Il Modello di organizzazione, gestione e controllo ai sensi del D.lgs. 8 giugno 2001 n. 231

Parte Generale

di

C.R. TECHNOLOGY SYSTEMS S.p.A.

N.	REVISIONE	DATA	Per l'Assemblea
1	Prima approvazione del Modello Parte Generale		Il Presidente_____
2	Prima revisione Parte Generale		Il Presidente_____

INDICE

DEFINIZIONI

- **Attività sensibili:** attività svolta d C.R. TECHNOLOGY SYSTEMS S.p.A., come da oggetto sociale, nel cui ambito potrebbe essere realizzata una condotta in grado, anche solo potenzialmente, di integrare uno dei reati di cui al D.lgs. 231 del 2001.
- **CCNL:** contratto collettivo nazionale di lavoro vigente per categoria di dipendenti.
- **Cliente:** persona giuridica e/o persona fisica che acquista un bene o un servizio.
- **Codice di Comportamento o Codice Etico:** il codice di comportamento adottato da C.R. TECHNOLOGY SYSTEMS S.p.A..
- **Consulenti o Collaboratori:** soggetti che in ragione delle competenze professionali prestano la propria opera intellettuale a favore e/o per conto di C.R. TECHNOLOGY SYSTEMS S.p.A. sulla base di un mandato o di altro rapporto di collaborazione professionale.
- **D.lgs. 231/2001 o Decreto:** il decreto legislativo 8 giugno 2001 n. 231 e s.m.i..
- **Dipendenti:** soggetti aventi con C.R. TECHNOLOGY SYSTEMS S.p.A. un contratto di lavoro subordinato o parasubordinato.
- **C.R. TECHNOLOGY SYSTEM S.p.A.:** C.R. TECHNOLOGY SYSTEMS S.p.A. o Società.
- **Fornitore:** persona fisica o giuridica che producono - distribuiscono, prodotti, materie prime, componenti, servizi, consulenze professionali, consulenze tecniche etc.
- **Incaricato di un pubblico servizio:** colui che "a qualunque titolo presta un pubblico servizio", intendendosi per "pubblico servizio" un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima (cfr. art. 358 codice penale).
- **Linee guida Confindustria:** documento guida di Confindustria (approvato il 7 marzo 2002 ed aggiornato il 31 marzo 2008 e nuovamente aggiornato nel marzo 2014 e s.m.i) per la costruzione di modelli di organizzazione, gestione e controllo di cui al Decreto Legislativo n. 231 del 2001.
- **Modello:** il modello di organizzazione, gestione e controllo ai sensi del Decreto Legislativo 231/2001.
- **Organi Sociali:** assemblea, collegio sindacale e revisore, organo amministrativo.
- **Organismo di vigilanza o OdV:** l'organismo di cui all'articolo 6 del Decreto legislativo 8 giugno 2001, n. 231.
- **Partner:** parti contrattuali, persone fisiche o giuridiche, con cui C.R. TECHNOLOGY SYSTEMS S.p.A. addivenga ad una qualunque forma di collaborazione.
- **P.A.:** la pubblica amministrazione, il pubblico ufficiale o l'incaricato di un pubblico servizio.
- **Pubblico ufficiale:** colui che "esercita una pubblica funzione legislativa, giudiziaria o amministrativa" (cfr. articolo 357 codice penale).
- **Reato presupposto e/o Reato:** i reati presupposto della responsabilità amministrativa di cui al Decreto legislativo 8 giugno 2001 n. 231.

- **Soggetto Apicale:** persona che riveste funzioni di rappresentanza, di amministrazione, di direzione di C.R. TECHNOLOGY SYSTEMS S.p.A. o di una sua unità dotata di autonomia finanziaria e funzionale, nonché persona che esercita, anche di fatto, la gestione o il controllo di C.R. TECHNOLOGY SYSTEMS S.p.A. ai sensi del Decreto Legislativo 8 giugno 2001, n. 231.
- **Soggetto Subordinato:** persone sottoposte alla direzione o alla vigilanza di uno dei Soggetti Apicali ai sensi del Decreto legislativo 8 giugno 2001, n. 231.
- **TUF:** Decreto legislativo 24 febbraio 1998, numero 58 (testo unico della finanza).
- **TUSSL:** Decreto legislativo 9 aprile 2008, numero 81 (testo unico sulla sicurezza).
- **TUA:** Decreto legislativo 3 aprile 2006, n. 152 (testo unico in materia ambientale).
- **Vertice:** Consiglio di Amministrazione di C.R. TECHNOLOGY SYSTEMS S.p.A..

****

C.R. TECHNOLOGY SYSTEMS S.p.A., ai sensi di statuto, ha quale oggetto sociale l'installazione, la compravendita, la manutenzione, la riparazione e la rappresentanza di impianti tecnologici, elettromeccanici, edili, chimici, elettronici, termici, elettrici, idraulici e simili, nonché la compravendita e la rappresentanza di automobili, autobus, camion, trattori, motocicli, ciclomotori e relativi ricambi e lo svolgimento di ogni altra attività collaterale ed inerente a quanto sopra; l'elaborazione di dati contabili nonché la tenuta delle scritture contabili in genere per conto di terzi nei modi e limiti consentiti dalla legge. La società può inoltre: - con fini meramente strumentali per il conseguimento del proprio oggetto: compiere tutte le operazioni mobiliari ed immobiliari, commerciali, industriali, bancarie e finanziarie utili o necessarie; - esclusivamente con finalità strumentali per il conseguimento dell'oggetto sociale: a) rilasciare fideiussioni, avvalli e garanzie di qualsiasi genere e compiere tutte le operazioni mobiliari ed immobiliari, industriali, commerciali e finanziarie connesse e relative direttamente o indirettamente a siffatta normativa dettata dal d.lgs. n. 385 del 1° settembre 1993 (TUB), su eventuali successive modifiche legislative ed atti amministrativi emanati in operazioni del caso in cui sia attuata nei confronti dei dipendenti, entro i limiti e con le modalità consentite dell'art. 1 del decreto del ministero del tesoro del 29 marzo 1995, in attuazione delle disposizioni del citato decreto n, 385 del 1° settembre 1993 (TUB); b) assumere, non nei confronti del pubblico, né a scopo di collocamento, interessenza e partecipazioni in altre società o aziende commerciali sia direttamente che indirettamente, purché il possesso di tali interessenze e partecipazioni non si ponga in contrasto con la normativa dettata dal d.lgs. n. 385 del 1 settembre 1993 (TUB).

PREMESSA

Il Modello organizzativo, strutturato in una Parte Generale e in Parti Speciali, comprende di massima una disamina della disciplina contenuta nel D.lgs. 8 giugno 2001, n. 231 e costituisce le linee guida che descrivono il processo di adozione del Modello da parte delle società.

Il Modello parte generale individua:

- le fattispecie presupposto dei reati di cui al D.lgs. 8 giugno 2001 n. 231;
- i Destinatari del Modello e del Codice Etico;
- le modalità di adozione e attuazione del Modello;
- i criteri di costituzione dell'Organismo di Vigilanza;
- il sistema sanzionatorio a presidio delle violazioni;
- gli obblighi di informazione e comunicazione e di formazione del personale sul Modello;
- il modulo di segnalazione di violazioni al Codice Etico e al Modello di C.R. TECHNOLOGY SYSTEMS S.p.A..

Le Parti Speciali, tenuto conto dell'oggetto sociale della società, individuano le attività della stessa sensibili ai rischi di cui al Decreto legislativo 8 giugno 2001, n. 231, i principi generali e specifici di buon comportamento, gli elementi di prevenzione posti dalla società a presidio dei suddetti rischi e le misure di controllo essenziali deputate alla prevenzione o alla mitigazione degli illeciti.

Oltre a quanto di seguito espressamente stabilito, sono inoltre parte integrante del presente documento:

- il Codice Etico che definisce i principi etico-morali dell'azienda;
- tutte le disposizioni, i provvedimenti interni, gli atti, i sistemi gestionali e le procedure operative aziendali che di questo documento costituiscono attuazione (es. conferimento/riconoscimento/delega di poteri, organigrammi, *job description*, statuto, procedure per la sicurezza sui luoghi di lavoro, manuale qualità, DVR, Sistema gestionale in materia salute sicurezza, qualità e ambiente, analisi dei rischi in materia di riservatezza e di trattamento dei dati personali, SGSL, etc.).

2. LA RESPONSABILITA' AMMINISTRATIVA DELLE PERSONE GIURIDICHE, DELLE SOCIETA' E DELLE ASSOCIAZIONI

Il Decreto legislativo 8 giugno 2001 n. 231, ha introdotto e disciplinato, per la prima volta nel nostro ordinamento, la responsabilità amministrativa degli enti dotati di personalità giuridica a seguito di condotte integranti fattispecie di Reato commesse nell'interesse ed a vantaggio degli stessi.

Le previsioni del D.lgs. 8 giugno 2001 n. 231 operano qualora i soggetti Apicali e/o Subordinati abbiano tenuto comportamenti non conformi e/o condotte illecite integranti una delle fattispecie presupposto di cui al Decreto e da tale condotta la società abbia tratto interesse o vantaggio.

In tali circostanze alla Società potrà essere ascritta, in sede penale, una autonoma responsabilità rispetto a quella personale dell'Apicale o Subordinato che ha tenuto il comportamento non conforme o la condotta illecita integrante

il Reato; responsabilità che, in capo alla medesima Società, permane ai sensi di legge anche nei casi in cui non venga identificato l'autore dell'illecito e/o il Reato si estingua per una causa diversa dall'amnistia.

La responsabilità amministrativa in sede penale delle società ai sensi del Decreto invero, va sempre ad aggiungersi e mai a sostituirsi a quella della persona fisica responsabile della condotta illecita, il cui comportamento costituisce il presupposto per l'addebito della specifica responsabilità.

Il Decreto legislativo 8 giugno 2001 n. 231 ha tra i suoi obiettivi, anche, quello di sensibilizzare tutti i portatori di interessi della società, colpendo anche il patrimonio di coloro che hanno avuto un interesse o hanno tratto un vantaggio dal comportamento illecito dei propri Soggetti Apicali e/o Subordinati.

L'apparato sanzionatorio del Decreto prevede differenti tipologie di sanzione che si prescrivono nel termine di cinque anni dalla data di consumazione del Reato, tra queste ricordiamo: le sanzioni amministrative pecuniarie, le sanzioni interdittive, la pubblicazione della sentenza e la confisca.

I criteri di riferimento per la determinazione delle sanzioni da applicare sono: la gravità del fatto, il grado di responsabilità della società e le attività messe in atto da quest'ultima per prevenire il Reato.

