA si impegna a favorire la conoscenza e la comprensione del Modello Organizzativo sia da parte dei soggetti apicali sia da parte dei dipendenti, attraverso:

- Appositi corsi di formazione, con grado di approfondimento diversificato, a seconda dell'inquadramento, della posizione e del ruolo;
- Corsi di formazione estesi, di volta in volta, ai neo-assunti.

La partecipazione ai corsi è obbligatoria. Le rispettive presenze, nonché le informative, dovranno essere opportunamente tracciate. In particolare, la struttura e la calendarizzazione dei corsi, dei seminari e di eventuali altre iniziative vengono approvate dall'Organismo di Vigilanza, su proposta dell'Area Aziendale competente. L'Organismo di Vigilanza provvederà a monitorare l'attuazione delle iniziative di formazione e comunicazione.
La formazione avrà i seguenti contenuti ed obiettivi minimi, da adattarsi in relazione alle specifiche esigenze organizzative della Società e ai diversi livelli di destinatari:

- Illustrare il Modello e il Codice Etico ed approfondirne il contenuto;
- Informare il personale sul sistema delle segnalazioni e dei flussi informativi previsti dal Modello;
- Informare e formare sul sistema di principi di controllo e di comportamento previsti dal Modello;
- Favorire lo scambio di informazioni sulle aree a rischio della Società e sul relativo sistema di controllo;
- Informare sui comportamenti etici richiesti dalla Società e su quanto richiesto ai fornitori.

Tutte le iniziative formative adottate dovranno essere adeguatamente tracciate.

4.2 Aggiornamento del Modello

L'adozione e l'efficace attuazione del Modello sono – per espressa previsione legislativa – una responsabilità rimessa all'Amministratore Delegato. Ne deriva che il potere di adottare eventuali aggiornamenti del Modello compete, dunque, all'Amministratore Delegato.
L'attività di aggiornamento, intesa sia come integrazione sia come modifica, è volta a garantire l'adeguatezza e l'idoneità del Modello, valutate rispetto alla funzione preventiva di commissione dei reati previsti dal Decreto. Compete all'Organismo di Vigilanza la concreta verifica circa la necessità od opportunità di procedere all'aggiornamento del Modello.

SEZIONE QUINTA

5. Sistema Disciplinare

A mente di quanto previsto dagli artt. 6 e 7 del Decreto, la Società ha adottato anche un Sistema Disciplinare, integrato nel Codice Etico, volto a sanzionare le eventuali violazioni del Modello stesso e degli Allegati ad esso connessi, incluso lo stesso Codice Etico.
Nel rispetto di quanto previsto anche dalle Linee Guida di Confindustria, è previsto che l'instaurazione di un procedimento disciplinare e l'applicazione delle relative sanzioni prescindono dall'instaurazione e/o dall'esito di eventuali procedimenti penali aventi ad oggetto le medesime condotte rilevanti ai fini del Sistema Disciplinare.
Le previsioni contenute nel Sistema Disciplinare non precludono la facoltà dei soggetti destinatari di esercitare tutti i diritti, ivi inclusi quelli di contestazione o di opposizione avverso il provvedimento disciplinare ovvero di costituzione di un Collegio Arbitrale, loro riconosciuti da norme di legge o dalla contrattazione collettiva.
Dopo una sintetica premessa in cui sono delineati i principi generali concernenti il sistema sanzionatorio costituito nell'ambito del Modello, il Sistema Disciplinare illustra:

- i criteri di applicazione delle sanzioni;
- le violazioni sanzionabili;
- le misure nei confronti di ciascuna delle categorie di Destinatari (dipendenti, dirigenti, lavoratori autonomi, amministratori e cd. Terzi Destinatari).

PARTE SPECIALE "A" – REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

A.1 La tipologia dei reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del Decreto)

Per quanto concerne la presente Parte Speciale "A" di seguito si rimette una breve descrizione dei reati in essa contemplati, indicati negli artt. 24 e 25 del Decreto e suddivisi tra: reati potenzialmente realizzabili e reati che, per quanto non si possano escludere tout court, sono stati ritenuti remoti in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente coperti dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico adottato dalla Società. L'identificazione delle aree di attività a rischio di commissione dei reati previsti e le considerazioni svolte

sulla possibile realizzabilità dei predetti reati, sono state realizzate anche attraverso le interviste ai soggetti aziendali di ciascuna Area aziendale competente, come tali provvisti della più ampia e approfondita conoscenza della operatività di ciascun singolo settore della attività aziendale.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Corruzione per un atto di ufficio o contrario ai doveri di ufficio (**artt. 318 – 319 c.p)**

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere o ritardare atti del suo ufficio (determinando un vantaggio in favore dell'offerente). L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio il pubblico ufficiale che accetta denaro per garantire la aggiudicazione di una gara). Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

Corruzione in atti giudiziari (art. 319 – ter c.p.)

Tale ipotesi di reato si configura nel caso in cui i fatti indicati negli artt. 318 e 319 c.p. sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo. Il reato di corruzione in atti giudiziari può essere commesso nei confronti di giudici o membri del Collegio Arbitrale competenti a giudicare sul contenzioso/arbitrato nell'interesse dell'Ente (compresi gli ausiliari e i periti d'ufficio), e/o di rappresentanti della Pubblica Amministrazione, quando questa sia una parte nel contenzioso, al fine di ottenere illecitamente decisioni giudiziali e/o stragiudiziali favorevoli.

Pene per il corruttore (art. 321 c.p.)

Le pene stabilite nel primo comma dell'art. 318, nell'art. 319, nell'art. 319 – bis, nell'art. 319 – ter e nell'art. 320 c.p., in relazione alle suddette ipotesi degli artt. 318 e 319 c.p., si applicano anche a chi dà o premette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro o altre utilità.

Istigazione alla corruzione (art. 322 c.p.)

Tale ipotesi di reato si configura nei confronti di chiunque offra o prometta denaro o altra utilità non dovuti ad un pubblico ufficiale o incaricato di pubblico servizio che rivesta la qualità di pubblico impiegato per indurlo a compiere, omettere o ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri e tale offerta e promessa non sia accettata.

Induzione indebita a dare o promettere utilità (art. 319 – quater c.p.)

Tale ipotesi di reato punisce la condotta dei soggetti apicali o dei soggetti subordinati che siano indotti a versare o promettere denaro o altra utilità, in ragione dell'abuso di potere del pubblico ufficiale o l'incaricato di pubblico servizio.

Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea (art. 640, comma 2 n. 1, c.p.)

La fattispecie prevede un reato comune che può essere commesso da chiunque. Il fatto che costituisce reato consiste nel procurare a sé o ad altri un ingiusto profitto a danno di un'altra persona (in questa fattispecie il danno deve essere subito dallo Stato o da altro ente pubblico, inducendo, mediante artifici o raggiri, taluno in errore. Tale reato può realizzarsi, ad esempio, nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta), al fine di ottenere l'aggiudicazione della gara stessa.

Truffa aggravata per il conseguimento di erogazione pubbliche (art. 640 – bis c.p.)

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche.

Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

È opportuno notare che il reato di cui all'art. 640 – bis assume carattere generale, rispetto a quello previsto dall'art. 316 – ter (cfr. infra) che assume, invece, carattere sussidiario. Inoltre il reato in questione può facilmente concorrere con quello di cui all'art. 316 – bis, in quanto può concretizzare condotte prodromiche alla erogazione del contributo distratto dalla destinazione prevista.

Malversazione a danno dello Stato o dell'Unione Europea (art. 316 – bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'aver distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta). Tenuto conto che il consumo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

Indebita percezione di erogazioni in danno dello Stato e dell'Unione Europea (art. 316-ter c.p.)

Tale ipotesi di reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute – si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione Europea. In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316 –bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti. Infine va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato.

Concussione (art. 317 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, abusando della sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli. Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal

Decreto; in particolare, tale forma di reato potrebbe ravvisarsi, nell'ambito di applicazione del decreto stesso, nell'ipotesi in cui un dipendente o agente della società concorra nel reato del pubblico ufficiale, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute (sempre che, da tale comportamento derivi in qualche modo un vantaggio per la società).

Circostanze aggravanti (art. 319 – bis c.p.)

La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene nonché il pagamento o il rimborso di tributi.

Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari della Comunità Europea e degli Stati esteri (art. 322 – bis c.p.)

Le disposizioni degli artt. 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:

1) ai membri della Commissione delle Comunità Europee, del Parlamento Europeo, della Corte di Giustizia e della Corte dei Conti delle Comunità Europee;

2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità Europee o del regime applicabile agli agenti delle Comunità Europee;

3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità Europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità Europee;

4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità Europee;

5) a coloro che, nell'ambito di altri Stati Membri dell'Unione Europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio.

Le disposizioni degli artt. 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:

1) alle persone indicate nel primo comma del presente paragrafo;

2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali.

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di pubblico servizio negli altri casi.

A.2 Aree a rischio

I reati sopra considerati trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione. Le aree di attività ritenute più specificatamente a rischio ai fini della presente Parte Speciale "A" sono:

- GESTIONE DEI RAPPORTI DI PROFILO ISTITUZIONALE CON SOGGETTI APPARTENENTI ALLA PUBBLICA AMMINISTRAZIONE

- Gestione dei rapporti di "alto profilo" con soggetti istituzionali e/o altri soggetti appartenenti a Enti pubblici di rilevanza nazionale e internazionale in occasione di incontri, conferenze, tavoli di lavoro, eventi promozionali e di divulgazione istituzionale.

- GESTIONE DEI RAPPORTI E DEGLI ADEMPIMENTI VERSO ENTI PUBBLICI E AUTORITÀ AMMINISTRATIVE INDIPENDENT O ORGANI DI VIGILANZA, ANCHE IN OCCASIONE DI VERIFICHE ED ISPEZIONI

- Gestione dei rapporti, anche per via telematica e anche in fase di verifiche ispettive, con Enti pubblici e Autorità Amministrative Indipendenti, quali a titolo esemplificativo:
  1) Gestione dei rapporti con i Funzionari di Guardia di Finanza, dell'Agenzia delle Entrate e degli altri Enti competenti in materia fiscale e tributaria, anche in occasione di verifiche, ispezioni ed accertamenti e gestione delle relative comunicazioni;
  2) Gestione delle comunicazioni e degli adempimenti nei confronti dell'Autorità Garante della Privacy, anche in occasione di visite ispettive, ai sensi del Regolamento UE 2016/679;
  3) gestione delle comunicazioni e degli adempimenti richiesti dall'Autorità di Vigilanza sui contratti pubblici, anche in occasione di visite ispettive.

- GESTIONE DEL SISTEMA SICUREZZA AI SENSI DEL D.LGS 81/2008 (TSTO UNICO SICUREZZA) E SS.MM.II.

- Espletamento e gestione degli adempimenti in materia di tutela della salute e della sicurezza nei luoghi di lavoro, ai sensi del D.Lgs 81/2008 e ss.mm.ii.;

- Gestione dei rapporti con le Autorità di controllo in materia di tutela della salute e della sicurezza nei luoghi di lavoro, anche in occasione di verifiche e ispezioni (es. ASL, Vigili del Fuoco, Ispettorato del Lavoro etc.).

- GESTIONE DEGLI ADEMPIMENTI IN MATERIA DI ASSUNZIONI, CESSAZIONE DEL RAPPORTO DI LAVORO, RETRIBUZIONI, RITENUTE FISCALI E CONTRIBUTI PREVIDENZIALI E ASSISTENZIALI, RELATIVI A DIPENDENTI E COLLABORATORI

- Gestione dei rapporti con Funzionari competenti (INPS, INAIL, ASL, Direzione Provinciale del Lavoro ecc.), anche tramite il supporto di un consulente esterno, per l'osservanza degli obblighi previsti dalla normativa di riferimento:
  1) predisposizione delle denunce relative a costituzione, modifica ed estinzione del rapporto di lavoro;
  2) comunicazione elenchi del personale attivo, assunto e cessato presso l'INAIL;
  3) controlli e verifiche circa il rispetto dei presupposti delle condizioni previste dalla normativa vigente;
  4) predisposizione ed esecuzione dei pagamenti verso gli Enti pubblici competenti.

- Gestione dei rapporti con i Funzionari Pubblici nell'ambito del rispetto dei presupposti e delle condizioni richieste dalla normativa vigente per le assunzioni agevolate, anche in occasione di verifiche ispettive:
  1) stipula di una Convenzione Ordinaria o di Integrazione Lavorativa al fine di assolvere l'obbligo di assunzione dei disabili in maniera graduale e programmata;
  2) presentazione del prospetto informativo riportante la situazione occupazionale dell'azienda ai competenti uffici istituiti presso i Centri per l'impiego di ciascuna Provincia;
  3) definizione del Piano formativo, durata, rispetto dei limiti di età, etc.

- GESTIONE DEI CONTENZIOSI GIUDIZIALI E PROBLEMATICHE CONNESSE

- Gestione dei rapporti con i Giudici, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito di procedimenti giudiziari (civili, penali, amministrativi), con particolare riferimento alla nomina dei legali e dei consulenti tecnici di parte.

- GESTIONE DEGLI ADEMPIMENTI SOCIETARI

- Gestione dei rapporti con i Funzionari degli enti competenti in materia di adempimenti societari (ad es. CCIAA);
- Gestione dei rapporti con la Corte dei Conti, la società di revisione e i soci nelle attività di verifica della gestione aziendale.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'Organismo di Vigilanza in considerazione del verificarsi di fattori esterni (ad esempio legislativi, come la introduzione di nuove categorie di reati) o di fattori interni (ad esempio le modifiche organizzative o di business).

A.3 Destinatari della Parte Speciale e principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale.
In particolare la presente Parte Speciale ha la funzione di:

- Fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- Fornire all'Organismo di Vigilanza e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifiche previste.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale, la presente Parte Speciale prevede l'espresso divieto a carico del Destinatari del Modello di:

- Porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate;
- Porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarle;
- Porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Obiettivo della presente Parte Speciale è che tutti i Destinatari adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di impedire il verificarsi dei reati previsti nel Decreto ed in

particolare sono tenuti a osservare, oltre ai principi generali enunciati nella Parte Generale, i seguenti principi:

- Stretta osservanza di tutte le leggi e regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione;
- Instaurazione e mantenimento di qualsiasi rapporto con i terzi in tutte le attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio sulla base di criteri di correttezza e trasparenza che garantiscano il buon andamento della funzione o servizio e imparzialità nello svolgimento degli stessi.