Per le ipotesi di maggiore gravità, quali ad esempio i reati commessi in violazione delle disposizioni in materia di salute e sicurezza dei luoghi di lavoro, è prevista anche l'applicazione di sanzioni interdittive quali:

a) l'interdizione dall'esercizio dell'attività;
b) la sospensione o revoca di autorizzazioni o licenze o concessioni;
c) il divieto di contrattare con la Pubblica Amministrazione;
d) l'esclusione da finanziamenti agevolati o simili sussidi o la revoca di quelli già concessi;
e) la pubblicazione della sentenza.

3. IL CAMPO DI APPLICAZIONE

Il Decreto si applica a tutti gli enti dotati di personalità giuridica, alle società, alle associazioni anche prive di personalità giuridica, agli enti privati concessionari di un pubblico servizio. Il Decreto non è invece applicabile allo Stato, agli Enti pubblici territoriali, agli Enti pubblici non economici, agli Enti che svolgono funzioni di rilievo costituzionale (esempio: sindacati, partiti politici, etc.).

4. DESTINATARI

Si intendono Destinatari ai sensi del presente Modello senza alcuna eccezione:

- il Personale di C.R. TECHNOLOGY SYSTEMS S.p.A., definendo in tal modo i dipendenti, anche all'estero, di C.R. TECHNOLOGY SYSTEMS S.p.A., nonché tutti quei soggetti che collaborano con la stessa in forza di un rapporto di lavoro parasubordinato e di collaborazione in genere, inclusi collaboratori a progetto, prestatori di lavoro temporaneo ed in somministrazione, etc.;

- coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo per C.R. TECHNOLOGY SYSTEMS S.p.A. o per una sua unità organizzativa, organi societari inclusi (Amministratori, Sindaci, Revisore e Società di Revisione, organismo di vigilanza etc.);
- coloro che direttamente o indirettamente, stabilmente o temporaneamente, instaurano con C.R. TECHNOLOGY SYSTEMS S.p.A., a qualsiasi titolo, contratti e/o rapporti di collaborazione, operando per conto della stessa o cooperando allo svolgimento della sua attività ed al perseguimento dei suoi fini;
- tutti i soggetti che comunque agiscono nell'interesse di C.R. TECHNOLOGY SYSTEMS S.p.A. in quanto legati alla stessa da rapporti giuridici contrattuali o da accordi di altra natura (ad esempio *partner* in *joint-venture*, soci in iniziative di business etc.).

I Destinatari del Modello sono tenuti a rispettare puntualmente le disposizioni contenute nello stesso e nei suoi allegati che ne costituiscono parte integrante e sostanziale.

5. CRITERI DI IMPUTAZIONE DELLA RESPONSABILITÀ

L'accertamento della responsabilità delle società ai sensi del Decreto presuppone la commissione o (anche solo) il tentativo di commissione da parte di una persona fisica di un "determinato reato-presupposto": pertanto, non ogni reato comporta la responsabilità dell'ente, ma solo quelli espressamente previsti dal decreto, in ottemperanza al principio di legalità. Tale accertamento costituisce, tuttavia, un presupposto necessario, ma non sufficiente; affinché sorga la responsabilità dell'ente è, infatti, indispensabile che il reato sia ad esso riconducibile in base ad un profilo tanto oggettivo, quanto soggettivo.

Pertanto, i criteri di imputazione della responsabilità ai sensi del Decreto alle società (dunque anche a C.R. TECHNOLOGY SYSTEMS S.p.a.) si distinguono in soggettivi e oggettivi. A tal proposito, anche con specifico riferimento al caso di specie, valga quanto segue.

A) Criterio soggettivo: la responsabilità ai sensi del Decreto è attribuibile alla Società quando il Reato viene integrato da un soggetto legato alla medesima da un rapporto qualificato e, più precisamente: 1) dai Soggetti in posizione Apicale, intesi come coloro che rivestono funzioni di rappresentanza, di amministrazione o di direzione di C.R. TECHNOLOGY SYSTEMS S.p.A. o di una sua unità organizzativa finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo della stessa; 2) dai Soggetti Subordinati ossia le persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui al punto 1).

Al fine di individuare questi ultimi, assume particolare rilevanza non solo l'esistenza di un contratto di lavoro subordinato, ma viene considerata altresì l'attività dai medesimi svolta in concreto, ciò al fine di evitare che si possa aggirare il disposto del Decreto legislativo 8 giugno 2001 n. 231 affidando all'esterno attività della Società che possono integrare le fattispecie presupposto di cui al Decreto.

B) Criterio oggettivo: la responsabilità ai sensi del Decreto è attribuibile alla Società quando il Reato viene commesso nell'interesse ed a vantaggio della medesima in un ambito inerente o funzionale al proprio oggetto sociale.

Per le suddette ragioni, affinché la condotta illecita dell'Apicale e/o del Subordinato possa integrare responsabilità per C.R. TECHNOLOGY SYSTEMS S.p.A. è sufficiente che sia integrata una sola delle due condizioni oggettive - interesse o vantaggio - a favore della società.

A tal fine è utile chiarire che:

- l'interesse sussiste quando l'Apicale e/o il Subordinato ha agito con l'intento di favorire C.R. TECHNOLOGY SYSTEMS S.p.A. indipendentemente dalla circostanza che tale obiettivo sia stato realmente conseguito (sulla base di una valutazione *ex ante* della condotta),
- il vantaggio sussiste quando C.R. TECHNOLOGY SYSTEMS S.p.A. ha tratto o avrebbe potuto trarre dal comportamento dell'Apicale e/o Subordinato un risultato positivo economico o di altra natura (sulla base di una valutazione *ex post* della condotta).

Infine corre l'obbligo di precisare che, per giurisprudenza consolidata, la responsabilità conseguente alle condotte illecite commesse da Apicali e/o Subordinati di altra società, appartenenti ad un gruppo, può essere estesa alla capogruppo e l'illecito commesso dalla controllata potrebbe essere addebitato alla controllante.

6. L'ESIMENTE

Il Decreto legislativo 8 giugno 2001, n. 231 prevede l'esclusione da responsabilità per la Società se, prima della commissione del Reato, la stessa abbia adottato ed efficacemente attuato un Modello di organizzazione, gestione e controllo effettivo, efficace ed idoneo a prevenire i reati della categoria cui appartiene il reato-presupposto verificatosi.

Il Decreto legislativo 8 giugno 2001 n. 231 prevede altresì che la Società non viene ritenuta responsabile qualora gli Apicali e/o i Subordinati abbiano agito nell'interesse esclusivo proprio o di terzi.

Ai fini dell'esimente da responsabilità, occorre specificare che qualora l'autore dell'illecito fosse un Soggetto Apicale e o Subordinato l'imputabilità del medesimo alla Società si ha per presunta salvo che quest'ultima non sia in grado di dimostrare:

- di avere adottato ed efficacemente attuato prima della commissione del fatto costituente Reato, un Modello di organizzazione, gestione e controllo idoneo a prevenire la commissione di illeciti come quello verificatosi;
- di aver istituito un Organismo di Vigilanza indipendente, autonomo e che assicuri continuità d'azione a cui sia affidato il compito di vigilare sul funzionamento, sull'osservanza del Modello e di curarne il suo aggiornamento;
- che il comportamento illecito sia stato commesso eludendo fraudolentemente il Modello di organizzazione, gestione e controllo in essere;
- che non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

In base alle disposizioni del Decreto legislativo 8 giugno 2001 n. 231 la Società ha un titolo autonomo di responsabilità e non solidale con l'autore del Reato. La responsabilità della Società si integra, come già sopra

anticipato, anche quando l'autore del Reato non sia stato identificato e/o il medesimo Reato subisca una vicenda estintiva.

7. I REATI PRESUPPOSTO E LE SANZIONI

La società può essere chiamata a rispondere per le fattispecie presupposto di cui al Decreto legislativo 8 giugno 2001 n. 231.

In Allegato A l'elenco dei reati applicabili.

I reati commessi all'estero

In forza dell'art. 4 del Decreto, l'ente può essere chiamato a rispondere in Italia anche di reati presupposto commessi all'estero.

Il Decreto, tuttavia, subordina questa possibilità alle seguenti condizioni:

- non procede lo Stato del luogo in cui è stato commesso il reato;
- l'ente ha la propria sede principale nel territorio dello Stato italiano;
- il reato è commesso all'estero da un soggetto apicale o subordinato dell'ente italiano;
- sussistono le condizioni generali di procedibilità previste dagli articoli 7, 8, 9, 10 del codice penale per poter perseguire in Italia un reato commesso all'estero

Il rinvio agli artt. 7-10 c.p. è da coordinare con le previsioni degli articoli da 24 a 25 quiquies decies del D.lgs. 231/2001, sicché - anche in ossequio al principio di legalità di cui all'art. 2 del D.lgs. 231/2001 - a fronte della serie di reati menzionati dagli artt. 7-10 c.p., la società potrà rispondere soltanto di quelli per i quali la sua responsabilità sia prevista da una disposizione legislativa ad hoc.

8. LA GOVERNANCE

C.R. TECHNOLOGY SYSTEMS S.p.A. è amministrata da un Consiglio di Amministrazione al quale spettano tutti i poteri di ordinaria e straordinaria amministrazione e che può, a sua volta, attribuire poteri e cariche a propri componenti.

La rappresentanza legale della società di fronte a terzi ed in giudizio innanzi a qualsiasi autorità amministrativa o giudiziaria spetta al Presidente del Consiglio di Amministrazione ed ai delegati del medesimo Consiglio disgiuntamente entro i limiti di materia e di potere assegnati.

Il Consiglio svolge un ruolo di indirizzo, coordinamento e controllo dell'attività di C.R. TECHNOLOGY SYSTEMS S.p.A..

9. IL SISTEMA DI CONTROLLO

Principi generali

Il Sistema di Controllo di C.R. TECHNOLOGY SYSTEMS S.p.A. è strutturato per assicurare una corretta informativa ed un adeguato monitoraggio delle sue attività. Con particolare attenzione alla struttura organizzativa, C.R. TECHNOLOGY SYSTEMS S.p.A. identifica compiti, funzioni e responsabilità del proprio personale.

Inoltre, nella distribuzione degli incarichi o attività aziendali opera sempre verificando che l'organizzazione interessata rispetti i seguenti principi:

i. Segregazione delle funzioni, ovvero, nessuno può gestire in autonomia un intero processo.

ii. Controllo, ovvero, ogni operazione, transazione, azione deve essere: verificabile, documentata, coerente e congrua.

iii. Documentazione dei controlli, ovvero, il controllo eseguito, anche se solo di supervisione, deve essere documentabile.

Le attività di Controllo

Le attività di Controllo di C.R. TECHNOLOGY SYSTEMS S.p.A. prevedono, di massima, che:

- sia chiaramente definito e divulgato l'organigramma societario ed anche quello ai fini della sicurezza;
- ogni operazione significativa sia preventivamente autorizzata da chi ha i poteri per farlo;
- siano individuate chiare responsabilità nell'esecuzione delle proprie attività caratteristiche;
- i poteri di rappresentanza, le procure e/o le deleghe siano conferite nel rispetto degli ambiti di esercizio e di limiti di importo strettamente collegati con le responsabilità assegnate;
- sia assicurata l'integrità e la completezza dei dati gestiti attraverso il necessario scambio di informazioni tra le strutture operative a cui sono assegnati compiti, fasi e processi tra loro connessi.