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

- Effettuare, ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia a pubblici funzionari;
- Distribuire omaggi al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo offerto o ricevuto eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei paesi in cui la elargizione di doni rappresenta una prassi), o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico (ad esempio la distribuzione di libri d'arte), o il brand image della Società. I regali offerti – salvo quelli di modico valore – devono essere documentati in modo adeguato per consentire le prescritte verifiche;
- Accordare altri vantaggi di qualsiasi natura (promesse di assunzione ecc) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al precedente punto;
- Effettuare prestazioni in favore dei consulenti, dei Partner e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere;
- Presentare dichiarazioni non veritiere a organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- Destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazione, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
- Alterare il funzionamento di sistemi informativi e tematici o manipolare i dati in essi contenuti;
- Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari ecc) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità;
- Nei rapporti con interlocutori appartenenti alla Pubblica Amministrazione è fatto divieto di effettuare spese di rappresentanza (rimborso di viaggi, soggiorni ecc) ingiustificate;
- Inoltre, nei confronti della Pubblica Amministrazione è fatto espresso divieto di:
  1) esibire documenti e dati incompleti e/o comunicare dati falsi e alterati;
  2) sottrarre o omettere l'esibizione di documenti veri;

3) omettere informazioni dovute;

- Nel corso dei processi civili, penali o amministrativi, è fatto divieto di porre in essere (direttamente o indirettamente) qualsiasi attività che possa favorire o danneggiare una delle parti in causa;
- In particolare, a titolo meramente esemplificativo e non esaustivo, è fatto divieto di elargire, promettere o dare denaro o altra utilità a giudici, arbitri, funzionari di cancelleria, periti, testimoni, ecc. ovvero a persone comunque indicate da codesti soggetti, nonché adottare comportamenti – anche a mezzo di soggetti terzi (es. professionisti esterni) – contrari alla legge e ai presidi aziendali, per influenzare indebitamente le decisioni dell'organo giudicante ovvero le posizioni della Pubblica Amministrazione, quando questa sia una parte nel contenzioso;
- È altresì fatto divieto di favorire indebitamente gli interessi della Società inducendo con violenza o minaccia, o, alternativamente, con offerta di danaro o altra utilità, a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale;
- Nell'ambito di ispezioni effettuate da parte delle autorità di vigilanza presso la sede della società, dovrà essere assicurata la presenza di almeno due soggetti appartenenti alla Struttura interessata dall'Ispezione, fatte salve le situazioni particolari delle quali dovrà essere data espressa e tempestiva comunicazione all'organismo di vigilanza.

A. 4 Responsabile interno

Per ogni area a rischio l'Amministratore Delegato della Società, o un dirigente da questi incaricato, nomina un "Responsabile Interno".
Il responsabile interno:

- Diviene il soggetto referente e responsabile delle attività a rischio;
- Garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- Collabora con l'Organismo di Vigilanza nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- Comunica tempestivamente all'Organismo di Vigilanza eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'Organismo di Vigilanza.

A.5 Processi strumentali

Di seguito sono riportati i processi c.d. strumentali nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reati di cui alla presente Parte Speciale:

- Acquisti di beni, servizi e consulenze;
- Rapporti con la Pubblica Amministrazione e con le Autorità Amministrative Indipendenti;
- Gestione dei flussi monetari e finanziari;
- Selezione, assunzione e gestione del personale;

- Gestione dei rimborsi spese e delle spese di rappresentanza;
- Gestione sponsorizzazioni, donazioni e omaggi;
- Gestione della sicurezza sui luoghi di lavoro;
- Formazione del bilancio e gestione dei rapporti con Soci e Organi di controllo.

PARTE SPECIALE "B" – REATI SOCIETARI

B. 1 Le tipologie dei reati societari (art. 25-ter del Decreto)

Per quanto concerne la presente Parte Speciale "B", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati e indicati all'art. 25 – ter del Decreto (di seguito i Reati Societari) e suddivisi tra: reati potenzialmente realizzabili e reati che, per quanto non si possano escludere tout court, sono stati ritenuti remoti in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente coperti dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico adottato dalla Società. L'identificazione delle aree di attività a rischio di commissione dei reati previsti e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, è stata realizzata anche attraverso le interviste ai soggetti aziendali di ciascuna Area aziendale competente, come tali provvisti della più ampia e profonda conoscenza della operatività di ciascun singolo settore dell'attività aziendale.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

False comunicazioni sociali e comunicazioni sociali in danno della Società, dei Soci o dei Creditori (artt. 2621 e 2622 c.c.)

I reati previsti dagli artt. 2621 e 2622 c.c. possono essere commessi esclusivamente dagli amministratori, dai direttori generali, dai dirigenti preposti alla redazione dei documenti contabili societari, dai sindaci o dai liquidatori della società. La fattispecie prevista dall'art. 2621 c.c. è configurata come contravvenzione, mentre quella prevista dall'art. 2622 c.c. è configurata come delitto, punito a querela della persona offesa se commesso da amministratori, da direttori generali, dai dirigenti preposti alla redazione dei documenti contabili societari , dai sindaci o dai liquidatori di una società non quotata (art. 2622, primo comma, c.c.) e perseguibile d'ufficio se commesso dai medesimi esponenti di una società quotata (art. 2622, terzo comma, c.c.). l'elemento che distingue la contravvenzione ex art. 2621 c.c. dalle due fattispecie delittuose di cui all'art. 2622 c.c. è costituito dall'avere, in questi ultimi due casi, cagionato un danno patrimoniale alla società, ai soci o ai creditori. Oggetto delle condotte punibili sono i bilanci, le relazioni o le altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico. Le false informazioni punibili hanno ad oggetto la situazione economica, patrimoniale o finanziaria della società o del gruppo (nel caso che si tratti di bilancio consolidato). La punibilità è estesa anche all'ipotesi nella quale le informazioni riguardino beni posseduti o amministrati dall'ente per conto di terzi. Le modalità della condotta incriminata possono estrinsecarsi tanto in forma attiva (esposizione dei fatti materiali non rispondenti al vero, ancorché oggetto di valutazione) quanto in forma omissiva. Per quanto concerne la forma attiva, è opportuno considerare che il canone interpretativo maggiormente rigoroso include nell'area del penalmente rilevante anche le valutazioni verificabili attraverso parametri idonei (escludendo le valutazioni di natura schiettamente soggettiva). Quanto alla forma omissiva, il fatto è

integrato dalla omissione di informazioni imposte dalla legge (viene quindi in considerazione ogni legge che imponga una comunicazione con obblighi specifici nonché con clausole generali che rimandino al principio della completezza dell'informazione): con riferimento alle valutazioni, si può ipotizzare che l'omessa indicazione dei criteri utilizzati per le valutazioni possa integrare una omissione significativa.
Il mancato superamento anche di una delle soglie quantitative stabilite (variazione del 5% del risultato economico di esercizio al lordo delle imposte; variazione dell'1% del patrimonio netto; variazione del 10% rispetto alla valutazione corretta per le valutazioni estimative) importa per ciò solo la non rilevanza penale del fatto. Residua tuttavia in tali ipotesi, la configurabilità di un illecito amministrativo di cui sono chiamati a rispondere amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci o liquidatori. L'illecito amministrativo in discorso, che non genera responsabilità diretta dell'Ente ai sensi del D.Lgs 231/2001, è punito con la sanzione pecuniaria da 10 a 100 quote e con le sanzioni della "interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché di ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa".

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
Tale ipotesi di reato consiste nella effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o di scissioni, tali da cagionare danno ai creditori. Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Impedito controllo (art. 2625 c.c.)
Tale ipotesi di reato consiste nell'impedire o ostacolare, mediante occultamento di documenti o altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali qualora tale condotta abbia cagionato un danno ai soci.
L'illecito può essere commesso esclusivamente dagli amministratori.

Formazione fittizia del capitale (art. 2632 c.c.)
Tale ipotesi di reato è integrata dalle seguenti condotte: a) formazione o aumento in modo fittizio del capitale sociale mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale; b) sottoscrizione reciproca di azioni o quote; c) sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori e i soci conferenti.
Si precisa che non è, invece, incriminato l'omesso controllo ed eventuale revisione da parte di amministratori e sindaci, ai sensi dell'art. 2343, III comma, c.c., della valutazione dei conferimenti in natura contenuta nella relazione di stima redatta dall'esperto nominato dal Tribunale.

Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di Vigilanza (art. 2638 c.c.)
Si tratta di due ipotesi di reato distinte per modalità di condotta e momento offensivo:

- La prima si realizza (i) attraverso l'esposizione nelle comunicazioni previste dalla legge alle Autorità pubbliche di Vigilanza (al fine di ostacolare l'esercizio delle funzioni di quest'ultime) di fatti materiali non rispondenti al vero, ancorché oggetto di valutazione, sulla situazione

economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza ovvero (ii) mediante l'occultamento, con altri mezzi fraudolenti, di fatti che avrebbero dovuto essere comunicati e concernenti la medesima situazione economica, patrimoniale o finanziaria. La responsabilità sussiste anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;

- La seconda si realizza con il semplice ostacolo all'esercizio delle funzioni di vigilanza svolte da parte di pubbliche Autorità, attuato consapevolmente e in qualsiasi forma, anche omettendo le comunicazioni dovute alle Autorità medesime.

Il termine "Autorità pubblica di Vigilanza" è chiaramente generico, completamente indeterminato e fa sorgere rilevanti dubbi interpretativi. In maniera precauzionale il termine è stato interpretato in maniera tale da includere tutte le autorità amministrative esistenti nel nostro sistema giuridico senza considerare il tipo di vigilanza concretamente svolto dalle stesse e l'indipendenza dal potere politico: pertanto, l'autorità garante per la protezione dei dati personali (così come l'autorità garante della concorrenza e del mercato e l'autorità per la garanzia nelle comunicazioni) può essere considerata autorità di vigilanza. L'esercizio delle funzioni di tali autorità è tutelato dal dettato normativo dell'art. 2638 c.c.

Dato quanto sopra, il reato di cui all'art. 2368 c.c. deve essere riferito a specifiche e determinate tipologie di informazione, che possono attenere alla posizione economica e finanziaria del soggetto sottoposto alla vigilanza dell'autorità in questione. Tale requisito richiesto espressamente dalla legge limita la sua applicazione e richiede di riflettere sulla tipologia di dati e informazioni che nel caso specifico verranno comunicati all'autorità di vigilanza. Il reato si realizza solo quando l'informazione comunicata ha le caratteristiche previste dalla legge.

Considerazioni analoghe devono essere fatte con riferimento ai rapporti della Società con le altre autorità di vigilanza.

Soggetti attivi dell'ipotesi di reato descritta sono gli amministratori, i direttori generali, i sindaci e i liquidatori.

Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)

Tale ipotesi di reato consiste nella ripartizione di utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, ovvero nella ripartizione di riserve (anche non costituite con utili) che non possono per legge essere distribuite.

Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima delle termie previsto per l'approvazione del bilancio estingue il reato.

Soggetti attivi del reato sono gli amministratori. Il decreto non ha inteso punire anche i soci beneficiari della ripartizione degli utili o delle riserve, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

Corruzione tra privati (art. 2635 c.c.)

Tale ipotesi di reato rileva ai fini della responsabilità amministrativa dell'ente qualora i soggetti apicali o i soggetti subordinati diano o promettano denaro o altra utilità a:

- Amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori di altre società;
- Coloro che siano sottoposti alla direzione o alla vigilanza di uno dei soggetti di cui al punto che precede.

Si fa presente che l'ente risponderà del reato quando i predetti soggetti agiscano come corruttori, non anche quando siano stati corrotti.

Indebita restituzione dei conferimenti (art. 2626 c.c.)

Tale ipotesi di reato consiste nel procedere, fuori dei casi di legittima riduzione del capitale sociale, alla restituzione, anche simulata, dei conferimenti ai soci o alla liberazione degli stessi dall'obbligo di eseguirli.
Soggetti attivi del reato sono gli amministratori. Il decreto non ha inteso punire anche i soci beneficiari della ripartizione degli utili o delle riserve, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

Illecita influenza sull'assemblea (art. 2636 c.c.)

Tale ipotesi di reato consiste nel determinare la maggioranza in assemblea con atti simulati o fraudolenti, allo scopo di conseguire, per sé o per altri, un ingiusto profitto.
Il reato è costruito come reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

I reati la cui commissione è stata ritenuta remota sono i seguenti:
Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)

Tale ipotesi di reato consiste nella ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Soggetti attivi del reato sono esclusivamente i liquidatori.

Omessa comunicazione del conflitto di interessi (art. 2629 c.c.)

Tale ipotesi di reato consiste nella violazione degli obblighi previsti dall'art. 2391, comma primo, c.c. da parte dell'amministratore

Estensione delle qualifiche soggettive (art. 2639 c.c.)

Per tutti i reati previsti dal paragrafo B.1, al soggetto formalmente investito della qualifica o titolare della funzione prevista dalla legge civile è equiparato sia chi è tenuto a svolgere la stessa funzione, diversamente qualificata, sia chi esercita in modo continuativo e significativo i poteri tipici inerenti alla qualifica o alla funzione.

Fuori dei casi di applicazione delle norme riguardanti i delitti dei pubblici ufficiali contro la pubblica amministrazione, le disposizioni sanzionatorie relative agli amministratori si applicano anche a coloro che sono legalmente incaricati dall'autorità giudiziaria o dall'autorità di pubblica vigilanza di amministrare la società o i beni dalla stessa posseduti o gestiti per conto di terzi.

B.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree di attività ritenute più specificatamente a rischio, ai fini della presente Parte speciale "B" del Modello, e le correlate "attività sensibili", risultano essere le seguenti:

- COORDINAMENTO E GESTIONE DELLA CONTABILITÀ GENERALE E FORMAZIONE DEL BILANCIO

- Coordinamento e gestione della contabilità generale, con particolare riferimento alle attività di:
  a) rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi, finanziari ed economici;
  b) corretta tenuta dei rapporti amministrativi con i terzi (es. clienti, fornitori etc.);
  c) gestione amministrativa e contabile dei cespiti;
  d) accertamenti di tutti gli altri fatti amministrativi in corso d'anno (es. costi del personale, penalità contrattuali, finanziamenti e relativi interessi etc.)

- Raccolta e aggregazione dei dati contabili necessari per la predisposizione delle bozze di bilancio civilistico;

- Collaborazione e supporto all'Organo Amministrativo nello svolgimento delle attività di ripartizione degli utili di esercizio, delle riserve e restituzione dei conferimenti.

- GESTIONE DEGLI ADEMPIMENTI SOCIETARI

- Gestione dei rapporti con la Corte dei Conti, la società di revisione e i soci nelle attività di verifica della gestione aziendale;
- Tenuta delle scritture contabili e dei Libri Sociali;
- Predisposizione della documentazione che sarà oggetto di discussione e delibera in Assemblea e gestione dei rapporti con tale organo sociale.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'Organismo di Vigilanza in considerazione del verificarsi di fattori esterni (ad esempio legislativi, quali la introduzione di nuove categorie di reati) o di fattori interni (ad esempio modifiche organizzative o di business).

B. 3 Destinatari della Parte Speciale e principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello, come definiti nella Parte Generale del presente Modello che, a qualunque titolo, operino negli ambiti aziendali interessati dalle attività e dagli adempimenti di natura societaria e nelle aree di business.
In particolare, la presente Parte Speciale ha la funzione di:

- Fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- Fornire all'Organismo di Vigilanza e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

La Presente Parte Speciale prevede l'espresso divieto, a carico dei Destinatari, di:

- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che – considerati individualmente o collettivamente – integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-ter del D.Lgs 231/2001);
- Violare i principi e le procedure aziendali previste nella presente Parte Speciale.