Le risorse finanziarie

Con particolare riferimento alle modalità di gestione delle risorse finanziarie, C.R. TECHNOLOGY SYSTEMS S.p.A. monitora costantemente (attraverso le funzioni interne ed esterne a ciò preposte) che il sistema concretamente posto mantenga nel tempo requisiti di idoneità tali da assicurare la loro gestione nel rispetto degli obblighi posti dalle leggi italiane, comunitarie ed internazionali; in particolare, salvo quanto sarà precisato nell'ambito di ciascuna delle specifiche Parti Speciali del Modello (come previste dal D.lgs. 8 giugno 2001 n. 231) con riguardo alle modalità di gestione delle risorse finanziarie, l'attività di monitoraggio svolta da C.R. TECHNOLOGY SYSTEMS S.p.A. è in generale rivolta a titolo esemplificativo e non esaustivo alla verifica:

- ✓ del rispetto dei limiti di materia attribuiti dalla legge agli organi sociali (Assemblea – Consiglio di Amministrazione);
- ✓ del rispetto dei limiti di potere attribuiti ai sensi di statuto al Presidente, all'Amministratore Delegato ed al Direttore Generale;
- ✓ della conformità alla legge degli atti posti da C.R. TECHNOLOGY SYSTEMS S.p.A. in materia di gestione delle risorse finanziarie;
- ✓ dell'adeguata assegnazione di poteri rispetto all'assetto organizzativo, ai ruoli, ai compiti ed alle responsabilità a ciascuno assegnate;
- ✓ della tracciabilità delle attività eseguite con le risorse finanziarie e della loro rintracciabilità;
- ✓ dell'effettività delle attività di controllo in materia finanziaria e della tracciabilità dei controlli eseguiti;
- ✓ delle tempistiche di pianificazione e predisposizione dei budget;

- ✓ dell'approvazione del budget;
- ✓ della operatività oltre i limiti di budget;
- ✓ della obbligatorietà di approvazione da parte del Consiglio di Amministrazione/o dell'Assemblea delle operazioni di carattere straordinario;
- ✓ del rispetto delle delibere di autorizzazione all'avvio delle operazioni straordinarie dell'Assemblea;
- ✓ dell'adeguata attribuzione e del rispetto dei limiti di poteri riconosciuti per operare sui c/c della Società e sulle risorse finanziarie, per la realizzazione di operazioni straordinarie e la realizzazione delle operazioni ammesse dall'oggetto sociale in materia finanziaria;
- ✓ dell'attribuzione di *specimen* di firma bancari per operare sui conti correnti della Società dopo l'autorizzazione da parte dell'organo di vertice ed avendo cura che negli stessi siano riportati i limiti di operatività definiti con delibera del Consiglio o con procura speciale o con delega;
- ✓ del rispetto del limite di doppia firma oltre definiti limiti di valore ed operazioni su risorse finanziarie anche straordinarie;
- ✓ del riporto periodico da parte degli organi delegati ai sensi dell'art. 2381 c.c. sullo *status* e sulle modalità di esercizio della delega attribuita anche in materia finanziaria e/o per operazioni straordinarie.

9.3. GLI ORGANI PREPOSTI AL CONTROLLO

Organo Amministrativo

All'Organo Amministrativo (*alias* Consiglio di Amministrazione) compete il potere di indirizzo, coordinamento e controllo sulla gestione societaria. All'Organo Amministrativo compete la responsabilità dell'intero Sistema di Controllo interno e l'esecuzione di adeguata vigilanza sull'operato degli organi delegati.

Collegio Sindacale

Al Collegio sindacale spetta ai sensi di legge e di Statuto il monitoraggio sull'adeguatezza dell'assetto organizzativo amministrativo, contabile e finanziario.

Revisore Contabile

Il Controllo Contabile è svolto dal Collegio Sindacale qualora, ai sensi di legge, la Società non abbia nominato un revisore esterno.

Datore di lavoro

In materia di tutela della salute e sicurezza sui luoghi di lavoro ed ambiente il Consiglio di Amministrazione ha individuato il Datore di Lavoro ai sensi dell'art. 2 comma 1 lett. b) di cui al D.lgs. 9 aprile 2008, n. 81.

Delegato di funzione ex art. 16 D.lgs. 9 aprile 2008 n. 81 (ove nominato)

Il Delegato di funzione, nell'ambito delle attribuzioni allo stesso riconosciute dal Datore di Lavoro e dallo stesso accettate, è l'*alter ego* del Datore di Lavoro e spetta allo stesso un ruolo di garanzia del rispetto della corretta attuazione degli obblighi di cui al D.lgs. 9 aprile 2008, n. 81 entro le competenze e materie assegnate.

Responsabile qualità

Il Responsabile qualità è responsabile del supporto nella progettazione, implementazione, monitoraggio e miglioramento del sistema di gestione della qualità dei flussi e dei processi di produzione di C.R. TECHNOLOGY SYSTEMS S.p.A..

Responsabile del sistema gestionale in materia di salute sicurezza ambiente

Il Responsabile del sistema gestionale in materia di salute sicurezza ambiente è responsabile del supporto nelle fasi di progettazione, implementazione, monitoraggio e miglioramento del sistema di gestione della materia salute e sicurezza in C.R. TECHNOLOGY SYSTEMS S.p.A..

Titolare e Incaricato ai fini del trattamento delle informazioni e dati *(decreto privacy come modificato dal Regolamento Europeo - GDPR)*

Il Titolare e l'Incaricato ai fini del trattamento delle informazioni e dei dati gestiscono in nome e per conto di C.R. TECHNOLOGY SYSTEMS S.p.A. gli adempimenti previsti dalla specifica normativa di riferimento.

Responsabili tecnici e di funzione

I Responsabili tecnici e di funzione o d'area di C.R. TECHNOLOGY SYSTEMS S.p.A., nell'ambito delle competenze loro assegnate, sono responsabili delle attività da loro condotte nell'interesse o vantaggio della società e delle attività svolte dai propri Dipendenti.

Dipendenti (operai ed impiegati)

I Dipendenti di C.R. TECHNOLOGY SYSTEMS S.p.A. sono responsabili del corretto assolvimento delle attività assegnate e del riporto dell'esito delle stesse al proprio Responsabile.

Organismo di Vigilanza

L'Organismo di vigilanza nominato con delibera del Consiglio di Amministrazione ha il compito di vigilare sul funzionamento, sull'osservanza del Modello e di curarne il suo aggiornamento.

10. IL SISTEMA DELLE DELEGHE

10.1. Premessa

L'attribuzione dei poteri ad operare è ispirata ai seguenti criteri di massima:

- "esattezza" della materia delegata e delle limitazioni dei poteri;
- "pubblicità" interna ed esterna dei poteri attribuiti e delle relative responsabilità;
- "coerenza" dei poteri di rappresentanza attribuiti con le competenze assegnate;
- "certezza" nell'esecuzione del potere di rappresentanza e/o di firma attribuito.

10.2. Deleghe e Procure

Requisiti essenziali di attribuzione

Il rilascio di mandati, deleghe e procure per operare quali rappresentanti negli interessi e a vantaggio di C.R. TECHNOLOGY SYSTEMS S.p.A., rispetta i seguenti principi:

- tutti coloro che intrattengono per conto di C.R. TECHNOLOGY SYSTEMS S.p.A. rapporti con la Pubblica Amministrazione devono essere espressamente autorizzati;
- ciascuna delega e/o procura definisce in modo specifico ed inequivocabile i poteri attribuiti ed i limiti entro cui operare;
- al delegato e/o procuratore sono riconosciuti poteri di spesa adeguati alle funzioni conferite;
- le deleghe e le procure sono rese pubbliche.

Conferimento e revoca delle deleghe e procure

Il conferimento delle deleghe e delle procure deve avvenire nel rispetto dei limiti posti dalla legge, nonché dalle previsioni dello Statuto, con le modalità gestionali poste dall'organo di vertice.

Il Consiglio di Amministrazione verifica periodicamente, anche con il supporto delle competenti funzioni aziendali, il rispetto del Sistema delle deleghe e procure in vigore e la sua coerenza con l'assetto organizzativo.

11. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Adozione del Modello

L'adozione del presente documento è di competenza esclusiva dell'Organo Amministrativo.

Il presente Modello è stato elaborato da C.R. TECHNOLOGY SYSTEMS S.p.A. tenendo conto della struttura dell'attività concretamente svolta, della natura e delle dimensioni della sua organizzazione.

C.R. TECHNOLOGY SYSTEMS S.p.A. ha proceduto con l'avvio di un'analisi preliminare del contesto aziendale. In particolar modo sono stati analizzati: la storia di C.R. TECHNOLOGY SYSTEMS S.p.A., il contesto societario, il mercato di appartenenza, l'organigramma aziendale, il sistema di governance, il sistema di controllo, il sistema delle deleghe, le procedure già formalizzate all'interno di C.R. TECHNOLOGY SYSTEMS S.p.A. per lo svolgimento dell'attività sociale. Sono state, quindi, svolte:

- interviste individuali con l'amministratore ed i responsabili delle aree;
- una analisi degli organigrammi aziendali e del sistema di ripartizione delle responsabilità e dei poteri;
- una analisi di tenuta delle procedure e/o controlli posti in essere;
- una analisi del Sistema di Controllo vigente.

Obiettivi perseguiti

C.R. TECHNOLOGY SYSTEMS S.p.A. assicura condizioni di correttezza e trasparenza nella conduzione del proprio business. A tal fine ha colto l'opportunità fornitagli dal D.Lgs. 8 giugno 2001 n. 231 ed ha avviato un progetto di analisi dei propri strumenti organizzativi e di gestione del controllo al fine di verificare la rispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto.

In tal senso l'adozione del Modello costituisce un valido strumento di sensibilizzazione di tutti coloro che operano in nome e per conto di C.R. TECHNOLOGY SYSTEMS S.p.A., oltre che uno stimolo a tenere comportamenti corretti.

In particolare C.R. TECHNOLOGY SYSTEMS S.p.A., con l'adozione del Modello, si pone i seguenti principali obiettivi:

- determinare, in tutti coloro che operano nell'interesse o a vantaggio della stessa, la consapevolezza di poter incorrere, in caso di violazioni (delle disposizioni di legge comprese quelle riportate nel D.lgs. 231/2001 e quelle presenti nella parte speciale del Modello), in sanzioni penali comminabili nei loro confronti e in sanzioni amministrative addebitabili all'azienda;
- ribadire che il comportamento illecito è fortemente condannato da C.R. TECHNOLOGY SYSTEMS S.p.A., in quanto contrario, oltre che alle disposizioni di legge, anche ai principi del Codice Etico ed ai valori ai quali C.R. TECHNOLOGY SYSTEMS S.p.A. intende attenersi nell'esercizio dell'attività aziendale;
- un'azione di monitoraggio sulle aree di attività a rischio al fine di intervenire tempestivamente per prevenire e contrastare la commissione di condotte illecite che possano integrare le fattispecie presupposto di cui al Decreto;
- fornire un'adeguata informazione ai Destinatari circa l'adozione del Modello;
- continuare a diffondere una cultura di impresa basata sul controllo preventivo e sulla legalità;
- condannare ogni comportamento non conforme alla legge o alle disposizioni interne e, in particolare, alle istruzioni contenute nel presente Modello ed al Codice Etico di C.R. TECHNOLOGY SYSTEMS S.p.A.;
- creare e mantenere un'efficace ed efficiente organizzazione dell'impresa, mediante processi che pongano l'attenzione sui ruoli, sulla formazione delle decisioni e sulla gestione dell'informazione interna ed esterna;
- attuare tutte le misure necessarie per eliminare, nel più breve tempo possibile, eventuali situazioni di rischio di commissione di condotte illecite integranti i Reati presupposto di cui al D.lgs. 231 del 2001.

Valore del Modello e del Codice Etico

Il presente documento costituisce regolamento interno di C.R. TECHNOLOGY SYSTEMS S.p.A., vincolante per la medesima e per tutti i suoi Destinatari. In particolare il Codice Etico è l'espressione dei valori etico – morali di C.R. TECHNOLOGY SYSTEMS S.p.A.

Il rispetto del Modello presuppone il rispetto anche di quanto previsto nel Codice Etico che costituisce parte integrante e sostanziale dello stesso.

Modifiche ed aggiornamento del Modello

Modifiche, integrazioni ed aggiornamenti del Modello sono di competenza dell'Organo Amministrativo, che può intervenire anche su proposta dell'Organismo di Vigilanza. A titolo esemplificativo e non esaustivo, l'aggiornamento del Modello deve essere avviato quando:

- siano sopravvenute violazioni o elusioni delle prescrizioni in esso contenute che ne abbiano dimostrato la inefficacia e/o l'incoerenza ai fini della prevenzione dei Reati presupposto;
- siano sopravvenuti cambiamenti significativi nel quadro normativo, nell'organizzazione o nell'attività di C.R. TECHNOLOGY SYSTEMS S.p.A. che comportino l'avvio di analisi specifiche e la elaborazione di parti speciale e protocolli specifici;
- in tutti gli altri casi in cui si renda necessaria o utile la modifica, l'integrazione e/o l'aggiornamento del Modello.

Il Presidente del Consiglio di Amministrazione potrà apportare al Modello modifiche, integrazioni e o aggiornamenti di natura ordinaria e di mero adeguamento formale alla legge. In tali circostanze il Presidente dovrà fornire resoconto al Consiglio di Amministrazione dell'attività svolta.

L'Organismo di Vigilanza andrà costantemente informato sulle modifiche, integrazioni ed aggiornamenti apportate al Modello, ai protocolli, alle procedure ed ai controlli esistenti in C.R. TECHNOLOGY SYSTEMS S.p.A.

12. L'ORGANISMO DI VIGILANZA ED IL FLUSSO DI INFORMAZIONI

Il rispetto dei requisiti previsti dal D.lgs. 8 giugno 2001, n. 231 costituisce elemento essenziale anche ai fini della nomina dell'Organismo di Vigilanza.

In ragione di ciò è necessario che detto organo di controllo abbia la possibilità di esercitare i poteri e la propria funzione in modo concreto e l'organo amministrativo lo ponga nella condizione di poterli assolvere correttamente. Quanto detto costituisce il presupposto indispensabile per l'effettività dell'azione di controllo demandata all'Organismo di Vigilanza e quindi presupposto iniziale per il relativo esonero da responsabilità dell'ente.

Per una corretta configurazione dell'Organismo di Vigilanza è necessario valutare attentamente, in ragione dei compiti e delle funzioni che quest'ultimo sarà chiamato ad assolvere, il possesso dei requisiti di indipendenza, autonomia e continuità di azione che la legge richiede a ciascun membro ed all'intero Organismo di Vigilanza.

Compiti e Funzione

L'Organismo di Vigilanza ha il compito di vigilare costantemente:

- sul funzionamento del Modello;
- sull'osservanza del Modello, e
- di curarne il suo aggiornamento.

Il Regolamento dell'Organismo di Vigilanza

L'Organismo di Vigilanza alla sua prima seduta dovrà dotarsi di un proprio Regolamento di funzionamento, nel quale tra l'altro dovrà dare evidenza delle modalità di pianificazione delle attività di controllo assegnate, oltre a proporre annualmente all'Organo Amministrativo l'approvazione del proprio budget.

Composizione dell'Organismo di Vigilanza

Tenuto conto delle proprie dimensioni, dell'attività caratteristica di C.R. TECHNOLOGY SYSTEMS S.p.A. e del suo fatturato, la Società, al fine di garantire una maggiore effettività dei controlli demandati dalla legge, ha optato

per la composizione plurisoggettiva dell'Organismo di Vigilanza. L'Organo Amministrativo procederà a definire il numero dei componenti dell'Organismo di Vigilanza in fase di nomina.

Possono essere chiamati a far parte dell'Organismo di Vigilanza componenti esterni a C.R. TECHNOLOGY SYSTEMS S.p.A., purché ciascuno sia in possesso dei seguenti requisiti:

- **Autonomia e indipendenza:** dovrà essere tale da garantire l'autonomia dei membri da ogni forma d'interferenza e di condizionamento da parte di qualunque componente di C.R. TECHNOLOGY SYSTEMS S.p.A. ed in particolare dei vertici operativi e/o organi dirigenziali, soprattutto considerando che la funzione esercitata si esprime anche nella vigilanza dell'attività degli organi Apicali, tra cui rientrano i componenti dell'Organo Amministrativo.

Per tale motivazione, l'Organismo di Vigilanza deve essere inserito nell'organigramma di C.R. TECHNOLOGY SYSTEMS S.p.A. in una posizione gerarchica che sia la più elevata possibile, rispondendo, nello svolgimento della sua funzione, soltanto all'Organo Amministrativo.

L'Organismo di Vigilanza deve poter disporre di specifiche risorse aziendali e potersi avvalere della collaborazione di tutto il personale e funzioni/aree di C.R. TECHNOLOGY SYSTEMS S.p.A..

A tal fine l'Organo Amministrativo metterà a disposizione dell'Organismo di Vigilanza risorse aziendali specificatamente dedicate, di numero e valore proporzionato ai compiti affidati, approvando annualmente il budget dallo stesso proposto, quale dotazione adeguata di risorse finanziarie.

L'Organismo di Vigilanza, potrà disporre delle predette risorse per ogni esigenza necessaria al corretto svolgimento dei propri compiti avvalendosi, ove necessario, anche di consulenze specialistiche, sostenendo trasferte, etc.

L'Organo Amministrativo nella composizione dell'Organismo di Vigilanza (nel caso di specie in forma plurisoggettiva) dovrà tenere in evidenza dei seguenti criteri di cui alle Linee guida Confindustria:

1. nel caso di composizione con soli componenti esterni, i requisiti di autonomia e di indipendenza dovranno essere riferiti ai singoli componenti;

2. nel caso di composizione mista dell'Organismo, non essendo esigibile dai componenti di provenienza interna una totale indipendenza dall'ente, il grado di indipendenza dell'Organismo dovrà essere valutato nella sua globalità.

- **Professionalità:** l'Organismo di Vigilanza deve inoltre possedere, al suo interno, competenze tecnico - professionali adeguate ai compiti ed alle funzioni che è chiamato a svolgere.

Pertanto, è necessario che siano presenti soggetti con professionalità in materia economica, legale, di analisi dei processi, di controllo e gestione dei rischi aziendali, di esecuzione di indagini, di controlli e verifiche.

In particolare, l'Organismo di Vigilanza deve possedere le capacità tecniche specialistiche necessarie al fine di svolgere attività ispettiva.

L'Assemblea dei soci, una volta individuati i componenti dell'Organismo di Vigilanza, all'atto della nomina, è tenuto a verificare la sussistenza delle condizioni richieste dal Modello, basandosi sui *profili professionali*, sulle

concrete esperienze fatte sul campo, acquisendo, se utile, le necessarie referenze anche da parte di terzi e le dichiarazioni raccolte direttamente dai candidati.

Considerata l'eterogeneità degli aspetti tecnici che regolano l'operato di C.R. TECHNOLOGY SYSTEMS S.p.A., l'Organismo di Vigilanza, al fine di implementare le professionalità utili o necessarie per il corretto espletamento delle proprie attività e garantire la propria professionalità (oltre che la sua autonomia), può utilizzare lo specifico *budget* di spesa messo a disposizione dall'Organo Amministrativo, allo scopo di acquisire all'esterno dell'ente, quando necessario, le competenze per integrare le proprie.

L'Organismo di Vigilanza può, così, anche avvalendosi di professionisti esterni, dotarsi, a titolo esemplificativo e non esaustivo, di risorse competenti in materia giuridica, di organizzazione aziendale, revisione, contabilità, finanza, sicurezza sui luoghi di lavoro, ambientale, etc.

- **Continuità d'azione:** l'Organismo di Vigilanza è tenuto a svolgere in modo continuativo le attività necessarie per la vigilanza sull'applicazione del Modello con adeguato impegno e con i necessari poteri di indagine.

La continuità di azione non deve essere intesa come *"incessante operatività"*, dal momento che tale interpretazione imporrebbe necessariamente un Organismo di Vigilanza esclusivamente interno all'ente.

La continuità di azione comporta che l'attività dell'Organismo di Vigilanza non debba limitarsi ad incontri periodici dei propri membri, ma essere organizzata in base ad un piano di azione ed alla conduzione costante di attività di monitoraggio e di analisi del sistema di prevenzione dell'ente.

E', inoltre, importante ricordare quanto riportato sul punto a pag. 60 delle linee guida di Confindustria - edizione 2014 - nella parte in cui, riprendendo la sentenza del Tribunale di Roma del 4 aprile 2003, si precisa che *"(...) per garantire l'efficace e costante attuazione di un modello così articolato quale é quello delineato dal decreto 231, soprattutto nelle aziende di grandi e medie dimensioni, si rende necessaria la presenza di una struttura dedicata a tempo pieno all'attività di vigilanza sul Modello* (l'Organismo di Vigilanza), *priva di mansioni operative che possano portarla ad assumere decisioni con effetti economico - finanziari*.".