La presente Parte Speciale comporta, conseguentemente, l'obbligo a carico dei Destinatari di rispettare, oltre ai principi generali enunciati nella Parte Generale, i seguenti principi di comportamento:

1. Tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;
2. Osservare rigorosamente tutte le norme poste dalla legge a tutela della integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
3. Assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonchè la libera e corretta formazione della volontà assembleare;
4. Effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza.

Nell'ambito dei suddetti comportamento è fatto divieto, in particolare, di:
con riferimento al precedente punto 1:

- Rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società;
- Omettere dati e informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società;

con riferimento al precedente punto 2:

- Restituire conferimenti ai soci o liberarli dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;

- Ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- Effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- Procedere a formazione o aumento fittizio del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale;

con riferimento al precedente punto 3:

- Porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo da parte del socio, del Collegio Sindacale o della società di revisione;
- Porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- Mantenere traccia di tutta la documentazione richiesta e consegnata agli organi di controllo, nonché di quella utilizzata nell'ambito di attività assembleari;

con riferimento al precedente punto 4:

- Omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti dell'Autorità di Vigilanza, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalla predetta autorità;
- Esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali e finanziarie della società;
- Porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle autorità pubbliche di vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

Al fine di prevenire la commissione del reato di corruzione tra privati, è fatto inoltre divieto di:

- Effettuare, ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia, a soggetti appartenenti ad enti privati;
- Distribuire omaggi al di fuori di quanto previsto dalla prassi aziendale. In particolare, è vietata qualsiasi forma di regalo a soggetti appartenenti ad enti privati, o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico o la brand image della società. I regali offerti – salvo quelli di modico valore – devono essere documentati in modo adeguato a consentire le prescritte verifiche;
- Accordare altri vantaggi di qualsiasi natura (promesse di assunzioni etc), in favore di soggetti appartenenti ad enti privati che possano determinare le stesse conseguenze previste al precedente punto;
- Effettuare prestazioni in favore dei consulenti, dei partner e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere.

Ad integrazione dei principi di comportamento, si prescrivono le seguenti regole di comportamento, funzionali alla riduzione al minimo del rischio di commissione di taluni reati, come di seguito indicato.
a) Per la prevenzione dei reati di false comunicazioni sociali (ex art. 2621 c.c.) e false comunicazioni sociali in danno dei soci e dei creditori (ex art. 2622 c.c.), la redazione del bilancio annuale, della relazione di gestione e della relazione semestrale si richiede:

- La sottoscrizione da parte dei responsabili che hanno concorso alla formazione della bozza di bilancio e delle altre comunicazioni sociali di una dichiarazione attestante la veridicità, la completezza e la coerenza dei dati e delle informazioni ivi contenute;
- L'esame del progetto di bilancio, antecedentemente all'approvazione assembleare, da parte dell'Organismo di Vigilanza;
- La verifica, con cadenza periodica, dei saldi dei conti di contabilità generale al fine di garantire la quadratura della contabilità generale con i rispettivi partitari e con i conti sezionali;
- L'identificazione delle risorse interessate, dei dati e delle informazioni che le stesse devono fornire, nonché delle tempistiche, per la predisposizione del bilancio o di altra comunicazione sociale;
- La verifica della completezza e correttezza dei dati e delle informazioni comunicate dalle suddette risorse e sigla sulla documentazione analizzata;
- Lo svolgimento e formalizzazione dell'analisi degli scostamenti rispetto ai dati del periodo precedente e formalizzazione delle motivazioni che hanno portato i maggiori scostamenti.

b) Per la prevenzione dei reati di indebita restituzione di conferimenti (ex art. 2626 c.c.), illegale ripartizione degli utili e delle riserve (ex art. 2627 c.c.), illecite operazioni sulle azioni sociali (ex art. 2628 c.c.), operazioni in pregiudizio dei creditori (ex art. 2629 c.c.), formazione fittizia del capitale (ex art. 2632 c.c.), considerato che l'obiettivo è evitare tutte le condotte idonee, anche solo potenzialmente, a ledere l'integrità del capitale sociale, è necessario:

- Assegnare specificatamente le responsabilità decisionali ed operative per l'effettuazione di attività che vengono ad incidere sul capitale sociale e stabilire meccanismi di coordinamento tra le varie funzioni coinvolte;
- Informare delle attività di cui al punto precedente l'Organismo di Vigilanza.

c) Per la prevenzione dei reati di omessa convocazione dell'assemblea (ex art. 2631 c.c.) e illecita influenza sull'assemblea (ex art. 2636 c.c.), considerato che si tratta di condotte illecite dirette ad influenzare la libera e corretta formazione della volontà assembleare e del mercato, è necessario disciplinare le procedure attraverso le quali l'organo amministrativo rilascia informazioni ai soci in ordine alle materie all'ordine del giorno, anche attraverso l'adozione di uno specifico regolamento assembleare;

d) Per la prevenzione dei reati inerenti i rapporti con il Collegio Sindacale e i revisori, i soggetti che, in ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione di tali rapporti sono tenuti ad eseguire le seguenti attività e controlli:

- Espletare le attività conseguenti alle richieste del Collegio Sindacale e dei revisori, fornendo le informazioni e l'eventuale documentazione tempestivamente, verificandone previamente l'integrità e la completezza;

- Assicurare la tracciabilità della consegna della documentazione richiesta, archiviando documenti di presa in consegna della documentazione sottoscritti dai componenti del Collegio Sindacale e dai responsabili delle attività di revisione esterna.

B.4 Responsabile interno

Per ogni area a rischio, come individuate al punto B.2, il Presidente del Consiglio di Amministrazione della Società, o un dirigente da questi incaricato, nomina un "Responsabile Interno".

Il Responsabile interno:

- Diviene il soggetto referente e responsabile delle attività a rischio;
- Garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- Collabora con l'Organismo di Vigilanza nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- Comunica tempestivamente all'Organismo di Vigilanza eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Ogni Responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'Organismo di Vigilanza.

PARTE SPECIALE "C2 – REATI DI CRIMINALITÀ INFORMATICA

C.1 Le tipologie di reati di criminalità informatica (art. 24-bis del decreto)

Per quanto concerne la presente Parte Speciale "C", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 24-bis del decreto, e suddivisi tra reati potenzialmente realizzabili e reati che, per quanto non si possano escludere tout court, sono stati ritenuti remoti in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente coperti dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico adottato dalla Società. L'identificazione delle aree di attività a rischio di commissione dei reati previsti e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state realizzate anche attraverso le interviste ai soggetti aziendali di ciascuna Area aziendale competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:
Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.)

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamene destinati ad elaborarli.

I reati la cui commissione è stata ritenuta remota sono i seguenti:

Accesso abusivo ad un sistema informatico o telematico (art. 615 –ter c.p.)

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

La pena è della reclusione da uno a cinque anni se:

1. Il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2. Il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3. Dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo, , riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre agli otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635- quinques c.p.)

Se il fatto di cui all'art. 635 quater c-p. (rubricato "Danneggiamento di sistemi informatici o telematici") è diretto a distruggere, danneggiare, rendere in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da 1 a 4 anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto, inservibile, la pena è della reclusione da 3 a 8 anni.

Se ricorre la circostanza di cui al n. 1) del secondo comma dell'art. 365 c.p. ovvero il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Frode informatica del certificatore di firma elettronica (art. 640- quinques c.p.)

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a 3 anni e con la multa da 51 a 1.032 €.

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

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso

ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5.164,00 €.

La pena è della reclusione da uno a due anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617 – quater.

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

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

Se ricorre la circostanza di cui al n. 1) del secondo comma dell'art. 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede di ufficio.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 – quinques c.p.)

Chiunque allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione sino a 2 anni e con la multa sino a 10.329,00 euro.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 – quater c.p.)

Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi e quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

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

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1. In danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2. Da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3. Da chi esercita anche abusivamente la professione di investigatore privato.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 –quinques c.p.)

Chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da 1 a 4 anni. La pena è della reclusione da 1 a 5 anni nei casi previsti dal quarto comma dell'art. 617-quater.

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

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da 1 a 4 anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, 'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da 3 a 8 anni.

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

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da 1 a 5 anni.

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

Indebito utilizzo, falsificazione, alterazione e ricettazione di carte di credito o di pagamento (art. 55 comma 5 D.lgs 231/2007)

Chiunque, ai fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da 1 a 5 anni e con la multa da 310 a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per latri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

C.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte Speciale "C" del Modello, le aree di attività ritenute più specificatamente a rischio e le correlate "attività sensibili" sono:

- GESTIONE DEI RAPPORTI E DEGLI ADEMPIMENTI VERSO ENTI PUBBLICI E AUTORITÀ AMMINISTRATIVE INDIPENDENTI, ANCHE IN OCCASIONE DI VERIFICHE E ISPEZIONI

- Gestione dei rapporti, anche per via telematica e anche in fase di verifiche ispettive, con Enti Pubblici e Autorità Amministrative Indipendenti, quali a titolo esemplificativo:
  a) gestione dei rapporti con i Funzionari della Guardia di Finanza, dell'Agenzia delle Entrate e degli altri Enti competenti in materia fiscale e tributaria, anche in occasione di verifiche, ispezioni ed accertamenti e gestione delle relative comunicazioni;
  b) gestione delle comunicazioni e degli adempimenti nei confronti dell'Autorità Garante della Privacy, anche in occasione di verifiche ispettive;
  c) gestione delle comunicazioni e degli adempimenti richiesti dall'Autorità di Vigilanza sui Contratti Pubblici, anche in occasione di verifiche ispettive.

- GESTIONE DEL SISTEMA INFORMATICO AZIENDALE

- Utilizzo e gestione di software nell'ambito dei sistemi informativi aziendali;
- Gestione delle attività connesse all'implementazione, manutenzione e aggiornamento del sito internet e della rete telematica aziendale.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'Organismo di Vigilanza in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati(o di fattori interni (ad esempio modifiche organizzative o business).

C.3 Destinatari della Parte Speciale e principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale ed ha la funzione di:

- Fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- Fornire all'Organismo di Vigilanza e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifiche previste.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale, la presente Parte Speciale (i) prevede che l'utilizzo delle risorse informatiche e di rete avvenga in modo corretto, in conformità a quanto previsto dalle procedure aziendali interne e nel rispetto delle misure di sicurezza adottate dalla Società e (ii) prevede l'espresso divieto, a carico di tutti i Destinatari, di:

- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che – considerati individualmente o collettivamente – integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;

- Porre in essere condotte, anche con l'ausilio di terzi, miranti ad accedere in maniera non autorizzata ai sistemi informativi utilizzati dalla Pubblica Amministrazione o a sistemi informativi altrui con l'obiettivo di:
  a) acquisire abusivamente informazioni contenute nei suddetti sistemi informativi;
  b) danneggiare, distruggere o alterare dati o programmi contenuti nei suddetti sistemi informativi;
  c) alterare, in qualsiasi modo, il funzionamento del sistema informativo;
  d) utilizzare abusivamente codici di accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi;
- Formare falsamente documenti societari aventi rilevanza esterna, mediante accesso ai sistemi e alterazione dei dati;
- Distruggere, alterare, danneggiare informazioni, dati, programmi informatici della Società o della Pubblica Amministrazione, per ottenere vantaggi o condizioni favorevoli per l'azienda;
- Porre in essere condotte miranti alla distruzione o all'alterazione dei documenti informatici aventi finalità probatoria in assenza di una specifica autorizzazione;
- Utilizzare o installare programmi diversi da quelli autorizzati;
- Aggirare o tentare di aggirare i meccanismi di sicurezza aziendali;
- Lasciare il proprio Personal Computer incustodito;
- Rilevare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche agli altri siti/sistemi;
- Detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- Entrare nella rete aziendale e nei programmi con un codice di identificazione utente diverso da quello assegnato.

I Responsabili delle Aree operative devono attivarsi, in base al proprio ruolo e responsabilità, al fine di porre in essere le azioni necessarie a:

- Verificare la sicurezza dei sistemi informativi utilizzati segnalando all'Area competente eventuali disservizi;
- Identificare e segnalare all'Area competente le potenziali vulnerabilità nel sistema dei controlli IT;
- Assicurare la corretta implementazione tecnica del sistema di "deleghe e poteri" aziendali a livello di sistemi informatici ed abilitazioni utente riconducibili ad una corretta segregazione dei compiti;
- Monitorare, per la parte di rispettiva competenza, il corretto utilizzo degli accessi (user-id e password) ai sistemi informatici da parte di terzi;
- Vigilare sulla corretta applicazione di tutti gli accorgimenti ritenuti necessari al fine di fronteggiare, nello specifico, i delitti informatici e di trattamento illecito dei dati, suggerendo ogni più opportuno adeguamento.

Sono infine previste le seguenti regole nell'utilizzo e nella gestione dei sistemi informativi aziendali:

- Deve essere assicurata una corretta gestione degli utenti di amministrazione, con la finalità di impedire l'utilizzo di tali credenziali a personale non autorizzato;

- Devono essere assicurati il corretto mantenimento e l'integrità dei file di log generati dai sistemi;
- Deve essere assicurata un'adeguata manutenzione/aggiornamento periodico delle credenziali utente al fine di prevenire eventuali erronee abilitazioni ai sistemi applicativi. A tal fine devono essere osservate, con riferimento ai diversi applicativi aziendali, le regole atte ad assicurare l'aggiornamento delle password dei singoli utenti;
- La navigazione in Internet e l'utilizzo della posta elettronica attraverso i sistemi informatici aziendali deve avvenire esclusivamente per lo svolgimento della propria attività lavorativa;
- Deve essere garantita la sicurezza fisica dell'infrastruttura tecnologica della Società, anche mediante monitoraggio delle attività di gestione e manutenzione sulla stessa;
- Nell'ambito delle attività svolte, i fornitori terzi devono rispettare i principi di comportamento e le regole indicate nella Presente Parte Speciale al fine di tutelare la sicurezza dei dati ed il corretto utilizzo dei sistemi informativi aziendali.

C.4 Responsabile Interno

Per ogni Area a rischio, il Presidente del Consiglio di Amministrazione o un Dirigente da questi incaricato, nomina un "Responsabile Interno".

Il Responsabile Interno:

- Diviene il soggetto referente e responsabile delle attività a rischio;
- Garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- Collabora con l'Organismo di Vigilanza nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- Comunica all'Organismo di Vigilanza eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Ogni responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'Organismo di Vigilanza.

C.5 I processi strumentali

Di seguito sono riportati i processi c.d. strumentali nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato contemplate nella presente Parte Speciale:

- Gestione della sicurezza, manutenzione e sviluppo dei sistemi informativi.