Proseguendo sul punto le linee guida di Confindustria - edizione 2014 - affermano che *"(...) ciò non esclude, peraltro, che (...)* l'Odv *possa fornire anche pareri sulla costruzione del Modello, affinché questo non risulti debole o lacunoso sin dalla sua elaborazione: in tal senso eventuali* ***consulenze****, infatti,* ***non intaccano l'indipendenza e l'obiettività di giudizio su specifici eventi*** *...".*

- **Durata della carica**

L'Organismo di Vigilanza rimane in carica per un massimo di un triennio dalla data della sua nomina; i medesimi componenti dell'Organismo di Vigilanza possono essere rieletti.

Requisiti di eleggibilità

L'Organo Amministrativo all'atto della nomina deve verificare che ciascun componente dell'Organismo di Vigilanza sia dotato di professionalità, onorabilità, indipendenza, autonomia e possa assicurare continuità di azione come sopra inteso e disponga delle competenze necessarie per lo svolgimento dei compiti affidatigli dal Decreto.

A tutti i membri dell'Organismo di Vigilanza è richiesto preventivamente di non trovarsi in alcuna delle condizioni di ineleggibilità e/o incompatibilità e di conflitto di interessi di seguito riportate.

(a) essere stati sottoposti a misure di prevenzione disposte dall'autorità giudiziaria ai sensi della legge 27 dicembre 1956 n. 1423 (*legge sulle misure di prevenzione nei confronti delle persone pericolose per la sicurezza e per la pubblica moralità*) o della legge 31 maggio 1965 n. 575 (*disposizioni contro la mafia*) e loro successive modifiche ed integrazioni;

(b) essere indagati o essere stati condannati, anche con sentenza non ancora definitiva o emessa ex artt. 444 e ss. c.p.p. (patteggiamento) o con pena condizionalmente sospesa, salvi gli effetti della riabilitazione;

(c) essere interdetto, inabilitato, fallito o essere stato condannato, anche con sentenza non definitiva, ad una pena che comporti l'interdizione, anche temporanea, da uffici pubblici o l'incapacità ad esercitare uffici direttivi.

Il verificarsi anche di una sola delle suddette condizioni comporterà l'ineleggibilità alla carica di membro dell'Organismo di Vigilanza e se eletto consentirà all'organo amministrativo di revocare il componente per giusta causa; in tale evenienza l'organo amministrativo provvederà alla sostituzione del componente revocato.

Revoca, sostituzione, decadenza e recesso

Fermo quanto previsto al punto precedente, la revoca dall'incarico di membro dell'Organismo di Vigilanza può essere disposta solo in presenza di giusta causa.

A titolo esemplificativo e non esaustivo sono condizioni legittimanti la revoca per giusta causa:

- la perdita dei requisiti di eleggibilità;
- l'inadempimento agli obblighi inerenti all'incarico affidato;
- il mancato rispetto dei principi del Codice Etico, dei protocolli di buon comportamento generale e speciale di ciascuna parte speciale adottata.

In presenza di giusta causa, il Consiglio revoca la nomina del membro dell'Organismo di Vigilanza non più idoneo e provvede alla sua immediata sostituzione, riconoscendo al componente l'emolumento fino alla data di permanenza nella carica.

Costituisce causa di decadenza dall'incarico, prima della scadenza del termine previsto nel presente Modello, la sopravvenuta incapacità o impossibilità ad esercitare l'incarico.

Ciascun componente dell'Organismo di Vigilanza può recedere in qualsiasi istante dall'incarico, previo preavviso di un mese, con comunicazione scritta e motivata al Consiglio di Amministrazione.

In caso di decadenza o recesso in capo ad uno dei componenti dell'Organismo di Vigilanza, l'Organo Amministrativo provvede tempestivamente alla sostituzione del componente divenuto inidoneo.

Attività e poteri

L'Organismo di Vigilanza nella sua prima seduta procede a dotarsi di un proprio regolamento e a nominare il suo Presidente. Per l'espletamento dei compiti assegnati l'Organismo di Vigilanza è investito dei compiti e delle funzioni di cui al presente Modello e di tutti i poteri di iniziativa e controllo su ogni attività aziendale. Il detto organo societario ha un esclusivo vincolo di dipendenza dall'Assemblea, cui riferisce tramite il proprio Presidente.

I compiti e le attribuzioni dell'Organismo di Vigilanza e dei suoi membri non possono essere sindacati da alcun altro organismo o struttura aziendale, fermo restando che il Consiglio di Amministrazione può verificare la coerenza delle attività svolte dall'Organismo di Vigilanza con le funzioni allo stesso demandate.

L'Organismo di Vigilanza svolge le sue funzioni coordinandosi con tutti gli altri organi o funzioni di controllo esistenti.

In particolare si coordina con:

- il Responsabile dell'area amministrazione finanza e contabilità;
- il Responsabile dell'area l'ufficio personale anche per ciò che concerne gli aspetti relativi all'informazione ed alla formazione del personale attinente alle tematiche inerenti al Decreto;
- il Datore di Lavoro ex art. 2 D.lgs. 9 aprile 2008, n. 81;
- il Delegato di funzione ex art. 16 D.lgs. 9 aprile 2008, n. 81 - ove nominato;
- il RSPP ex art. 2 D.lgs. 9 aprile 2008, n. 81;
- il Responsabile qualità;
- il Responsabile del sistema gestionale in materia di salute e sicurezza;
- il Responsabile del sistema gestionale ambientale;
- il Titolare, il Responsabile del trattamento dei dati personali e il Responsabile della gestione dei dati personali (questi ultimi ove nominati);
- i Direttori Tecnici e i Responsabili d'area o funzione di C.R. TECHNOLOGY SYSTEMS S.p.A.;
- i Dipendenti, considerando tali tutto il personale dipendente da C.R. TECHNOLOGY SYSTEMS S.p.A. compresi gli operai e gli impiegati;
- le funzioni che svolgono attività a rischio per tutti gli aspetti relativi al controllo delle procedure operative in essere;
- la funzioni con cui l'Organismo di Vigilanza ritiene utile, necessario e/o indispensabile confrontarsi.

L'Organismo di Vigilanza, nell'ambito dei suoi compiti, a titolo esemplificativo e non esaustivo può:

- svolgere o provvedere a far svolgere, sotto la sua diretta sorveglianza e responsabilità, attività ispettive periodiche;
- accedere a tutte le informazioni riguardanti le attività sensibili di C.R. TECHNOLOGY SYSTEMS S.p.A.;
- chiedere informazioni o esibizione di documenti in merito alle attività sensibili a tutto il personale dipendente di C.R. TECHNOLOGY SYSTEMS S.p.A. e, laddove necessario, all'Amministratore Unico, all'organo preposto alla revisione contabile (anche nell'ipotesi in cui venga nominata società di revisione), ai soggetti incaricati in ottemperanza a quanto previsto dalla normativa in materia antinfortunistica, ambientale ed a quelli ai fini del trattamento dei dati personali ed in generale a tutti gli interessati alle attività di C.R. TECHNOLOGY SYSTEMS S.p.A.;
- avvalersi di consulenti esterni per problematiche che ne richiedano l'ausilio;
- segnalare l'avvio di provvedimenti disciplinari e l'adozione di sanzioni disciplinari;

- verificare l'adeguatezza della pianificazione dei programmi di specifica formazione del personale;
- indirizzare, almeno con cadenza annuale, una relazione scritta all'Organo Amministrativo;
- informare immediatamente gli interessati e l'Amministratore Delegato e o il Direttore Generale sulle attività svolte;
- ricevere informazioni e comunicazioni da chiunque gli giungano;
- eseguire indagini sui fatti da chiunque comunicati;
- eseguire periodici Audit sulle attività individuate come a rischio.

Remunerazione e rimborsi spese

La remunerazione spettante ai componenti dell'Organismo di Vigilanza (ivi incluso il Presidente o quelli investiti di particolari cariche) è stabilita all'atto della nomina o con successiva decisione dell'Organo Amministrativo.

Ai componenti dell'Organismo di Vigilanza, spetta, inoltre, il rimborso delle spese sostenute per ragioni di ufficio e l'inserimento dei suoi componenti tra quelli per i quali è stata stipulata una copertura assicurativa D&O.

Obblighi di informazione nei confronti dell'Organismo di Vigilanza - Flussi informativi

Ai sensi del D.lgs. 8 giugno 2001 n. 231, il Modello prevede modalità di gestione dei flussi di informazione verso l'Organismo di Vigilanza (a seguire per brevità anche "Odv").

L'Organismo di Vigilanza basa il corretto ed efficiente espletamento delle sue funzioni sulla possibilità di disporre di tutti i dati e le informazioni relative alle aree di rischio individuate e allo stesso necessarie. Per tale motivo deve essere consentito dalla Società l'accesso dell'Odv a tali dati ed informazioni.

L'obbligo di dare informazioni all'OdV è rivolto a tutte le funzioni aziendali e può avere riguardo alle risultanze periodiche dell'attività di controllo dalle stesse poste in essere al fine di dare attuazione alle procedure ed ai controlli esistenti (ad es. report riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi, ecc.) ed alle anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili.

Oltre quanto previsto dai flussi informativi riportati nelle singole parti speciali, a titolo esemplificativo e non esaustivo, le informazioni alle quali deve avere accesso l'OdV possono riguardare:

- le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
- le motivazioni che hanno giustificato l'assistenza legale richiesta da dirigenti e o da dipendenti per atti sui quali l'Autorità Giudiziaria sta procedendo;
- i provvedimenti e/o notizie provenienti dagli organi di polizia giudiziaria o da altra autorità e dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, non solamente per i Reati presupposto di cui al D.lgs. 8 giugno 2001 n. 231;
- le indagini e/o relazioni interne dalle quali emergano responsabilità anche per le ipotesi di Reato presupposto di cui al D.lgs. 8 giugno 2001 n. 231;
- le notizie relative all'effettiva attuazione del Modello, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;

- i prospetti riepilogativi degli appalti affidati a terzi per l'esecuzione di attività all'interno ed all'esterno del sito della società;
- i prospetti riepilogativi delle gare ad evidenza pubblica alla quale C.R. TECHNOLOGY SYSTEMS S.p.A. prende o prenderà parte o alle quali sta partecipando;
- i prospetti riepilogativi dei contratti conclusi/stipulati con enti sia privati che pubblici con qualsiasi forma;
- le notizie relative a commesse attribuite da enti pubblici o soggetti che svolgano funzioni di pubblica utilità;
- le copie della reportistica periodica in materia di salute e sicurezza sul lavoro ed ambiente, tra cui Duvri, DVR, PSC, POS, atti di nomina per le funzioni di cantiere, etc;
- il report dei controlli eseguiti dal *management* aziendale sulle attività eseguite dai propri subordinati.

L'Organismo di vigilanza dovrebbe altresì ricevere copia della reportistica periodica in materia di salute, sicurezza sul lavoro, ambiente e qualità.

Va chiarito che le informazioni fornite all'Organismo di vigilanza mirano a consentire allo stesso il miglioramento delle proprie attività di pianificazione dei controlli e non ad imporgli attività di verifica puntuale e sistematica di tutti i fenomeni rappresentati[1].