PARTE SPECIALE "D" – "INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA"

D.1 Le tipologie di reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" (art. 25-decies del decreto)

Per quanto concerne la presente Parte Speciale "D", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25-decies del decreto. L'identificazione delle aree di attività a rischio di commissione dei reati previsti e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state realizzate anche attraverso le interviste ai soggetti aziendali di ciascuna Area aziendale competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

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

L'art. 377 – bis c.p. punisce il fatto di chi induce (mediante violenza o minaccia o con l'offerta o la promessa di denaro o altra utilità) a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere dichiarazioni utilizzabili in un procedimento penale, quando tale soggetto ha la facoltà di non rispondere.

La condotta di induzione a non rendere dichiarazioni (cioè di avvalersi dalla facoltà di non rispondere ovvero di rispondere dichiarazioni false) deve essere realizzata in modo tipico (o mediante violenza o minaccia o con l'offerta o la promessa di denaro o altra utilità).

Il soggetto passivo è necessariamente un soggetto al quale la legge attribuisca la facoltà di non rispondere: l'indagato (o l'imputato) di reato connesso o collegato (sempre che gli stessi non abbiano già assunto l'ufficio di testimone), nonché a quella ristretta categoria di testimoni (i prossimi congiunti), cui l'art. 199 c.p. conferisce la facoltà di astenersi dal testimoniare.

Non è facile immaginare una casistica che possa determinare la responsabilità dell'ente, ma è ipotizzabile il caso di un dipendente imputato o indagato che venga indotto a rendere false dichiarazioni (o ad astenersi dal renderle) per evitare un maggior coinvolgimento della responsabilità risarcitoria dell'ente stesso collegata al procedimento penale nel quale il dipendente è coinvolto.

D.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fine della presente Parte Speciale "D" del Modello, le aree di attività ritenute più specificatamente a rischio e le correlate "attività sensibili" sono:

- GESTIONE DEI CONTENZIOSI GIUDIZIALI E DELLE PROBLEMATICHE CONNESSE
  - Gestione dei rapporti con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'Organismo di Vigilanza in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati(o di fattori interni (ad esempio modifiche organizzative o business).

D.3 Destinatari della Parte Speciale: principi di comportamento

La presente Parte Speciale si riferisce a tutti i Destinatari del Modello così come definiti nella Parte Generale.

In particolare la presente Parte Speciale ha la funzione di:

- Fornire un elenco di principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- Fornire all'Organismo di Vigilanza e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare tutte le attività di controllo, monitoraggio e verifica previste.

Fermo restando il rispetto dei principi generali enunciati nella Parte Generale, la presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari di:

- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che – considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- Prendere contatti con dipendenti o terzi coinvolti in procedimenti penali, allo scopo di indurli a rendere dichiarazioni atte ad evitare l'eventuale rischio di un coinvolgimento della società;
- Porre in essere atti di minaccia o altre forme analoghe di coartazione ovvero di dare o promettere elargizioni in denaro o altre forme di utilità affinché il soggetto (dipendente o terzo) coinvolto in un procedimento penale non presti una fattiva collaborazione al fine di rendere dichiarazioni veritiere, trasparenti e correttamente rappresentative dei fatti o non esprima liberamente le proprie rappresentazioni dei fatti, esercitando la propria facoltà di non rispondere attribuita dalla legge, in virtù delle suddette forme di condizionamento.

In particolare, nel corso di procedimento giudiziari, è fatto divieto di:

- Elargire somme di denaro ai soggetti coinvolti quali testimoni nel procedimento penale;
- Offrire omaggi e regali alle figure coinvolte come testimoni in un procedimento penale o ai loro familiari, o a conferire loto qualsiasi forma di utilità che possa influenzare la testimonianza o impedirla, ostacolarla o indurre a false dichiarazioni in fase di dibattimento per assicurare un qualsivoglia vantaggio per l'azienda;
- Accordare altri vantaggi di qualsiasi natura (promesse di assunzione, promozione etc.) alle persone coinvolte quali testimoni in un procedimento penale o loro familiari;
- Effettuare alle persone coinvolte quali testimoni in un procedimento penale qualsiasi tipo di pagamento in contanti o in natura.

Inoltre, la Società dovrebbe selezionare i soggetti autorizzati ad interloquire con i dipendenti coinvolti in procedimenti penali e gli eventuali colloqui intercorsi dovrebbero essere verbalizzati.

D.4. Responsabile Interno

Per ogni Area a rischio, il Presidente del Consiglio di Amministrazione o un Dirigente da questi incaricato, nomina un "Responsabile Interno".

Il Responsabile Interno:

- Diviene il soggetto referente e responsabile delle attività a rischio;

- Garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;

- Collabora con l'Organismo di Vigilanza nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;

- Comunica all'Organismo di Vigilanza eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello.

Ogni responsabile Interno può delegare le attività operative a referenti da lui indicati, dandone comunicazione all'Organismo di Vigilanza.

D.5 I processi strumentali

Di seguito sono riportati i processi c.d. strumentali nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato contemplate nella presente Parte Speciale:

- Acquisti di beni, servizi e consulenze;
- Rapporti con la Pubblica Amministrazione e con le Autorità Ammnistrative Indipendenti;
- Gestione dei flussi monetari e finanziari;
- Selezione, assunzione e gestione del personale;
- Gestione dei rimborsi spese e delle spese di rappresentanza;
- Gestione sponsorizzazioni, donazioni e omaggi.

PARTE SPECIALE "E" – REATI COMMESSI IN VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

E.1 Finalità

La presente Parte Speciale E ha lo scopo di definire le regole di gestione ed i principi di comportamento che tutti i Destinatari dovranno seguire al fine di prevenire, nell'ambito delle specifiche attività svolte da ICTS Italia S.R.L. A SOCIO UNICO (da qui in avanti "ICTS" o "Società") e considerate "a rischio", la commissione dei reati in materia di Salute e Sicurezza sui luoghi di lavoro richiamati dall'art. 25 septies del D.Lgs. n. 231/2001.

I Destinatari del presente documento sono l'*Amministratore Delegato*, in qualità di *Datore di Lavoro* di ICTS ai sensi del D.Lgs. n. 81/2008 e s.m.i., i *Delegati* in materia di salute e sicurezza sui luoghi di lavoro, la Funzione *HSE*, i *Dirigenti*, i *Preposti* e i *Lavoratori ex* D.Lgs. n. 81/2008 e s.m.i. di ICTS e tutti coloro che sono coinvolti - a qualsiasi titolo - o che vigilano sugli adempimenti in materia di sicurezza sui luoghi di lavoro, nonché coloro i quali, pur non essendo funzionalmente legati a ICTS, agiscano sotto la direzione o vigilanza dei Vertici aziendali.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- indicare i principi di comportamento e i presidi di controllo che i Destinatari devono osservare ai fini della corretta applicazione del Modello;
- fornire all'*Organismo di Vigilanza* (*OdV*) e alle altre Funzioni di controllo gli strumenti per esercitare le attività di monitoraggio, controllo e verifica.

In linea generale, tutti i Destinatari dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi alle determinazioni contenute nei seguenti documenti aziendali:

- Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001;
- Codice Etico e Disciplinare aziendale;
- normativa interna (*policy* e procedure organizzative, procedure e istruzioni del Sistema di Gestione della Salute e Sicurezza sui luoghi di lavoro predisposto in conformità della Norma ISO 45001:2018);
- sistema di procure / deleghe in vigore;
- ogni altro documento aziendale che regoli attività rientranti nell'ambito di applicazione del Decreto.

È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge con riferimento in particolare al D.Lgs. n. 81/2008 e s.m.i.

E.2 Le fattispecie rilevanti (art. 25 *septies* del D.Lgs. n. 231/2001)

I reati presupposto

Con l'approvazione della Legge 3 agosto 2007, n. 123, che ha inserito nel D.Lgs. n. 231/2001 l'art. 25 *septies*, è diventata operativa l'estensione della responsabilità dell'ente ai reati di omicidio colposo e

lesioni colpose gravi e gravissime commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro.

In data 1° aprile 2008 è stato approvato dal Consiglio dei Ministri il D.Lgs. n. 81/2008, attuativo della delega di cui all'articolo 1 della Legge 3 agosto 2007 n. 123 in materia di tutela della salute e sicurezza nei luoghi di lavoro.

Di seguito si riporta una breve descrizione delle fattispecie di reato "presupposto" della responsabilità amministrativa della Società.

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

La fattispecie in esame si realizza quando si cagiona per colpa la morte di una persona. Il delitto è rilevante ai sensi del D.Lgs. 231/2001 laddove l'evento sia stato causato dalla violazione delle norme per la prevenzione degli infortuni sul lavoro.

- **Lesioni colpose gravi o gravissime (art. 590, comma 3, c.p.)**

La fattispecie in esame si realizza quando si cagiona ad altri per colpa una lesione personale grave o gravissima e l'evento lesivo è causato da violazione delle norme per la prevenzione degli infortuni sul lavoro.

Il delitto, limitatamente ai fatti costituenti conseguenza di violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale, è perseguibile d'ufficio.

Ai sensi dell'art. 583 c.p., la lesione personale è:

- *grave*:
  - se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;
  - se il fatto produce l'indebolimento permanente di un senso o di un organo;
- *gravissima* se dal fatto deriva:
  - una malattia certamente o probabilmente insanabile;
  - la perdita di un senso;
  - la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella.

Esclusione della responsabilità amministrativa della società

Il D.Lgs. n. 81/2008 e s.m.i., all'art. 30, ha indicato le caratteristiche e i requisiti che deve possedere un modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa di cui al D.Lgs. 8 giugno 2001, n. 231.

In particolare, secondo il citato articolo, il modello, per avere efficacia esimente, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi ai seguenti ambiti:

- rispetto degli *standard* tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- attività di sorveglianza sanitaria;
- attività di informazione e formazione dei lavoratori;
- attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- acquisizione di documentazioni e certificazioni obbligatorie di legge;
- verifiche periodiche dell'applicazione e dell'efficacia delle procedure adottate.

Inoltre, il modello organizzativo e gestionale deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle suddette attività.

Sempre ai sensi dell'art. 30 del D.Lgs. 81/2008, il modello organizzativo:

- deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
- deve prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

Infine, il comma 5 del medesimo art. 30 dispone che: "*In sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sui luoghi di lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui ai commi precedenti per le parti corrispondenti*".

E.3 Struttura organizzativa e sistema delle deleghe in materia di Sicurezza sui luoghi di lavoro

ICTS ha articolato la propria organizzazione aziendale per la sicurezza e la salute sui luoghi di lavoro con le figure di seguito indicate:

- *Datore di Lavoro*: con delibera del Consiglio di Amministrazione è stato individuato quale *Datore di Lavoro* ai sensi del D.Lgs. n. 81/2008 e s.m.i. di ICTS l'*Amministratore Delegato* della Società, a cui

sono stati conferiti illimitati poteri organizzativi e di spesa per la gestione degli aspetti di salute e sicurezza sui luoghi di lavoro nell'ambito di tutte le attività e sedi aziendali;

- *Delegati per la Sicurezza* (anche "*Delegati*"): il Datore di Lavoro ha delegato, ai sensi dell'art. 16 del D.Lgs. n. 81/2008 e s.m.i. con atto reso noto all'interno dell'organizzazione, gli obblighi di cui all'art. 18 del D.Lgs. n. 81/2008 e s.m.i. ai *Direttori di Reparto*[1] e al *General Security Manager*[2], ai quali sono stati conferiti adeguati poteri organizzativi e di spesa per l'espletamento delle funzioni trasferite;
- *OHS Compliance Manager*: responsabile della Funzione aziendale a supporto dell'organizzazione ICTS nel perseguimento degli obiettivi di conformità normativa in materia di salute e sicurezza sui luoghi di lavoro, preposta, tra l'altro, alla definizione e alla verifica della corretta attuazione del Sistema di Gestione aziendale della Salute a Sicurezza sui luoghi di lavoro in conformità agli *standard* di controllo definiti nel presente documento ed ai requisiti della Norma ISO 45001;
- *Responsabili di contratto/Responsabili di turno/Supervisori* (anche *"Referenti operativi"*): nell'ambito di ciascun *Reparto*, sono incaricati, dai *Direttori di Reparto,* anche di volta in volta, i soggetti responsabili della gestione operativa del contratto di servizio stipulato con il Cliente, i soggetti responsabili di ciascun turno di lavoro e i soggetti che svolgono attività di supervisione per specifici ambiti di attività. Tali soggetti, individuati come *Preposti* ai sensi del D.Lgs. n. 81/2008 e s.m.i., svolgono i compiti previsti dalla normativa vigente in coordinamento con i *Direttori di Reparto* e nel rispetto delle disposizioni aziendali;
- *Responsabile del Servizio Prevenzione e Protezione (RSPP)*: il *Datore di Lavoro* nomina, ai sensi del D.Lgs. n. 81/2008 e s.m.i., anche consultando il *Rappresentante dei Lavoratori (RLS)*, il *Responsabile del Servizio di Prevenzione e Protezione*, previa verifica circa il possesso dei requisiti necessari;
- *Medico Competente (MC):* i *Delegati per la Sicurezza* nominano, previa verifica circa il possesso dei requisiti necessari e consultazione del RLS, il Medico Competente per lo svolgimento dei compiti previsti dalla normativa applicabile;
- *Incaricati alle emergenze*: l'individuazione degli incaricati alle emergenze (squadre antincendio e primo soccorso) avviene mediante lettera di incarico previa verifica di assenza di eventuali fattori ostativi, del possesso di specifici requisiti (anche in termini di copertura di turni di lavoro e localizzazione) e dell'avvenuta formazione in accordo alle disposizioni legislative in materia, nonché previa consultazione del RLS;
- *Rappresentanti dei lavoratori per la sicurezza (RLS)*: eletti/nominati ai sensi della normativa vigente.

ICTS adotta ed attua, inoltre, un Sistema di Gestione della Salute e Sicurezza sui luoghi di lavoro (SGSL) conforme ai requisiti di cui all'art. 30 del D.Lgs. n. 81/2008 e s.m.i. ed a quelli della Norma ISO 45001, anche oggetto di certificazione da parte di Ente terzo qualificato e indipendente.

Per completezza, anche prima della certificazione ai sensi della Norma ISO 45001:2018, sin dal 2018, ICTS ha ottenuto la certificazione del proprio SGSL secondo la Norma OHSAS 18001:2007, richiamata all'art. 30 del D.Lgs. 81/2008 e s.m.i..

[1] Ciascuno, in particolare, con riferimento alla sicurezza del personale operante in sedi o siti specifici afferenti al perimetro di responsabilità assegnato.

[2] Con riferimento al personale operante presso Clienti e non operante stabilmente presso specifici sedi/siti operativi.

Gli atti interni, nonché i documenti organizzativi aziendali, descrivono nel dettaglio i ruoli e le responsabilità attribuiti da ICTS in materia di Salute e Sicurezza sui luoghi di lavoro, anche in relazione al SGSL adottato dalla Società.

E.4 Identificazione dei processi e delle aree sensibili

In esito alle analisi svolte ai sensi dell'art. 6, comma 1, lett. *a),* del D.Lgs. n. 231/2001 con riferimento al rischio di commissione dei reati di cui all'art. 25 *septies*, ICTS, in un'ottica di integrazione tra le prescrizioni del Modello Organizzativo - in particolare, della presente Parte Speciale - e quelle del Sistema di Gestione Sicurezza sui luoghi di lavoro adottato in conformità alla Norma ISO 45001 e alle prescrizioni, per le parti corrispondenti, dell'art. 30 del D.Lgs. n. 81/2008 e s.m.i., ritiene opportuno definire, per i processi e le fasi in cui si struttura il SGSL, specifici presidi in funzione preventiva.

Più esattamente, assumono rilevanza le seguenti fasi:

- **Pianificazione**: si tratta delle attività di pianificazione e organizzazione dei ruoli e delle attività connesse alla tutela della salute, sicurezza e igiene sul lavoro volte a fissare obiettivi coerenti con la politica aziendale, stabilire i processi necessari al raggiungimento degli obiettivi, definire e assegnare le risorse necessarie.
- **Attuazione e funzionamento**: si tratta delle attività volte a definire strutture organizzative e responsabilità e modalità per la formazione, consultazione e comunicazione, gestione del sistema documentale, controllo dei documenti e dei dati, controllo operativo e gestione delle emergenze.
- **Verifica e azioni correttive**: si tratta delle attività volte a implementare modalità di misura e monitoraggio delle prestazioni del Sistema di gestione, la registrazione, l'analisi e il monitoraggio degli infortuni e degli incidenti, la gestione delle non conformità e delle azioni correttive, modalità di esecuzione di *Audit* periodici e delle attività di sorveglianza.
- **Riesame della Direzione**: si tratta delle attività di riesame periodico del Vertice Aziendale al fine di valutare se il sistema di gestione della salute e sicurezza è stato completamente realizzato e se è sufficiente alla realizzazione della politica e degli obiettivi definiti dalla Società.

E.5 Principi di comportamento e attuazione dei processi decisionali

E.5.1 Principi di comportamento

Fatto salvo quanto previsto dal Codice Etico aziendale, da considerare a ogni effetto parte integrante del Modello, a tutti i Destinatari è fatto obbligo di:

- osservare tutti i dettami previsti da leggi e regolamenti in materia di salute e sicurezza sui luoghi di lavoro (in particolare, D.Lgs. n. 81/2008 e s.m.i.);
- osservare i protocolli e le procedure che disciplinano l'attività aziendale, con riferimento al Modello di *Governance* in materia di sicurezza, agli elementi di controllo declinati nel presente documento ed alle procedure del SGSL definito.

Tutti i soggetti aventi compiti e responsabilità nella gestione degli adempimenti in materia di sicurezza sui luoghi di lavoro, quali, in particolare, ma non limitatamente:

- il *Datore di lavoro*, i *Delegati*, *OHS Compliance Manager* e i *Referenti del SGSL*;
- i *Dirigenti*, i *Preposti* e i *Lavoratori* - come identificati dalla legislazione vigente - che prestano la propria attività lavorativa presso le sedi/unità operative/cantieri della Società o presso le sedi/unità operative di clienti, nonché i loro *Rappresentanti per la Sicurezza*;
- il *Responsabile* e gli *Addetti al Servizio di Prevenzione e Protezione*, il *Medico Competente*, gli *Addetti alle emergenze*;
- i *Responsabili di contratto/Responsabili di turno/Supervisori* e i responsabili funzione competenti;
- i lavoratori (dipendenti e collaboratori) di società terze le cui attività presentano rischi per la sicurezza e salute interferenti presso le sedi/unità operative/cantieri della Società o presso le sedi/unità operative di clienti;

ciascuno nell'ambito delle proprie responsabilità e competenze, devono:

- rispettare le leggi vigenti ad essi applicabili, con riferimento, in particolare, al D.Lgs. n. 81/2008 e s.m.i., nonché i principi esposti nel Modello Organizzativo e nella presente Parte Speciale, nel Codice Etico aziendale e negli *Standard* di Gruppo, le *policy* e le procedure del SGSL di ICTS;
- operare in coerenza con il sistema di deleghe e procure in essere;
- osservare scrupolosamente le disposizioni e le istruzioni impartite dai soggetti preposti al fine di preservare la salute e la sicurezza propria e di tutti i lavoratori;
- collaborare, mediante i propri rappresentanti, alla valutazione dei rischi per la sicurezza e salute del lavoro, compresi quelli interferenziali;
- segnalare tempestivamente alle strutture individuate e con le modalità definite nelle procedure aziendali in vigore, eventuali situazioni di pericolo e rischio, infortuni, malattie professionali o situazioni di *near miss* (o quasi incidenti), nonché violazioni riscontrate alle regole di comportamento e alle procedure vigenti;
- utilizzare, secondo le istruzioni, le attrezzature presenti sul luogo di lavoro, nonché i dispositivi di sicurezza e protezione, ove previsti;
- non rimuovere o modificare in nessun modo i dispositivi di sicurezza di macchine e attrezzature o altri dispositivi di segnalazione o di controllo;
- non compiere di propria iniziativa operazioni o manovre che possano compromettere la sicurezza propria o di altri lavoratori o che possano esporre se stessi, i propri colleghi o terzi a situazioni di pericolo;
- segnalare ogni anomalia, situazione o rischio per la sicurezza e salute differenti da quelli noti o particolarmente significativi;
- partecipare alle sessioni formative e di addestramento organizzate dalla Società sui rischi per la sicurezza e salute del lavoro.

Il *Datore di Lavoro* ICTS, ovvero i *Delegati* della Società, in collaborazione con *OHS Compliance Manager*, ciascuno per gli aspetti di competenza, tenendo anche in considerazione le valutazioni tecniche del *RSPP*, devono inoltre:

- mantenere aggiornato e rispettare il corpo regolamentare e il sistema di procure e deleghe in materia di sicurezza;
- perseguire l'obiettivo di "*nessun danno alle persone*";

- promuovere una cultura nella quale tutti i lavoratori - compreso il personale delle ditte terze in subappalto operante presso le unità operative della Società con rischi di interferenza per la sicurezza e salute del lavoro - partecipino a questo impegno;
- garantire l'idoneità delle risorse umane - in termini di numero, qualifiche professionali e formazione - e dei materiali, necessaria al raggiungimento degli obiettivi prefissati dalla Società per il mantenimento e/o miglioramento dei livelli di sicurezza e salute dei lavoratori;
- garantire l'acquisizione e la gestione dei mezzi, delle attrezzature, degli impianti e, in generale, delle strutture aziendali nel rispetto degli *standard* tecnico-strutturali di legge, anche attraverso un processo continuo di manutenzione (ordinaria e straordinaria) degli stessi;
- definire gli obiettivi per la sicurezza e la salute dei lavoratori, valutando, anche sulla base dei contributi dei tecnici, i rischi connessi con tutte le attività svolte dai lavoratori ICTS, attraverso un efficace e preventivo scambio di informazioni e cooperazione con il datore di lavoro del sito ospitante o con quello delle società esterne che dovessero operare presso i siti/cantieri della Società e prevedendo che, ove necessario, determinate tipologie di lavorazioni possano essere svolte solo in presenza di specifici permessi (es. permesso di lavoro pericoloso);
- garantire un adeguato livello di formazione e informazione ai lavoratori, nonché richiedere che un adeguato livello di formazione e informazione sia garantito dai Datori di Lavoro ai lavoratori delle ditte terze in subappalto per quanto di loro competenza e relativamente ai rischi da interferenza, sul sistema di gestione della sicurezza definito dalla Società e sulle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole di comportamento e controllo definite dalla Società stessa;
- segnalare tempestivamente alle strutture individuate a norma di legge e/o internamente eventuali segnali / eventi di rischio / pericolo indipendentemente dalla loro gravità.

Sono in ogni caso fatte salve le procedure gestionali e operative poste in essere da ICTS per lo svolgimento delle attività sensibili ai reati di sicurezza sui luoghi di lavoro *ex* D.Lgs. n. 231/2001 e facenti parte del SGSL a Norma ISO 45001 anche conforme, per le parti corrispondenti, ai requisiti di cui all'art. 30 del D.Lgs. n. 81/2008 e s.m.i.; tali procedure integrano i suddetti *Principi di comportamento* e i *Protocolli di gestione* individuati da ICTS e di seguito definiti, attraverso la declinazione delle responsabilità e delle modalità operative da attuarsi.

E.5.2 Protocolli di gestione e sistema dei controlli

Pianificazione

- ***Politica*** (Prot[3] *P1*)

Il *Datore di Lavoro*, tenendo in considerazione i valori fondanti della Società e del Gruppo e il contesto della propria organizzazione, stabilisce la *Politica* di ICTS, ovverossia gli indirizzi e gli obiettivi generali che la Società si prefigge di raggiungere e le responsabilità che essa stessa intende assumere in materia di Salute e Sicurezza sui luoghi di lavoro. La *Politica* è comunicata a tutto il personale e alle parti interessate (tra cui Clienti e Fornitori) e viene periodicamente riesaminata dal *Datore di Lavoro*, anche in

[3] Protocollo di gestione.

collaborazione con *OHS Compliance Manager*, almeno in occasione del riesame annuale della Direzione, per assicurare che sia appropriata all'evoluzione dei rischi presenti in Azienda e allineata ai nuovi regolamenti e leggi.

- ***Valutazione dei rischi e predisposizione delle relative misure di prevenzione e protezione*** (Prot *P2*)

Il *Datore di Lavoro*, in coordinamento con il *RSPP* e con il supporto dei *Delegati* e/o dei *Referenti operativi*, del *Medico Competente* e dei *RLS*, nonché del *OHS Compliance Manager*, tenendo conto di tutti i fattori interni ed esterni, individua e aggiorna proattivamente i pericoli ed effettua una valutazione dei rischi per la salute e la sicurezza, anche al fine di identificare e attuare le misure di prevenzione e protezione dei lavoratori, riducendo a misure accettabili i rischi connessi alle attività lavorative, in relazione alle conoscenze acquisite ed alla priorità definita.

Tale analisi è formalizzata in appositi documenti ("***Documenti di valutazione dei rischi***" o "***DVR***"), nel rispetto di quanto previsto dalla normativa vigente in materia di salute e sicurezza sui luoghi di lavoro, contenente, tra l'altro, l'identificazione e la valutazione dei rischi per ogni mansione aziendale nell'ambito di ciascun attività e sede/sito produttivo, le misure di prevenzione e protezione e i dispositivi di protezione individuale assegnati a ciascun lavoratore, nonché quanto previsto in materia di DVR dall'art. 28, comma 2, D.Lgs. n. 81/2008 e s.m.i., sottoscritto a cura del *Datore di Lavoro* e dalle altre figure specialistiche, anche ai fini della data certa, come previsto dalla normativa vigente.

Il *Datore di Lavoro*, in collaborazione con i suddetti referenti aziendali, avendo a riferimento il contesto interno ed esterno in cui opera ICTS, provvede pertanto a:

- valutare tutti i rischi associati alle attività aziendali e alle mansioni dei lavoratori ICTS nell'ambito delle diverse sedi o siti ove le stesse vengono svolte, e ad elaborare e formalizzare il *Documento di Valutazione dei Rischi*;
- aggiornare il *DVR*, specifico di sito e/o inerente alle attività e mansioni aziendali (anche a seguito di eventuali segnalazioni da parte dei *Delegati*), per sopravvenuti mutamenti organizzativi e procedurali, modifiche tecniche, modifiche rese necessarie da evoluzioni normative, nonché a seguito di infortuni significativi e/o risultati sanitari che ne evidenzino la necessità, in tempi brevi e comunque non oltre i termini previsti dalla normativa applicabile dagli avvenuti mutamenti e modifiche;
- comunicare al personale e alle Funzioni aziendali interessate un'informativa riepilogativa degli aggiornamenti significativi intercorsi ai *DVR*.

Nei casi in cui ICTS rivesta il ruolo di Committente ai sensi e per gli effetti del D.Lgs. 81/2008 e a.m.i., i *Delegati*[4], con riferimento alla gestione dei servizi, lavori e forniture erogati da terzi presso le sedi/siti operativi della Società (di proprietà o meno), assicurano, ai sensi dell'art. 26 del D.Lgs. n. 81/2008 e s.m.i., anche attraverso la collaborazione dei *Referenti Operativi* e delle Funzioni aziendali competenti:

[4] Ciascuno in relazione ai poteri conferiti dal sistema di deleghe in essere.

- la verifica dell'idoneità tecnico professionale delle imprese affidatarie, appaltatrici e dei lavoratori autonomi in relazione ai lavori, ai servizi e alle forniture da affidare in appalto o mediante contratto d'opera o di somministrazione;
- l'elaborazione (in coordinamento con il/i Datore/i di Lavoro delle/delle società terze e/o delle società prestatrici di opera in subappalto), di documentazione, da allegare al contratto, che indichi le misure di cooperazione e coordinamento definite e le misure da adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi da interferenze (*DUVRI*), al fine di promuovere la cooperazione ed il coordinamento tra i datori di lavoro, provvedendo anche alla stima dei relativi oneri non soggetti a ribasso delle misure preventive e protettive finalizzate alla sicurezza e salute dei lavoratori;
- la presenza, nei contratti di appalto/fornitura, di specifiche clausole di risoluzione e sanzionatorie da applicarsi in caso di violazione/omissione del rispetto dei requisiti normativi o imposti da ICTS in materia di sicurezza, applicabili ai fornitori, appaltatori e contrattisti, nonché dei costi delle misure adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi in materia di salute e sicurezza sul lavoro derivanti dalle interferenze delle lavorazioni;
- la diffusione al personale interessato delle informazioni relative alle misure da adottare per la prevenzione dei rischi di interferenza;
- attività di monitoraggio in ordine al rispetto delle misure di cooperazione e coordinamento stabilite nonché di quelle contenute nel *DUVRI*, ove previsto, e la segnalazione tempestiva di eventuali non conformità, violazioni o criticità riscontrate al fine di definire e attuare le necessarie azioni di trattamento e correttive;
- l'analisi di affidabilità del servizio prestato, come rispondenza alle prescrizioni normative in materia di Sicurezza ed a quanto stabilito nel *DUVRI*, al fine di qualificare i fornitori e indirizzare la scelta delle successive forniture.

I *Delegati*[4], con riferimento alla gestione dei servizi, lavori e forniture erogati dalla società presso sedi/siti di terzi in cui sono presenti lavoratori / lavorazioni di altri Datori di Lavoro, assicurano, anche ai sensi dell'art. 26 del D.Lgs. n. 81/2008 e s.m.i. per quanto applicabile, attraverso la collaborazione dei *Referenti Operativi* e delle Funzioni aziendali competenti:

- attività di cooperazione e coordinamento con il Datore di Lavoro committente e gli altri Datori di Lavoro ai fini della valutazione dei rischi interferenziali incidenti sull'attività lavorativa oggetto dell'appalto;
- attività di coordinamento degli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, informando gli altri Datori di Lavoro e ricevendo dagli stessi le necessarie informazioni, anche al fine di eliminare rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'attività complessiva;
- la diffusione al personale interessato delle informazioni relative alle misure da adottare per la prevenzione dei rischi di interferenza;
- attività di monitoraggio in ordine al rispetto delle misure di cooperazione e coordinamento stabilite nonché di quelle contenute nel *DUVRI*, ove previsto, e la segnalazione tempestiva di eventuali non conformità, violazioni o criticità riscontrate al fine di definire e attuare le necessarie azioni di trattamento e correttive.