Relativamente al presente obbligo di comunicazione verso l'Organismo di Vigilanza è utile sottolineare che l'obbligo di informare il datore di lavoro sui comportamenti contrari al Modello rientra nel più ampio dovere di diligenza ed obbligo di fedeltà del prestatore di lavoro ai sensi degli artt. 2104 e 2105 c.c. che prevedono che questi:

- deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale;
- deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di quest'ultimo dai quali gerarchicamente dipende;
- non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa o farne uso in modo da poter recare ad essa pregiudizio.

[1] cfr. pag. 69 Linee guida di Confindustria edizione 2014 - *"...Con particolare riferimento ai flussi informativi periodici provenienti dal management, se prevedono l'obbligo di comunicare gli esiti di controlli già effettuati e non la trasmissione di informazioni o documenti da controllare, tali flussi periodici fanno chiarezza sui diversi ruoli in materia di prevenzione. Infatti, se ben definiti, i flussi informativi precisano che il management deve esercitare l'azione di controllo, mentre l'Odv - quale meccanismo di assurance - deve valutare i controlli effettuati dal management. Peraltro, l'obbligo di riferire gli esiti dei controlli all'Odv, produce un effetto di responsabilizzazione del management operativo. L'Organismo di vigilanza dovrebbe altresì ricevere copia della reportistica periodica in materia di salute e sicurezza sul lavoro. Va chiarito che le informazioni fornite all'Organismo di vigilanza mirano a consentirgli di migliorare le proprie attività di pianificazione dei controlli e non, invece, ad imporgli attività di verifica puntuale e sistematica di tutti i fenomeni rappresentati. In altre parole, all'Odv non incombe un obbligo di agire ogni qualvolta vi sia una segnalazione, essendo rimesso alla sua discrezionalità (e responsabilità) di stabilire in quali casi attivarsi. È il caso di aggiungere che l'obbligo di informazione è stato probabilmente previsto anche allo scopo di conferire maggiore autorevolezza alle richieste di documentazione che si rendono necessarie all'Organismo di vigilanza nel corso delle sue verifiche. ..."*

Flussi informativi verso l'Organismo di Vigilanza - Whistleblowing[2]

Allo scopo di consentire a tutti i Destinatari del Modello di poter comunicare con l'Odv, C.R. TECHNOLOGY SYSTEMS S.p.A. ha messo a disposizione i seguenti strumenti e mezzi di posta interna ed esterna riservata, nonché casella di posta elettronica dedicata.

Posta interna: la comunicazione, al fine di garantire la massima riservatezza, dovrà pervenire alla area amministrazione, indirizzata *all'Organismo di Vigilanza di C.R. TECHNOLOGY SYSTEMS S.p.A.* con la seguente dicitura sull'esterno della busta chiusa: "C*omunicazione per l'Organismo di Vigilanza. Informativa strettamente confidenziale"*

Posta esterna ordinaria: La comunicazione, al fine di garantire la massima riservatezza, dovrà essere indirizzata *all'Organismo di Vigilanza di C.R. TECHNOLOGY SYSTEMS S.p.A., con sede in Treviglio (BG) via Rossano n. 9*, con la seguente dicitura sull'esterno della busta: "C*omunicazione per l'Organismo di Vigilanza. Informativa strettamente confidenziale".*

Casella di posta elettronica: odv231crtechnologysystems@gmail.com

In tutti i casi sopra indicati la corrispondenza non deve essere aperta e consegnata direttamente al Presidente dell'Odv.

Si precisa che le segnalazioni che perverranno attraverso i predetti canali non dovranno avere un fine meramente delatorio (ovvero di denuncia anonima, fatta essenzialmente per tutelare i propri interessi ma talvolta anche per i più svariati motivi infamanti, di dispetto, di vendetta etc.) e dovranno:

- riportare esplicita indicazione identificativa del segnalante e del suo recapito e se dipendente, del reparto di appartenenza;
- indicare chiaramente:
  - ✓ l'evento e/o il fatto accaduto;
  - ✓ gli estremi (nome e cognome) delle persone coinvolte se conosciute;
  - ✓ i tempi e le modalità di esecuzione dell'evento segnalato;
  - ✓ quanto altro possa essere utile alla descrizione dell'evento e dei suoi autori.

Per le comunicazioni all'Odv potrà essere anche utilizzato il format in ***Allegato n. 2*** alla presente Parte Generale.

C.R. TECHNOLOGY SYSTEMS S.p.A. e l'Odv per quanto di rispettiva competenza si impegnano ad adottare tutte le misure idonee affinché le segnalazioni destinate all'Odv siano garantite da riservatezza (tra cui il predetto canale preferenziale di comunicazione/segnalazione costituisce un primo ed essenziale elemento), impegnandosi a trattare i dati e le informazioni comuni e sensibili contenuti nelle predette segnalazioni ai sensi del Decreto *privacy*, del GDPR e loro successive modifiche ed integrazioni.

[2] Legge 30 novembre 2017, n. 179 Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato - D.lgs. 8 giugno 2001 n. 231 - art. 6 comma 2 - disposizioni in tema di *whistleblowing*

I segnalanti in buona fede saranno garantiti da qualsiasi forma di ritorsione, discriminazione o penalizzazione anche ai sensi della Legge 30 novembre 2017, n. 179[3] e sarà loro assicurata la riservatezza dell'identità, fatti salvi gli obblighi di legge e la tutela dei diritti di C.R. TECHNOLOGY SYSTEMS S.p.A. o delle persone accusate erroneamente o in mala fede.

I comportamenti delatori e quelli destinati a rallentare l'attività dell'Odv saranno comunicati al responsabile del procedimento disciplinare per le valutazioni del caso.

Le segnalazioni sopra indicate dovranno essere messe a disposizione dell'Organismo di Vigilanza che attiverà un processo di accertamento della verità e della fondatezza delle segnalazioni ricevute.

Flussi informativi verso il vertice aziendale

L'Odv riferirà *esclusivamente* al Consiglio di Amministrazione in merito allo stato di attuazione del Modello, alle eventuali criticità, all'esigenza di eventuali aggiornamenti e adeguamenti del Modello, all'esito dell'attività eseguita e alla segnalazione delle violazioni accertate.

L'Odv predispone una relazione con periodicità almeno annuale che illustri di massima:

- l'attività ed i controlli svolti durante l'anno;
- le eventuali discrepanze tra le procedure operative e le disposizioni del Modello;
- i nuovi ambiti di commissione dei reati presupposto previsti dal Decreto;
- la verifica effettuata a seguito delle segnalazioni ricevute su violazioni del Modello e, nel rispetto della riservatezza richiesta dalla legge, i risultati delle verifiche riguardanti le suddette segnalazioni;
- gli eventuali interventi da porre in essere conseguenti alle modifiche del quadro normativo di riferimento, alle non conformità rilevate o segnalate, alle modifiche dell'attività sociale o del livello di rischio rilevato dalla società;
- un rendiconto delle spese sostenute rispetto al budget.

Fermo restando i termini di cui sopra, il Consiglio di Amministrazione ha la facoltà di convocare in qualsiasi momento l'Organismo di Vigilanza il quale, a sua volta, ha la facoltà di richiedere la convocazione dei predetti organi quando, per le necessità riconducibili alle attività del suo ufficio, lo ritenga opportuno.

Raccolta e conservazione delle informazioni

Ogni informazione, segnalazione, report, relazione prevista nel Modello, sarà custodita dalla segreteria dell'Odv in un apposito archivio (informatico e/o cartaceo) per il periodo necessario al completamento dell'attività e per il periodo previsto dalla legge.

13. SISTEMA SANZIONATORIO

[3] Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato - D.lgs. 8 giugno 2001 n. 231 - art. 6 comma 2 - disposizioni in tema di *whistleblowing.*

Le violazioni al Modello ed al Codice Etico da chiunque commesse devono essere comunicate all'Organismo di Vigilanza, ferme restando tutte le prerogative ed i provvedimenti di competenza del titolare del potere disciplinare. Il dovere di segnalare le violazioni del Modello grava su tutti i Destinatari dello stesso.

L'Odv, ricevuta la segnalazione, deve procedere, nel rispetto della riservatezza, alla comunicazione dell'esito degli accertamenti svolti all'Assemblea. Le eventuali sanzioni saranno erogate dagli organi di C.R. TECHNOLOGY SYSTEMS S.p.A. competenti in virtù dei poteri a loro conferiti dalla legge.

A titolo meramente esemplificativo e non esaustivo, tra le condotte che possono costituire infrazioni disciplinari si segnalano i seguenti comportamenti:

- mancato rispetto, con omissioni o in concorso con altri, del Codice Etico, dei protocolli, delle procedure e del Modello;
- la distruzione, la modifica, l'occultamento, la sottrazione della documentazione necessaria al controllo interno previsto dal Modello;
- la redazione di documentazione non veritiera, anche con l'aiuto di terzi;
- atti diretti ad impedire l'attività di vigilanza degli organi societari e dell'Odv;
- il diniego di accesso alla documentazione ed alle informazioni necessarie ai fini del controllo;
- qualsiasi altra condotta possa configurare la violazione del Modello, del Codice Etico, dei protocolli, delle procedure previste dal sistema di controllo, etc.;
- il sottrarsi senza giustificato motivo alla formazione;
- l'omissione delle azioni volte alla diffusione del sistema di controllo preventivo.

Sanzioni e misure disciplinari

Il Modello, conformemente a quanto previsto dallo statuto dei lavoratori e dal CCNL di categoria, costituisce un insieme di regole comportamentali alle quali il personale deve assolutamente uniformarsi. Ogni sua violazione comporta l'avvio del relativo procedimento disciplinare e l'irrogazione delle relative sanzioni. Tutti i Destinatari sono tenuti al rispetto delle disposizioni contenute nel Modello qualsiasi violazione alle disposizioni del Codice Etico e del Modello di organizzazione, gestione e controllo saranno valutate dal Datore di Lavoro al fine di avviare un procedimento disciplinare ai sensi dello Statuto dei Lavoratori.

In particolare, il potere disciplinare è riconosciuto al datore di lavoro dall'art. 2106 c.c. secondo il quale l'inosservanza delle disposizioni contenute negli artt. 2104 e 2105 c.c, precisamente l'inosservanza del dovere di diligenza, di obbedienza e dell'obbligo di fedeltà – tra cui rientrano anche le violazioni e o il mancato rispetto dei principi e delle disposizioni del presente Modello organizzativo - può dar luogo nei confronti del lavoratore, all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione.