Il *Datore di Lavoro,* ovvero i *Delegati*[4], con riferimento ad attività o progetti implicanti la realizzazione di lavori per mezzo di cantieri temporanei o mobili ai sensi del titolo IV del D.Lgs. n. 81/2008 e s.m.i., assicurano, anche attraverso la collaborazione delle Funzioni aziendali competenti:

- qualora la Società si configuri come Committente dei Lavori:

o la verifica dell'idoneità tecnico-professionale delle imprese / lavoratori autonomi operanti in cantiere;

o le attività di vigilanza sull'operato dei soggetti nominati ai sensi di legge, previa verifica circa il possesso degli opportuni requisiti professionali definiti dalla Norma, quali il *Responsabile Lavori*, il *Coordinatore della Sicurezza in fase di Progettazione* (CSP) e *in fase di Esecuzione* (CSE), con riferimento in particolare alla redazione, aggiornamento, riesame e comunicazione alle parti interessate (ditte appaltatrice ed esecutrici) del Piano di Sicurezza e Coordinamento (PSC) e del Fascicolo di prevenzione e protezione dai rischi, elaborati secondo le disposizioni normative vigenti, nonché alle attività di monitoraggio e verifica da parte di detti soggetti circa il rispetto delle disposizioni ivi contenute.

- ***Conformità Legislativa*** (Prot *P3*)

I *Delegati*, in collaborazione, per gli aspetti di competenza, con *OHS Compliance Manager*, il *RSPP*, il *MC*, *i Referenti operativi* e le altre Funzioni aziendali, assicurano, con riferimento alle attività e alle sedi/siti aziendali afferenti al perimetro delle responsabilità assegnate, ovvero alle sedi di lavoro anche presso i Clienti della Società in cui ICTS esercita le proprie attività:

- l'identificazione e l'aggiornamento dei requisiti di legge e delle altre prescrizioni applicabili alla Società in tema di salute e sicurezza sui luoghi di lavoro;
- l'individuazione di dove tali prescrizioni si applicano (area aziendale) e la definizione delle azioni da intraprendere per il raggiungimento della conformità a tali requisiti, nonché l'assegnazione delle relative responsabilità e dei tempi di attuazione;
- la comunicazione delle informazioni rilevanti al personale e alle parti direttamente interessate anche esterne;
- la valutazione di conformità delle attività svolte ai requisiti applicabili, periodico e su base evento (qualora ad esempio si presentino modifiche delle attività lavorative aventi potenziale impatto sulla salute e sicurezza, modifiche legislative o regolamentari o di accordi volontari, ovvero siano riscontrate non conformità, *etc*.).

- ***Obiettivi e programmi di miglioramento*** (Prot *P4*)

Il *Datore di Lavoro* e i *Delegati*[5], avvalendosi della collaborazione di *OHS Compliance Manager*, del *RSPP*, del *MC* e dei *Referenti operativi*, anche consultando i *RLS*, assicurano, tenendo in considerazione tutte le attività, le sedi e i siti operativi in cui ICTS esercita le proprie attività produttive:

- la definizione di opportuni obiettivi di miglioramento dei livelli di salute e sicurezza dei lavoratori e delle altre parti interessate e sotto l'ambito di responsabilità della Società;
- la predisposizione e il mantenimento di un programma in cui vengono chiaramente individuate, quindi comunicate ai soggetti interessati, le scadenze temporali, le responsabilità e la disponibilità delle risorse necessarie (finanziarie, umane, logistiche e accessorie) al raggiungimento degli obiettivi definiti;

[5] Ciascuno in relazione alle sedi/siti afferenti al perimetro delle responsabilità assegnate.

- il riesame periodico del programma e il relativo aggiornamento per assicurare il raggiungimento degli obiettivi definiti.

Attuazione e funzionamento

- ***Organizzazione e Responsabilità*** (Prot *A1*)

ICTS è dotata di un sistema di deleghe, elaborato tenendo in considerazione le indicazioni giurisprudenziali nel rispetto dei requisiti di cui all'art. 16 del D.Lgs. n. 81/2008 e s.m.i., che definisce le responsabilità, i compiti e i poteri in materia di sicurezza, prevenzione infortuni e igiene sul lavoro. È inoltre formalizzato e diffuso a tutto il personale un organigramma funzionale e nominativo della sicurezza in cui sono esplicitati i ruoli, le responsabilità e le autorità per stabilire, organizzare e attuare il sistema di gestione definito.

Il *Datore di Lavoro* e i *Delegati* provvedono al mantenimento ed eventuale aggiornamento delle deleghe, delle nomine e degli incarichi conferiti alle diverse figure specialiste previste dalla normativa vigente e di riferimento del SGSL (*RSPP*, *MC*, Incaricati alla gestione delle emergenze, *OHS Compliance Manager*, Referenti del Sistema di Gestione, Dirigenti e Preposti, *etc.*) [6], assicurando:

- il possesso dei requisiti specifici in capo a dette figure, tra cui adeguatezza, efficacia di ruolo e aggiornamento formativo, in linea con quanto stabilito dalla normativa vigente in materia;
- l'attuazione di opportune attività di vigilanza sull'operato dei Soggetti delegati/nominati/incaricati;
- la tempestiva comunicazione a tutta l'Organizzazione degli aggiornamenti intercorsi al sistema di deleghe e al funzionigramma della Sicurezza.

Il *Consiglio di Amministrazione* viene periodicamente aggiornato dal *Datore di Lavoro*, anche in occasione del riesame della Direzione, sullo stato di implementazione SGSL, con riferimento agli obiettivi raggiunti ed ai risultati ottenuti, nonché sulle criticità rilevate e le relative azioni definite.

- ***Informazione, formazione e addestramento*** (Prot *A2*)

I *Delegati*[7], avvalendosi del supporto, per quanto di competenza, di *OHS Compliance Manager*, del *RSPP*, del *MC*, dei *Referenti Operativi* e delle altre Funzioni interne competenti e del coinvolgimento del *RLS*, assicurano, con riferimento alle attività e alle sedi/siti aziendali afferenti al perimetro delle responsabilità assegnate, ovvero alle sedi di lavoro anche presso i Clienti della Società in cui ICTS esercita le proprie attività:

- la pianificazione periodica, almeno su base annuale, delle necessità informative, formative e di addestramento del personale ICTS, in relazione alle attività svolte[8] ed al ruolo assunto all'interno dell'Organizzazione in materia di Sicurezza (lavoratori, dirigenti, preposti, RLS, addetti alle emergenze, *etc*.);

[6] Consultando i *RLS* secondo le modalità stabilite dalla normativa vigente.

[7] Ciascuno con riferimento al personale rientrante nel perimetro delle responsabilità assegnate.

[8] Anche in relazione ai rischi specifici presenti nelle sedi/siti operativi presso i Clienti.

- l'erogazione e la relativa registrazione delle attività informative / formative e di addestramento sulla base di quanto pianificato ed in relazione alle condizioni dei lavoratori (all'assunzione, ovvero al primo inserimento in azienda, al trasferimento o cambiamento di mansione, all'introduzione di nuove attrezzature, tecnologie, sostanze e preparati pericolosi, a seguito di aggiornamenti normativi, organizzativi e procedurali), nel rispetto delle modalità e dei contenuti stabiliti dalla legislazione vigente in materia di sicurezza, anche con riferimento agli elementi di interesse del SGSL definito dalla Società ed alla necessaria organizzazione delle prove di emergenza/evacuazione, da attuarsi presso le sedi ed i siti produttivi aziendali con l'eventuale supporto delle Autorità competenti;
- la verifica di apprendimento e di efficacia della formazione e di consapevolezza in materia di sicurezza.

- ***Comunicazione, partecipazione e consultazione*** (Prot *A3*)

I *Delegati*, anche in collaborazione, per quanto di competenza, con *OHS Compliance Manager* e i *Referenti Operativi*, assicurano, con riferimento alle attività e alle sedi/siti aziendali afferenti al perimetro delle responsabilità assegnate, ovvero alle sedi di lavoro anche presso i Clienti della Società in cui ICTS esercita le proprie attività:

- la definizione di opportune modalità operative per ricevere, documentare, rispondere a:
  - comunicazioni interne, in materia di sicurezza, tra i vari livelli e funzioni dell'Organizzazione: comunicazione di informazioni verso tutti i lavoratori (*top-down*) e viceversa (*bottom-up*), nonché interna interfunzionale;
  - comunicazioni rilevanti con parti esterne interessate;
- il coinvolgimento e la consultazione dei lavoratori, anche per il tramite dei RLS, sulle tematiche inerenti alle diverse attività del sistema di gestione (ad esempio la scelta delle misure per il controllo dei rischi, suggerimenti per il miglioramento del sistema, il riscontro in merito all'introduzione di nuove macchine/attrezzature, *etc*.), anche attraverso la partecipazione alle riunioni periodiche previste dalla Normativa vigente ed in occasione di incontri finalizzati allo scambio di informazioni in materia ed inerenti la normale operatività aziendale.

- ***Documentazione del Sistema e controllo delle registrazioni*** (Prot *A4*)

OHS Compliance Manager assicura, nel rispetto di quanto previsto da norme interne[9], la definizione dei documenti facenti parte del SGSL di ICTS in conformità ai requisiti del presente documento e della Norma ISO 45001, nonché la corretta gestione degli stessi, sì da garantire che il personale abbia accesso alle informazioni più recenti e approvate e limitare l'uso di informazioni obsolete.

I *Delegati*, anche in collaborazione, per quanto di competenza, con *OHS Compliance Manager* e i *Referenti Operativi*, assicurano, con riferimento alle attività e alle sedi/siti aziendali afferenti al perimetro delle responsabilità assegnate, ovvero alle sedi di lavoro anche presso i Clienti della Società in cui ICTS esercita le

[9] Che disciplinano i criteri in base ai quali la documentazione deve essere prodotta, verificata, approvata, distribuita (eventualmente anche in forma controllata e/o numerata al fine di prevenire l'utilizzo di materiale obsoleto), quindi tenuta sotto controllo, conservata e archiviata.

proprie attività, la corretta gestione delle evidenze documentate del SGSL, in linea con quanto previsto dalle procedure del SGSL.

- ***Procedure documentate, controlli e criteri operativi*** (Prot *A5)*

I *Delegati*[10], avvalendosi della collaborazione o per il tramite di *OHS Compliance Manager* e del *RSPP,* anche coinvolgendo il *RLS*, assicurano la definizione e la formalizzazione di specifiche procedure / controlli operativi facenti parte del SGSL necessari alla gestione dei rischi connessi a operazioni e attività lavorative per le quali sono identificati, anche nell'ambito dei documenti di valutazione dei rischi, pericoli per la salute e sicurezza dei lavoratori (ad esempio, controlli correlati all'acquisto di beni o prodotti di terzi, alla guida di autoveicoli da parte del personale ICTS, all'utilizzo di sostanze pericolose, alla movimentazione manuale dei carichi).

In particolare, il SGSL adottato (coerentemente con quanto già stabilito dal DVR) deve prevedere, tra l'altro, procedure / controlli operativi per:

- le attività all'interno del sedime aeroportuale:
  - utilizzo di veicoli di ICTS in circolazione e manovra;
  - circolazione a piedi all'interno del sedime;
  - circolazione con automezzi ICTS;
  - attività in momenti di esposizione al rumore;
  - accesso in stiva per mezzo di piattaforme mobili elevabili;
  - lavorazioni in aree a rischio esplosione;
  - lavorazioni in ambienti con presenza di folla;
  - lavorazioni in rampa non previste;
  - attività di sorveglianza e controllo colli radioattivi;
  - attività durante le operazioni di rifornimento carburante aeromobile;
  - attività di controllo durante le operazioni di rifornimento *catering*;
  - attività di verifica stive e automezzi nelle fasi di carico e scarico bagagli e merci;
  - operazioni in condizioni meteo avverse con scarsa visibilità;
  - uso/movimentazione attrezzature per assistenza aeromobili;
  - pulizie a bordo aeromobili;
  - sostanze alcoliche e stupefacenti;
- l'utilizzo di veicoli aziendali;
- l'utilizzo di apparecchiature videoterminali;
- l'utilizzo di apparati elettrici, fissi o mobili;

[10] Ciascuno con riferimento alle attività e alle sedi/siti aziendali afferenti al perimetro delle responsabilità assegnate, ovvero alle sedi di lavoro anche presso i Clienti della Società in cui ICTS esercita le proprie attività.

- il lavoro in solitario;
- la gestione del rischio rumore;
- la segnalazione di possibili pericoli;
- la regolamentazione delle norme comportamentali che i lavoratori devono adottare nello svolgimento dei proprio compiti con indicazione delle possibili sanzioni disciplinari in caso di accertata violazione.

- ***Gestione degli asset*** (Prot *A6*)

I *Delegati*[10], anche in collaborazione, per quanto di competenza, con *OHS Compliance Manager* e i *Referenti Operativi*, assicurano la manutenzione degli *asset*(quali edifici, autoveicoli, impianti, attrezzature, *etc*.), affinché ne sia sempre garantita l'integrità e adeguatezza, attraverso:

- periodiche verifiche di adeguatezza, integrità e conformità ai requisiti normativi applicabili. Tali verifiche sono da operarsi anche al momento dell'ingresso in Azienda di nuove macchine, attrezzature e prima dell'utilizzo delle stesse da parte degli operatori abilitati, unitamente ad una valutazione dei rischi connessa al loro utilizzo prima del relativo impiego operativo;
- la pianificazione, effettuazione e verifica delle attività di ispezione e manutenzione, sia ordinaria che non, tramite personale qualificato e idoneo;
- nel caso di *asset* di terzi utilizzato da personale ICTS, l'acquisizione della documentazione attestante l'adeguatezza, conformità e avvenuta manutenzione in accordo alla normativa applicabile.

- ***Affidamento compiti e mansioni*** (Prot *A7*)

I *Delegati*[11], in collaborazione con i *Referenti Operativi*, garantiscono che ai lavoratori siano affidati compiti e mansioni, sia in fase di inserimento sia in caso di trasferimento o cambio di mansione, in base alle capacità e alle condizioni degli stessi in rapporto alla loro salute e alla sicurezza, oltre che a quanto emerso dai risultati degli accertamenti sanitari eseguiti.

- ***Dispositivi di Protezione Individuale*** (Prot *A8*)

I *Delegati*[11], in collaborazione con i *Referenti Operativi*, assicurano la gestione, distribuzione e mantenimento in efficienza dei Dispositivi di Protezione Individuali ("***DPI***"), attraverso:

- la verifica dei necessari requisiti quali resistenza, idoneità e mantenimento in buono stato di conservazione ed efficienza dei *DPI*;
- la tracciabilità delle attività di consegna e di verifica della funzionalità dei *DPI*.

[11] Ciascuno con riferimento alle attività e alle sedi/siti aziendali afferenti al perimetro delle responsabilità assegnate, ovvero alle sedi di lavoro anche presso i Clienti della Società in cui ICTS esercita le proprie attività.

- ***Gestione delle trasferte e dei distaccati*** (Prot *A9*)

I *Delegati*[11], in collaborazione con *OHS Compliance Manager* e i *Referenti Operativi,* assicurano la corretta gestione delle trasferte/distacchi presso clienti, fornitori, cantieri, atta a garantire la tutela della salute e sicurezza dei lavoratori, attraverso:

- il trasferimento di tutte le informazioni/formazione necessarie allo svolgimento in sicurezza delle attività presso la sede di destinazione;
- la verifica, da parte del *MC*, dell'idoneità a svolgere le attività nella sede di destinazione e che lo stesso sia in possesso dei *DPI* necessari allo svolgimento in sicurezza delle attività;
- la garanzia che *in loco*, se non fatto in via preventiva dalla sede, vengano fornite tutte le informazioni necessarie e relative alla gestione delle emergenze, vie di fuga, allarmi, *etc*. nonché sull'utilizzo dei *DPI* per l'accesso a specifiche aree;
- la formalizzazione delle modalità operative per l'autorizzazione allo svolgimento delle attività in trasferta/fuori sede.

- ***Gestione delle emergenze e del rischio incendio*** (Prot *A10*)

I *Delegati*[11], in collaborazione, per quanto di competenza, con *OHS Compliance Manager*, il *RSPP* e i *Referenti Operativi*, anche consultando i *RLS*, assicurano l'adozione delle misure necessarie alla prevenzione e gestione delle emergenze e del rischio incendio, attraverso[12]:

- l'identificazione delle potenziali situazioni di emergenza e l'individuazione delle misure per il controllo di dette situazioni (tenendo in considerazione anche le necessità delle parti interessate rilevanti tra cui l'ambiente esterno, i vicini, i vigili del fuoco, ambulanza, *etc*.), ivi comprese le indicazioni sulle modalità di abbandono del posto di lavoro o zona pericolosa in cui persiste un pericolo grave e immediato, e sulle modalità di intervento dei lavoratori incaricati dell'attuazione delle misure di prevenzione incendi, di evacuazione dei lavoratori in caso di pericolo grave e immediato e di pronto soccorso;
- la predisposizione dei Piani di Emergenza tenendo in considerazione anche lo storico di incidenti, emergenze e infortuni avvenuti nei diversi siti aziendali, nonché il riesame dei rapporti sulle esercitazioni effettuate e sulle valutazioni dell'efficacia delle azioni adottate, se richieste, dopo dette esercitazioni;
- l'effettuazione di opportune prove di emergenza per testare tutte le procedure identificate e coinvolgendo, quando praticabile e appropriato, tutte le parti interessate anche esterne;
- la definizione delle misure dirette ad evitare l'insorgere di un incendio e a limitare le conseguenze qualora si verifichi (mezzi di estinzione idonei alla classe di incendio e al livello di rischio presenti sul luogo di lavoro e prescrizioni per le modalità di utilizzo), quindi dei metodi di controllo e manutenzione degli impianti e delle attrezzature antincendio;
- la tenuta, il posizionamento e la conservazione delle cassette di pronto soccorso, nonché l'identificazione e la verifica del contenuto (verifica scadenze, completezza, aggiornamento).

[12] Anche attraverso l'acquisizione del Piano di emergenza e delle procedure di emergenza del Cliente, ovvero la collaborazione con il personale competente del Cliente.

- ***Sorveglianza sanitaria*** (Prot *A11*)

I *Delegati*[13], in collaborazione, per quanto di competenza, con *OHS Compliance Manager* e i *Referenti Operativi*, avvalendosi dell'operato del *MC*, assicurano, nel rispetto della normativa vigente, la conduzione delle attività di sorveglianza sanitaria, attraverso:

- la programmazione e gestione delle visite mediche e, più in generale, della sorveglianza sanitaria dei lavoratori, nonché della visita periodica degli ambienti di lavoro;
- la verifica del possesso e del mantenimento nel tempo da parte dei lavoratori dei requisiti di idoneità fisica alla mansione di destinazione;
- la definizione dei criteri in base ai quali effettuare le visite mediche (preventiva intesa a constatare l'idoneità alla mansione, periodica per monitorare il giudizio di idoneità, al cambio mansione, su richiesta del lavoratore, *etc*.) e dei provvedimenti da adottare nel caso di non idoneità riscontrata;
- la definizione delle modalità per la gestione e conservazione della documentazione relativa alla sorveglianza sanitaria (protocollo sanitario, la cartella sanitaria e di rischio dei lavoratori, *etc*.).

- ***Gestione di un'emergenza epidemiologica*** (Prot *A12*)

In relazione al possibile manifestarsi di una situazione di emergenza di natura epidemiologica il *Datore di Lavoro*, anche per il tramite dei *Delegati*[13], coadiuvato dal *RSPP* e dal *MC*, in collaborazione con *OHS Compliance Manager* e il *Comitato Crisi* (come indicato in appresso), sovrintende e garantisce:

- l'identificazione delle prescrizioni applicabili alla Società in relazione all'emergenza contingente (ad esempio, Decreti-legge, DPCM, Circolari del Ministero della salute, Circolari dell'INAIL, Ordinanze ministeriali, regionali e locali);
- l'individuazione degli ambiti di applicazione delle prescrizioni e la definizione delle azioni da intraprendere per il raggiungimento della conformità a tali requisiti, nonché l'assegnazione delle relative responsabilità e dei tempi di attuazione;
- la comunicazione delle informazioni rilevanti al personale e alle parti interessate anche esterne;
- il riesame delle attività svolte dall'Organizzazione rispetto ai requisiti e alle prescrizioni applicabili, ad intervalli periodici da definire in funzione delle circostanze e/o su base evento (in quest'ultimo caso qualora, ad esempio, si presentino modifiche delle attività lavorative, modifiche legislative o regolamentari, ovvero siano segnalate possibili non conformità);
- in collaborazione con il *RSPP* e il *MC*, con il coinvolgimento dei *RLS*[14] di cui al D.Lgs. n. 81/2008, una valutazione del rischio specifica[15], legata alla particolare realtà aziendale ICTS, che consideri le peculiarità sensibili sotto il profilo del rischio contagio (ad esempio, con riguardo alla distanza tra le persone, agli spostamenti, all'adozione di *DPI* non compatibili con quelli indicati dalle Autorità sanitarie competenti in materia), anche in relazione al rapporto con i fornitori/appaltatori/ditte

[13] Ciascuno con riferimento alle attività e alle sedi/siti aziendali afferenti al perimetro delle responsabilità assegnate, ovvero alle sedi di lavoro anche presso i Clienti della Società in cui ICTS esercita le proprie attività.

[14] Anche con il coinvolgimento delle Organizzazioni Sindacali, ove previsto dalla normativa applicabile in materia o ritenuto opportuno anche in relazione, ad esempio, a questioni giuslavoristiche.

[15] Nonché "indiretta", ovvero legata alle conseguenze dell'emergenza e delle necessarie misure da adottare in merito, anche con riferimento ai rischi psico sociali legati allo stress lavoro correlato.

affidatarie[16], quindi l'aggiornamento, ove necessario o ritenuto opportuno, del *DVR* e dei *DUVRI* e delle procedure aziendali impattate;

- la predisposizione di protocolli aziendali per la prevenzione e gestione del contagio che declinino, anche in termini di responsabilità e modalità di attuazione, misure tecniche, organizzative e procedurali[17] volte a recepire le previsioni normative applicabili all'emergenza contingente e le determinazioni stabilite in esito al processo di valutazione del rischio, anche di natura interferenziale;
- le necessarie attività di comunicazione, informazione/formazione e addestramento in accordo a quanto stabilito dal processo di valutazione dei rischi e dalla normativa applicabile in materia;
- la pianificazione e attuazione di verifiche, anche eventualmente avvalendosi della collaborazione di soggetti esterni qualificati e indipendenti, rivolte ad attestare l'idoneità dell'organizzazione e delle misure adottate per la gestione dell'emergenza nonché l'effettiva ed efficace applicazione;
- la tracciabilità delle diverse fasi del processo di gestione dell'emergenza epidemica, ovvero la conservazione della documentazione attestante l'espletamento delle rilevanti attività e decisioni assunte.

Il *Datore di Lavoro*, ove ritenuto opportuno o previsto dalla normativa applicabile, istituisce un *Comitato Crisi* (con la presenza di *Delegati*) dedicato alla gestione dell'emergenza - in possesso delle necessarie competenze di natura tecnica e organizzativa e a cui siano assegnate responsabilità e, ove ritenuto necessario, opportune risorse - avente i compiti, in particolare e fermi restando quelli previsti dalla suddetta normativa applicabile, di[18]:

- verificare l'adeguatezza dei protocolli aziendali anti-contagio e l'effettiva applicazione delle misure previste;
- valutare la necessità e, nel caso, promuovere l'aggiornamento dei protocolli anti-contagio con riferimento sia alle novità legislative, sia ai nuovi accorgimenti tecnico-sanitari idonei a evitare la diffusione del virus;

[16] Con riferimento, ad esempio, all'accesso alle sedi aziendali, all'utilizzo di spazi/aree o attrezzature comuni, alla regolamentazione delle attività, in termini di tempistiche / turnazioni e modalità di svolgimento delle attività in sicurezza.

[17] Potranno essere definiti specifici controlli operativi, anche ad integrazione delle procedure/istruzioni interne già in essere in materia di sicurezza, ad esempio, con riferimento a:

- pulizia e sanificazione degli impianti di areazione;
- sanificazione e utilizzo di ambienti di lavoro (uffici, aree comuni, mense, aree ristoro, *etc.*);
- dotazione e utilizzo di DPI (mascherine, gel igienizzante, *etc.*);
- la gestione degli appalti *ex* art. 26 e dei cantieri di cui al Titolo IV del D.Lgs. n. 81/2008 e s.m.i.;
- la gestione dell'emergenza, in relazione, in particolare, a ciò che attiene alle misure di primo soccorso per le manovre di rianimazione cardio polmonare, nonché alle mutate condizioni organizzative (ad esempio numero addetti disponibili, luoghi e condizioni di lavoro);
- al protocollo sanitario e alla gestione del personale, in relazione, in particolare, a:
  - regolamentazione delle visite mediche e degli esami diagnostici, dei casi sospetti o postivi, dei casi di fragilità prima del rientro a lavoro;
  - adozione di adeguate misure per la minimizzazione del rischio contagio del lavoratore sottoposto a visita/esami diagnostici o strumentali;
  - coinvolgimento del *MC*, per gli aspetti di competenza, nelle diverse fasi del processo di gestione dell'emergenza, anche in relazione alla gestione dei casi sospetti, positivi o delle situazioni di fragilità, ovvero per la ricostruzione della catena dei contatti;
  - eventuali prescrizioni o limitazioni alle attività lavorative del personale in condizioni di fragilità congenita o acquisita.

[18] Nello svolgimento dei propri compiti il *Comitato Crisi* può avvalersi della collaborazione dei *Delegati* e delle Funzioni aziendali competenti.

- supportare tutte le parti interessate, interne ed esterne, in ordine alla corretta applicazione dei suddetti protocolli, ovvero, più in generale, con rifermento alle diverse tematiche rilevanti, provvedendo, ove necessario o opportuno, a specifiche comunicazioni aziendali;
- prestare collaborazione con riferimento ai rapporti con le Autorità competenti preposte alla gestione della crisi epidemiologica;
- prendere in esame, con il supporto del *RSPP* e del *MC*, eventuali incidenti, casi sospetti e infortuni, al fine di identificare le opportune azioni da porre in essere;
- relazionare periodicamente, e comunque a loro richiesta, il *Datore di Lavoro* e l'*Organismo di Vigilanza* (che verrà comunque informato tempestivamente della costituzione del *Comitato Crisi*) sulle azioni intraprese dalla Società in adempimento alle normative applicabili e circa l'esito del monitoraggio svolto in ordine alla corretta attuazione delle misure stabilite.

- ***Vigilanza*** (Std *A6*)

I *Delegati*[19], avvalendosi della collaborazione, per quanto di competenza, di *OHS Compliance Manager*, del *RSPP*, del *MC* e dei *Referenti operativi*, assicurano la corretta attuazione delle misure di prevenzione e protezione stabilite dal *DVR*/*DUVRI* e delle procedure / controlli operativi del SGSL, supervisionando le attività di vigilanza dei Preposti e prevedendo attività periodiche di monitoraggio e verifica ispettiva, anche attraverso l'utilizzo di specifiche liste di controllo.

Verifica e azioni correttive

- ***Misura e monitoraggio delle prestazioni*** (Prot *V1*)

Il *Datore di Lavoro* e i *Delegati*[20], avvalendosi della collaborazione di *OHS Compliance Manager*, del *RSPP*, del *MC* e dei *Referenti Operativi*, assicurano la misura e il monitoraggio delle prestazioni degli elementi del SGSL, attraverso:

- il monitoraggio del grado di conseguimento degli obiettivi di miglioramento e dell'efficacia dei controlli definiti;
- l'analisi di misure proattive di prestazione che monitorino la conformità ai programmi, ai controlli ed ai criteri operativi stabiliti (es. frequenza delle riunioni periodiche, frequenza delle ispezioni e degli audit, numero di comunicazioni o suggerimenti inviati dal personale, numero di sopralluoghi effettuati dai referenti competenti, *etc.*);
- l'analisi di misure reattive di *performance* che monitorino le malattie, gli incidenti e altre evidenze storiche delle deficienze di prestazione del sistema (es. numero di attività svolte in condizioni di non sicurezza registrate, numero di reclami in materia sia del personale interno, sia degli esterni, numero di "Non Conformità" da *audit*, numero di prescrizioni rilasciate da organismi pubblici di controllo *etc.*).

- ***Analisi degli incidenti e infortuni*** (Prot *V2*)

[19] Ciascuno con riferimento alle attività e alle sedi/siti aziendali afferenti al perimetro delle responsabilità assegnate, ovvero alle sedi di lavoro anche presso i Clienti della Società in cui ICTS esercita le proprie attività.

[20] Ciascuno con riferimento alle attività e alle sedi/siti aziendali afferenti al perimetro delle responsabilità assegnate, ovvero alle sedi di lavoro anche presso i Clienti della Società in cui ICTS esercita le proprie attività.

I *Delegati*[20], in collaborazione con *OHS Compliance Manager,* i *Referenti Operativi*, il *RSPP* e il *MC*, ciascuno per gli aspetti di competenza, assicurano la segnalazione, rilevazione, investigazione interna degli incidenti, infortuni e delle malattie professionali al fine di determinare le deficienze che possono causare, anche indirettamente, il verificarsi di incidenti, nonché per l'analisi delle cause e l'identificazione e gestione delle azioni correttive, preventive e di miglioramento continuo dei livelli di salute e sicurezza dei lavoratori.