La modalità di esercizio del potere disciplinare

Le modalità concrete dell'esercizio del potere disciplinare sono fissate dall'*art. 7 dello statuto dei lavoratori*, che subordina l'adozione della sanzione ad uno specifico procedimento finalizzato a garantire l'effettività del diritto di difesa del lavoratore. Il codice disciplinare è portato a conoscenza dei lavoratori mediante affissione accessibile

a tutti i lavoratori. L'affissione non può avvenire con mezzi equipollenti, e in mancanza di valida affissione, il datore di lavoro non può sanzionare il lavoratore, pertanto la prima garanzia procedimentale è costituita dalla pubblicità del codice disciplinare, che è diretta a far conoscere al lavoratore le possibili condotte illecite e le relative sanzioni che possono essere irrogate. L'affissione nei locali aziendali (art. 7 statuto dei lavoratori) costituisce l'indefettibile requisito di legittimità della sanzione e, perseguendo essa lo scopo sia di dichiarare quale sia il codice disciplinare applicabile sia di assicurare un'agevole conoscibilità, è necessario che la suddetta affissione sia in atto al momento del fatto, che realizza la mancanza disciplinare, nonché in quello della contestazione dell'addebito e dell'irrogazione della sanzione, mentre è inidonea la conoscenza del codice da parte dei dipendenti per una precedente e temporanea forma di affissione o per l'avvenuta consegna di copia del codice medesimo.

Le sanzioni possono essere:

- il rimprovero verbale;
- la sospensione dal servizio;
- il rimprovero scritto;
- il licenziamento con preavviso;
- la multa;
- il licenziamento senza preavviso.

Ulteriore garanzia procedimentale è costituita dalla necessaria contestazione dell'addebito al lavoratore. Il datore di lavoro non può adottare nessun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza avergli dato la possibilità di essere sentito a sua difesa, in mancanza la contestazione è nulla. La contestazione dell'addebito deve essere tempestiva, il datore di lavoro deve procedere alla contestazione dell'addebito tempestivamente, né può ritardarla in modo da rendere difficoltoso per il lavoratore la sua difesa, ma deve effettuarla in immediata connessione temporale con il fatto addebitato al dipendente, cioè l'immediatezza deve essere valutata con riferimento al momento della commissione o della conoscenza del fatto contestato. La contestazione deve essere puntuale e specifica in modo da consentire al lavoratore una efficace difesa, fissando la portata ed i limiti del suo comportamento "asseritamente" illecito, pertanto deve contenere i dati e gli aspetti essenziali del fatto addebitato, anche se non necessariamente l'indicazione delle norme di legge o del contratto collettivo che si assumono violate.

La stessa non deve essere generica o sommaria. L'inosservanza di tali obblighi comporta la nullità della contestazione. Deve altresì contenere eventuali indicazioni di eventuali episodi precedenti, ove il datore di lavoro intende far pesare nella valutazione complessiva anche tale circostanza. L'addebito deve essere tempestivamente contestato, l'immediatezza deve essere valutata con riferimento al momento della commissione o della conoscenza del fatto che si contesta. Tale requisito deve essere inteso secondo buona fede ed è perciò compatibile con quell'intervallo di tempo che risulti necessario per il preciso accertamento della condotta del lavoratore. A seguito della contestazione dell'addebito avente forma scritta, tale requisito è considerato imprescindibile sia per esigenze di certezza e di immutabilità, che per fissare il tempo per l'applicazione della sanzione disciplinare, il lavoratore

può entro cinque giorni, presentare le sue giustificazioni scritte od orali. Il lavoratore nell'esporre le proprie ragioni, può farsi assistere da un rappresentante sindacale cui aderisce o conferirgli mandato. Una volta trascorso il termine di cinque giorni previsto dall'art. 7 il datore di lavoro può adottare la sanzione disciplinare.

In conformità all'art. 2106 c.c. la sanzione disciplinare deve essere proporzionata alla gravità del fatto. Con riferimento all'applicazione della sanzione, la misura di quest'ultima non deve essere determinata in astratto, ma in concreto prendendo in considerazione, non solo il fatto oggettivo posto in essere dal lavoratore, ma l'insieme delle circostanze nelle quali il lavoratore ha compiuto la condotta contestata.

Il datore di lavoro ha l'onere di provare i presupposti giustificativi delle sanzioni disciplinari con riferimento in linea di principio, anche al profilo della proporzionalità, pur quando questa non sia di particolare entità, poiché non esiste una correlazione necessaria ed immediata tra l'esistenza di inadempimento del lavoratore e l'erogabilità delle sanzioni disciplinari data la natura e la funzione particolare di quest'ultime, che non trovano il loro fondamento nelle regole generali dei rapporti contrattuali, cioè non sono assimilabili alle penali di cui all'art. 1382 c.c., e non hanno una funzione risarcitoria, ma hanno una portata afflittiva sul piano morale, hanno la funzione di diffidare dal compimento di ulteriori violazioni.

Sempre in conformità dell'art. 2106 c.c., le sanzioni devono essere proporzionate alla gravità dell'infrazione commessa. Sono comunque vietate sanzioni che comportano mutamenti definitivi del rapporto; sospensione dal servizio e dalla retribuzione per periodi superiori a 10 giorni; multe per importi superiori a 4 ore di retribuzione base. Il lavoratore al quale sia stata applicata una sanzione disciplinare può ricorrere anche per mezzo dell'associazione sindacale cui aderisce o conferirle mandato, alle procedure conciliative previste dai contratti collettivi, o adire l'autorità giudiziaria, oppure può promuovere, nei 20 giorni successivi, la costituzione di un collegio di conciliazione ed arbitrato. La costituzione avviene tramite la Direzione provinciale del lavoro, l'esecuzione della sanzione è sospesa fino alla pronuncia del collegio. Se entro 10 giorni dall'invito il datore di lavoro non nomina un proprio rappresentante, il collegio non provvede, e la sanzione disciplinare non ha effetto.

Il potere disciplinare è riconosciuto al datore di lavoro dall'art. 2106 c.c. secondo il quale l'inosservanza delle disposizioni contenute negli artt. 2104 e 2105 c.c, precisamente l'inosservanza del dovere di diligenza, di obbedienza e dell'obbligo di fedeltà, può dar luogo nei confronti del lavoratore, all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione.

Le misure disciplinari

Misure nei confronti dei dipendenti

In caso di violazioni del Modello da parte dei lavoratori dipendenti si applicheranno agli stessi le previsioni dell'articolo 7 della legge 20 maggio 1970, n. 300 e s.m.i. (statuto dei lavoratori) e del vigente CCNL di categoria. Se la condotta costituisce violazione dei doveri del rapporto di lavoro, fermo restando il procedimento disciplinare ed il relativo provvedimento conclusivo, C.R. TECHNOLOGY SYSTEMS S.p.A. potrà assumere decisioni che tengano conto di quanto previsto dall'art. 2119 e ss del codice civile.

Misure nei confronti dei dirigenti

In caso di violazioni del Modello da parte dei dirigenti, il titolare del potere disciplinare avvierà i procedimenti di sua competenza al fine delle eventuali contestazioni e della eventuale applicazione delle sanzioni previste, ai sensi di legge e del CCNL di categoria, con l'eventuale revoca dei poteri agli stessi attribuiti mediante atti formali quali procure, deleghe, etc.

Se a violare il Modello è un componente dell'Organo Amministrativo, di detta violazione l'OdV deve darne immediata comunicazione all'Assemblea. A seguito della comunicazione l'Assemblea, previa valutazione, applica nel rispetto della legge il provvedimento che ritiene opportuno in ragione della gravità, della colpa e del danno che dal comportamento dell'Amministratore sia derivato alla Società.

Qualora la violazione sia stata tale da ledere il rapporto di fiducia con la Società, l'Assemblea potrà procedere con gli atti formali alla revoca della carica per giusta causa.

Misure nei confronti degli Amministratori

Se a violare il Modello è l'Amministratore Unico, di detta violazione l'Odv deve darne immediata comunicazione all'Assemblea. A seguito della comunicazione l'Assemblea, previa valutazione, applica nel rispetto della legge il provvedimento che ritiene opportuno in ragione della gravità, della colpa e del danno che dal comportamento dell'Amministratore sia derivato alla Società. Qualora la violazione sia stata tale da ledere il rapporto di fiducia con la Società, l'Assemblea potrà procedere con gli atti formali alla revoca della carica per giusta causa.

Misure nei confronti dei membri del Collegio Sindacale

In caso di violazione del Modello da parte di un componente del Collegio Sindacale, l'Organo Amministrativo, qualora le violazioni siano tali da integrare la revoca per giusta causa, propone all'Assemblea, sentiti gli altri componenti del Collegio Sindacale, l'adozione dei provvedimenti di competenza provvedendo alle ulteriori incombenze previste dalla normativa di legge.

Misure nei confronti dei terzi

Per quanto riguarda i rapporti con i terzi, nei relativi contratti dovranno essere previsti meccanismi o clausole contrattuali con cui si dia informazione alle controparti dell'adozione del Modello di cui al D.lgs. 8 giugno 2001 n. 231. Si dovrà, inoltre, precisare che il mancato rispetto degli obblighi previsti dal D.lgs. 8 giungo 2002, n. 231 comporterà la risoluzione di diritto del contratto ai sensi dell'art. 1456 c.c., fatto salvo l'eventuale risarcimento per i danni arrecati alla Società. La mancata inclusione delle dette clausole o meccanismi contrattuali dovrà essere comunicata dalla funzione aziendale competente nella quale è operativo il contratto, correlata da debite motivazioni, all'Organismo di Vigilanza.

14. SISTEMA DI COMUNICAZIONE - INFORMAZIONE – FORMAZIONE

14.1. Comunicazione e Informazione

C.R. TECHNOLOGY SYSTEMS S.p.A. procederà a organizzare incontri per la comunicazione e diffusione del Codice Etico e del Modello di organizzazione, gestione e controllo adottato per la gestione e la prevenzione dei rischi di cui al D.lgs. 8 giugno 2001 n. 231. In considerazione dell'importanza che la conoscenza della materia riveste per il corretto svolgimento delle attività aziendali nel rispetto dei principi di trasparenza, osservanza delle disposizioni normative e regolamentari e dei principi etico – sociali, nonché al fine di assicurare all'interno dell'azienda una idonea diffusione, C.R. TECHNOLOGY SYSTEMS S.p.A. curerà l'attivazione di una cartella informatica accessibile a tutti i dipendenti, nel cui ambito far confluire i seguenti documenti e le sue successive modifiche ed integrazioni:

- ✓ il Codice Etico;
- ✓ il testo del D.lgs. 8 giugno 2001 n. 231;
- ✓ il Modello di organizzazione, gestione e controllo, parte generale e parte speciale.

Per clienti, fornitori e terzi in genere è altresì assicurata da C.R. TECHNOLOGY SYSTEMS S.p.A. una informativa circa l'adozione del Modello e del Codice Etico provvedendo altresì alla pubblicazione nel proprio sito:

- ✓ del Modello PG;
- ✓ del Codice Etico.