- ***Gestione delle Non Conformità, delle Azioni Correttive e Preventive*** (Prot *V3*)

I *Delegati*[20], in collaborazione con *OHS Compliance Manager*, i *Referenti Operativi*, il *RSPP* e il *MC*, assicurano la rilevazione, comunicazione e gestione tempestiva delle Non Conformità del SGSL e di ciascuna delle sue componenti, attraverso l'identificazione, l'analisi delle cause e la definizione delle opportune azioni correttive/preventive per mitigare le conseguenze sulla salute e sicurezza sui luoghi di lavoro e/o prevenire il loro verificarsi.

- ***Audit interno*** (Prot *V4*)

Il *Datore di Lavoro* assicura, avvalendosi di *OHS Compliance Manager* o di soggetti qualificati e indipendenti, la conduzione di periodiche verifiche ispettive interne finalizzate a determinare se il Sistema di Gestione sia conforme ai requisiti stabiliti, sia correttamente attuato e mantenuto attivo.

- ***Controlli e sanzioni*** (Prot *V5*)

Quanto al controllo sul corretto espletamento, ad ogni livello, delle funzioni in materia di prevenzione di infortuni sul lavoro, ICTS adotta e si impegna a diffondere e ad efficacemente attuare, anche ai sensi e per gli effetti dell'art. 30 D.Lgs. n. 81/2008 e s.m.i.:

- un **modello di verifica e controllo** a più livelli - "*specifico*" su singole attività, e "*generale*" sulla funzionalità del Modello - rispettivamente corrispondenti:
  - al *Datore di Lavoro*, ai *Delegati,* ai *Referenti Operativi,* a *OHS Compliance Manager* e al *RSPP*, responsabili, nell'ambito delle rispettive competenze, di garantire la valutazione e la gestione del rischio nonché il controllo sull'adeguatezza e sull'efficace attuazione delle misure di prevenzione e protezione nel tempo adottate;
  - al *CdA* e all'*OdV*, deputati al controllo sull'attuazione della presente Parte Speciale, oltre che più in generale del Modello, e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate, nonché al riesame e all'eventuale modifica degli stessi, ove siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;
- un **sistema disciplinare**, come previsto nel Codice Etico e Disciplinare e nel Modello Organizzativo adottati (da intendersi integralmente richiamato per quanto qui non diversamente stabilito), relativamente alle violazioni e sanzioni in materia di prevenzione di infortuni sul lavoro.

In particolare, il *Modello di verifica e controllo* e il *Sistema disciplinare* predisposti da ICTS risultano articolati secondo i seguenti principi:

- i *Referenti Operativi*, anche in qualità di preposti, vigilano sul rispetto da parte dei lavoratori delle procedure, istruzioni e norme comportamentali in materia di salute e sicurezza sui luoghi di lavoro anche definite nei documenti del SGSL, intervengono per modificare il comportamento non conforme fornendo le necessarie indicazioni di sicurezza e, in caso di mancata attuazione delle disposizioni impartite o di persistenza dell'inosservanza, interrompono l'attività del lavoratore informando i *Delegati* competenti. Informano, inoltre, immediatamente i *Delegati* in caso di infortuni o quasi-infortuni avvenuti;
- ogni *Delegato* effettua un monitoraggio periodico sull'esercizio dei compiti assegnati ai *Referenti Operativi*, assumendo informazioni direttamente dai *Referenti operativi* e/o da *OHS Compliance Manager* e/o dal *RSPP*, dal *MC*, dal *RLS* o da qualsiasi lavoratore ovvero da chiunque abbia incarichi rilevanti in materia di sicurezza sui luoghi di lavoro nell'ambito o nell'interesse di ICTS;
- nel caso in cui venga a conoscenza (direttamente o su segnalazione altrui) di violazioni gravi e/o reiterate commesse da parte di un lavoratore/*Referente Operativo*, il *Delegato*:
    - valuta la sua sostituzione[21] o interviene direttamente, ove sussista un pericolo grave ed imminente di infortunio;
    - informa immediatamente il *Datore di Lavoro* ai fini della valutazione, di concerto con *Risorse Umane* e il *Delegato stesso*, dell'eventuale applicazione di sanzioni disciplinari;
- ogni *Delegato* informa immediatamente il *Datore di Lavoro* di infortuni o quasi-infortuni avvenuti, nonché di ispezioni, provvedimenti, prescrizioni o contestazioni delle competenti Autorità nell'ambito rientrante nell'oggetto della propria delega e, comunque, invia periodicamente al *Datore di Lavoro* una relazione contenente la descrizione delle attività svolte nell'esercizio della delega, di tutti problemi emersi e dei corrispondenti interventi effettuati evidenziando, altresì, la necessità di disporre eventuali iniziative o azioni correttive ovvero spese di importo superiore al *budget* assegnato;
- il *Datore di Lavoro* effettua un monitoraggio periodico sull'esercizio di tutte le funzioni delegate, assumendo informazioni direttamente dal *Delegato* e/o da *OHS Compliance Manager* e/o dal *RSPP*, dal *MC*, dal *RLS* o da qualsiasi lavoratore ovvero da chiunque abbia incarichi rilevanti in materia di sicurezza sui luoghi di lavoro nell'ambito o nell'interesse di ICTS;
- il *Datore di Lavoro* incontra periodicamente i *Delegati*, *OHS Compliance Manager* e il *RSPP* (e, ove invitati, il *MC* e/o il *RLS*) nell'ambito di riunioni denominate "*Comitato Sicurezza*", di cui viene redatto (sia pur in forma sintetica) e archiviato verbale a cura dello stesso *Datore di Lavoro*, nell'ambito delle quali vengono condivisi i contenuti delle informative di cui ai punti precedenti;
- il *Datore di Lavoro* informa tempestivamente l'*OdV* di infortuni o quasi-infortuni particolari/significativi avvenuti, nonché di prescrizioni o contestazioni delle competenti Autorità e invia una relazione scritta con cadenza annuale al *CdA* e all'*OdV* contenente la descrizione, sia pur sintetica, delle attività svolte in materia di sicurezza, anche da parte dei *Delegati*, nonché delle risultanze dei controlli e delle verifiche effettuate sul corretto espletamento delle funzioni delegate, evidenziando fatti o eventi che possano incidere sulla funzionalità della presente Parte Speciale e, più in generale, del Modello ovvero comportare l'esigenza di modifiche organizzative, individuando, per ciascuno di essi, cause e responsabilità;
- nel caso in cui il *Datore di Lavoro* venga a conoscenza (direttamente o su segnalazione altrui) di gravi e/o reiterate violazioni commesse da parte di un *Delegato*:

[21] Ad esempio, in caso di gravi e/o reiterate violazioni.

- valuta la sua sostituzione[22] o interviene direttamente ove sussista un pericolo grave ed imminente di infortunio;
- valuta l'eventuale applicazione di sanzioni disciplinari;

- l'*OdV* informa periodicamente, in sede di relazione periodica, il *CdA* e il *Collegio sindacale* del monitoraggio svolto sull'esercizio delle funzioni in materia di sicurezza sui luoghi di lavoro descrivendo tipo e modalità dei controlli effettuati, riscontri ottenuti ed eventuali osservazioni in merito;
- nel caso in cui, in qualsiasi modo, il *CdA* venga a conoscenza di gravi, significative o reiterate violazioni in materia di sicurezza sui luoghi di lavoro da parte del *Datore di Lavoro*, dandone informativa all'*OdV*:
  - interviene provvedendo direttamente, ove sussista un pericolo di infortuni;
  - provvede all'applicazione nei confronti del *Datore di Lavoro* delle sanzioni disciplinari previste a carico di soggetti apicali;
- ogni violazione, da parte di appaltatori / fabbricanti / progettisti / istallatori / consulenti / collaboratori di ICTS, delle disposizioni, dei principi, delle procedure o delle regole di comportamento previste dal Modello e agli stessi applicabili, al fine della prevenzione dei reati in materia di igiene e sicurezza nei luoghi di lavoro, oltre a costituire grave inadempimento ai sensi dell'art. 1455 c.c. e fatto salvo il risarcimento completo dei danni subìti, comporta l'applicazione - da parte del *Datore di Lavoro* - delle sanzioni previste nelle specifiche clausole contrattuali *ex* D.Lgs. n. 231/2001 inclusi, a titolo meramente esemplificativo, la facoltà di risoluzione del contratto e/o il pagamento di penali.

Riesame della Direzione

- ***Conduzione del processo di Riesame del SGSL*** (Prot *R1*)

Il *Datore di Lavoro*, i *Delegati* e *OHS Compliance Manager* conducono, almeno su base annuale, una riunione di Riesame del Sistema di Gestione della Sicurezza, finalizzata a valutarne l'adeguatezza, l'efficacia e le possibilità di miglioramento. Durante le riunioni di Riesame sono analizzate le prestazioni di tutti gli elementi del Sistema come declinati nel presente documento, quindi verbalizzate almeno le seguenti informazioni:

- motivazioni di un eventuale mancato conseguimento di obiettivi definiti, di una loro modifica in fase di avanzamento e di un eventuale mancata effettuazione di *audit* e di formazione;
- giustificazioni (o segnalazioni per future indagini) di qualsiasi *trend* negativo di prestazioni del Sistema, nel periodo considerato;
- previsioni di azioni di adeguamento a nuove norme di prossima entrata in vigore che impattino significativamente sull'Organizzazione e sulla sua *Politica* di salute e sicurezza sui luoghi di lavoro;

Il *Datore di Lavoro* provvede alla comunicazione tempestiva dei risultati del Riesame al *CdA* e all'*OdV*.

[22] Ad esempio, in caso di gravi e/o reiterate violazioni

E.4 Riepilogo dei flussi informativi all'Organismo di Vigilanza

Si riporta a seguire una tabella dei flussi informativi oggetto di comunicazione all'*Organismo di Vigilanza*, indicativa del Soggetto/Funzione responsabile e della periodicità dell'invio.

Prospetto dei flussi informativi all'Organismo di Vigilanza		
Informazioni	**Responsabile della comunicazione**	**Periodicità**
Informativa riepilogativa delle voci di spesa e della tipologia degli investimenti sostenuti in materia di Salute e Sicurezza sui luoghi di lavoro, indicativa del relativo oggetto/ambito e importo	*Delegati*	Annuale
Verificarsi di un incidente/infortunio, con indicazioni dei risultati delle prime indagini/analisi effettuate e delle azioni stabilite	*Datore di Lavoro*	Tempestiva
Informativa riepilogativa degli esiti dei controlli e delle ispezioni e di eventuali contestazioni da parte delle Autorità pubbliche / Organi di controllo	*Delegati*	Semestrale[23]
Relazione di sintesi delle attività svolte in materia di sicurezza, anche da parte dei *Delegati*	*Datore di Lavoro*	Annuale[24]
Report degli infortuni, occorsi sia al personale ICTS sia al personale di ditte appaltatrici, con l'indicazione della tipologia di infortunio, della prognosi, delle cause, della struttura di appartenenza del lavoratore e delle (principali) azioni correttive attuate	*OHS Compliance Manager*	Annuale
Sanzioni disciplinari comminate, con indicazione del destinatario e delle violazioni contestate	*Datore di Lavoro*	Tempestiva
Aggiornamenti al sistema di deleghe *ex* art. 16 D.Lgs. n. 81/2008 e s.m.i.	*Datore di Lavoro*	Tempestiva
Pianificazione della formazione del personale e del relativo stato di attuazione, incluse le verifiche di apprendimento	*Delegati*	Annuale
Esiti delle verifiche ispettive interne e di certificazione del SGSL	*OHS Compliance Manager*	Tempestiva
Risultati del Riesame alla Direzione	*OHS Compliance Manager*	Annuale

E.5 Archiviazione e Conservazione

I Soggetti e le Funzioni interessate alle attività del processo "*Gestione della Salute e Sicurezza sui Luoghi di Lavoro*", ciascuno per gli aspetti di competenza, sono tenute ad archiviare e conservare la documentazione di pertinenza per un periodo di tempo pari ad almeno cinque anni.

E.6 Allegati

- **Allegato 1 alla Parte Speciale** – Allineamento dei protocolli di controllo rispetto a quanto previsto dall'art. 30 del D.Lgs. n. 81/2008 e s.m.i.

[23] Entro il 31 luglio dell'anno in corso.

[24] Entro il 31 gennaio dell'anno successivo.

Allegato 1 alla Parte Speciale – Allineamento dei protocolli di controllo rispetto a quanto previsto dall'art. 30 del D.Lgs. n. 81/2008 e s.m.i.

Protocolli di gestione		Riferimenti art. 30 D.Lgs. n. 81/2008 e s.m.i.											
		Art. 30, 1° co. lett. a) rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici	**Art. 30, 1° co. lett. b)** attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti	organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza	**Art. 30, 1° co. lett. d)** attività di sorveglianza sanitaria	**Art. 30, 1° co. lett. e)** attività di informazione e formazione dei lavoratori	con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori	**Art. 30, 1° co. lett. g)** acquisizione di documentazioni e certificazioni obbligatorie di legge	**Art. 30, 1° co. lett. h)** periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate	**Art. 30, 2° co.** Il modello organizzativo …deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività	**Art. 30, 3° co.** articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio	**Art. 30, 4° co.** sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati
P1	Politica												
P2	Valutazione dei rischi e predisposizione delle relative misure di prevenzione e protezione												
P3	Conformità Legislativa												
P4	Obiettivi e Programmi di miglioramento												
A1	Organizzazione Responsabilità												
A2	Informazione, formazione e addestramento												
A3	Comunicazione, partecipazione e consultazione												
A4	Documentazione del Sistema e controllo delle registrazioni												
A5	Procedure documentate, controlli e criteri operativi												
A6	Gestione degli asset												
A7	Affidamento compiti e mansioni												
A8	Dispositivi di protezione individuale												

Protocolli di gestione		Riferimenti art. 30 D.Lgs. n. 81/2008 e s.m.i.											
		Art. 30, 1° co. lett. a) rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici	**Art. 30, 1° co. lett. b)** attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti	organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza	**Art. 30, 1° co. lett. d)** attività di sorveglianza sanitaria	**Art. 30, 1° co. lett. e)** attività di informazione e formazione dei lavoratori	con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori	**Art. 30, 1° co. lett. g)** acquisizione di documentazioni e certificazioni obbligatorie di legge	**Art. 30, 1° co. lett. h)** periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate	**Art. 30, 2° co.** Il modello organizzativo ...deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività	**Art. 30, 3° co.** articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio	**Art. 30, 4° co.** sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati
A9	Gestione delle trasferte e dei distaccati												
A10	Gestione delle emergenze e del rischio incendio												
A11	Sorveglianza sanitaria												
A12	Gestione di un'emergenza epidemiologica												
V1	Misura e monitoraggio delle prestazioni												
V2	Analisi degli incidenti e infortuni												
V3	Gestione delle Non Conformità, delle Azioni Correttive e Preventive												
V4	Audit interno												
V5	Controlli e sanzioni												
R1	Conduzione del processo di riesame del SGSL												