In riferimento ai rapporti con i fornitori e con i terzi in genere che intrattengano rapporti commerciali con C.R. TECHNOLOGY SYSTEMS S.p.A., si darà loro comunicazione ed informativa circa l'adozione del Modello e del Codice Etico precisando altresì che la violazione alle disposizioni del D.lgs. 8 giugno 2001 n. 231 e del Codice Etico di C.R. TECHNOLOGY SYSTEMS S.p.A. potrà costituire motivo di risoluzione di diritto del rapporto contrattuale ai sensi dell'art 1456 c.c. La diffusione del Modello e del Codice Etico è obbligatoria: deve essere tracciata la specifica attività di comunicazione, informazione e formazione somministrata tanto al personale (impiegati ed operai), quanto al *management* ed ai vertici aziendali.

14.2. Formazione

Sul piano della formazione, C.R. TECHNOLOGY SYSTEMS S.p.A., oltre a pianificare una formazione di carattere generale diretta a comunicare, informare e formare i Destinatari sulle previsioni del Decreto, le ragioni di opportunità e quelle giuridiche che hanno ispirato l'adozione del Modello, pianificherà altresì un adeguato programma di formazione specifica rivolta al personale delle aree a rischio opportunamente somministrato in funzione dei luoghi di lavoro, dei livelli e delle mansioni svolte.

14.3 Piano Formativo

I principi

Il Piano formativo sarà articolato tenendo conto dei contenuti e delle modalità di erogazione, della qualifica dei Destinatari, del livello di rischio dell'area in cui operano, dei poteri e/o delle deleghe agli stessi conferite. La formazione ed i relativi contenuti saranno articolati secondo moduli distinti in base al livello e al ruolo organizzativo dei Destinatari, tenendo conto:

- delle responsabilità e dei ruoli (con particolare riguardo a quelli che svolgono attività sensibili);
- dei neoassunti e dei nuovi incarichi: particolare attenzione si dovrà porre ai nuovi assunti per i quali si dovranno prevedere specifici moduli formativi;
- del personale destinato a ricoprire nuovi incarichi (con particolare riguardo a quelli che svolgono attività sensibili).

Contenuto delle sessioni formative

La formazione dovrà prevedere i seguenti contenuti:

- una parte istituzionale comune a tutti i destinatari e avente ad oggetto la normativa di riferimento, il Modello ed il suo funzionamento;
- una parte speciale in relazione a specifici ambiti operativi, che avendo a riferimento la mappatura delle attività sensibili, sia volta a diffondere la conoscenza dei reati, le fattispecie configurabili ed i presidi specifici delle aree di competenza dei Destinatari.

La formazione **è obbligatoria** e deve essere tracciata anche con attestazione finale di frequenza dei corsi e del relativo apprendimento. Per la somministrazione della formazione potranno essere utilizzate le seguenti differenti modalità:

- sessioni in aula con incontri dedicati oppure introduzione, nelle sessioni formative standard già adottate, di moduli di formazione specifica;
- e-learning: attraverso un modulo relativo alla parte istituzionale per tutti i dipendenti e con test di verifica dell'apprendimento.

I contenuti formativi dovranno essere opportunamente aggiornati in ragione dell'evoluzione della normativa ed alle intervenute modifiche al Modello.

Controllo e verifica sull'attuazione del piano di formazione

Sarà cura di C.R. TECHNOLOGY SYSTEMS S.p.A. raccogliere le evidenze relative all'effettiva pianificazione della formazione, alla partecipazione ai programmi di formazione e alla custodia della documentazione negli appositi archivi e/o cartelle del personale interessato. L'Organismo di Vigilanza potrà effettuare controlli periodici sul grado di conoscenza da parte dei dipendenti del Decreto e del Modello.

15. CRITERI DI APPLICABILITÀ ASTRATTA DEI REATI PRESUPPOSTO ALL'ATTIVITÀ CARATTERISTICA DI C.R. TECHNOLOGY SYSTEMS S.p.A.

L'Organo Amministrativo procederà, altresì, a valutare la sensibilità alle fattispecie di cui al Decreto della attività specifica/caratteristica di C.R. TECHNOLOGY SYSTEMS S.p.A., tenendo in evidenza, a titolo meramente esemplificativo e non esaustivo, i seguenti criteri:

- condizioni soggettive di imputabilità;
- condizioni oggettive di imputabilità;
- criteri di esclusione;

- riconducibilità delle condotte o meno all'attività di C.R. TECHNOLOGY SYSTEMS S.p.A.;
- interesse o vantaggio per C.R. TECHNOLOGY SYSTEMS S.p.A.;
- ripetitività della condotta illecita nell'ambito dell'attività aziendale, nonché conseguenze e danni sofferti da C.R. TECHNOLOGY SYSTEMS S.p.A.;
- processi/flussi interni a cui si applica la condotta illecita;
- perseguibilità dell'illecito per dolo o colpa;
- ragionevole probabilità della realizzazione della condotta illecita a rischio all'interno dei processi/flussi aziendali.

Mediante l'uso dei detti criteri e degli eventuali altri che in *continuum* saranno presi in considerazione, C.R. TECHNOLOGY SYSTEMS S.p.A. ed il suo management potranno dare prevalenza di intervento e/o avviare adeguati piani d'azione delle attività aziendali maggiormente sensibili ai rischi 231 e di quelle che potranno esserlo in futuro.

C.R. TECHNOLOGY SYSTEMS S.p.A.

Per il Consiglio di Amministrazione

_____

ALLEGATO – 1

A seguire si riportano le fattispecie presupposto per l'applicabilità della responsabilità di cui al Decreto 231:

- ✓ **Delitti contro la pubblica amministrazione (art. 24)** – i cui reati presupposto sono: malversazione ai danni dello Stato (art. 316 bis c.p.), indebita percezione di erogazioni a danno dello Stato (art. 316 ter c.p.), truffa a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare (art. 640, 2° comma, n. 1, c.p.), frode nelle pubbliche forniture (art. 356 c.p.), Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.), frode informatica di cui all'art. 2 della L. n. 898/1986 (art. 640-ter c.p.).
- ✓ **Reati informatici e trattamento illecito dei dati (art. 24-*bis*)** – i cui reati presupposto sono: falsità in un documento informatico pubblico o privato (art. 491 bis c.p.), accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.), detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.), diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.), intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.), installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.), danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.), danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.), danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.), danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.), frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.), trattamento illecito di dati (artt. 167, 167 bis e 167 ter D.lgs. 30 giugno 2003 n. 196 – introdotti da d. lgs. 101/2018), falsità nelle dichiarazioni e notificazioni al Garante (art. 168 D.lgs. 30 giugno 2003 n. 196), misure di sicurezza (art. 169 D.lgs. 30 giugno 2003 n. 196 - abrogato), inosservanza di provvedimenti del Garante (art. 170 D.lgs. 30 giugno 2003 n. 196), altre fattispecie (art. 171 D.lgs. 30 giugno 2003 n. 196).
- ✓ **Delitti di criminalità organizzata (art. 24-*ter*)** - i cui reati presupposti sono: associazione per delinquere (art. 416 c.p., ad eccezione del sesto comma), associazione a delinquere finalizzata alla riduzione o al mantenimento in schiavitù, alla tratta di persone, all'acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni sull'immigrazione clandestina di cui all'art. 12 D.lgs.286/1998 (art. 416, sesto comma, c.p.), associazione di tipo mafioso (art. 416-bis c.p.), scambio elettorale politico-mafioso (art. 416-ter c.p.), sequestro di persona a scopo di estorsione (art. 630 c.p.), associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 9 ottobre 1990, n. 309), illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al

pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo(*) (art. 407, co. 2, lett. a), numero 5), c.p.p.). (*) Escluse quelle denominate «da bersaglio da sala», o ad emissione di gas, nonché le armi ad aria compressa o gas compressi, sia lunghe sia corte i cui proiettili erogano un'energia cinetica superiore a 7,5 joule, e gli strumenti lanciarazzi, salvo che si tratti di armi destinate alla pesca ovvero di armi e strumenti per i quali la "Commissione consultiva centrale per il controllo delle armi" escluda, in relazione alle rispettive caratteristiche, l'attitudine a recare offesa alla persona.

- ✓ **Peculato, corruzione e abuso d'ufficio, concussione e induzione indebita a dare o promettere utilità (art. 25) -** Corruzione per un atto d'ufficio (art. 318 c.p. - art. 321 c.p.), Istigazione alla corruzione (art. 322, c.p.), Concussione (art. 317 c.p.), Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p. - art. 319-bis - art. 321 c.p.), Corruzione in atti giudiziari (art. 319-ter , 2° comma, c.p.; art. 321 c.p.), Induzione indebita a dare o promettere utilità (art. 319 quater c.p.), Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri (art. 322-bis c.p.), Traffico di influenze illecite (art. 346 bis c.p.). Quando il fatto offende gli interessi finanziari dell'Unione Europea: Peculato (art. 314, comma 1, c.p.), Peculato mediante profitto dell'errore altrui (art. 316 c.p.), Abuso d'ufficio (art. 323 c.p.).
- ✓ **Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis*)** – i cui reati presupposto sono: falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.), alterazione di monete (art. 454 c.p.), spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.), spendita di monete falsificate ricevute in buona fede (art. 457 c.p.), falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.), contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.), fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.), uso di valori di bollo contraffatti o alterati (art. 464 c.p.), contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.), introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).
- ✓ **Delitti contro l'industria e il commercio (art. 25-*bis 1*)** – i cui reati presupposto sono: turbata libertà dell'industria o del commercio (art. 513 c.p.), frode nell'esercizio del commercio (art. 515 c.p.), vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.), vendita di prodotti industriali con segni mendaci (art. 517 c.p.), fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.), contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.), illecita concorrenza con minaccia o violenza" (art. 513-bis c.p.), frodi contro le industrie nazionali (art. 514).

- ✓ **Reati societari (art. 25-*ter*)** – i cui reati presupposto sono: false comunicazioni sociali (art. 2621 c.c.), fatti di lieve entità (art. 2621 bis c.c.), false comunicazioni sociali in danno dei soci o dei creditori (art. 2622 c.c.), contravvenzione e delitto di falso in prospetto (art. 2623 c.p.), contravvenzione e delitto di falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624 1° e 2° comma c.c.), impedito controllo (art. 2625 c.c.), indebita restituzione dei conferimenti (art. 2626 c.c.), illegale ripartizione di utili e riserve (art. 2627 c.c.), illecite operazioni sulle azioni o quote sociali o proprie o della controllante (art. 2628 c.c.), operazioni in pregiudizio ai creditori (art. 2629 c.c.), omessa comunicazione del conflitto d'interessi (art. 2629 bis c.c.), formazione fittizia del capitale sociale (art. 2632 c.c.), indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.), corruzione tra privati (art. 2635 c.c.), istigazione alla corruzione tra i privati (art. 2635 bis c.c.), illecita influenza sull'assemblea (art. 2636 c.c.), aggiotaggio (art. 2637 c.c.), ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).
- ✓ **Delitti con finalità di terrorismo ed eversione dell'ordine democratico (art. 25-*quater*)** - i cui reati presupposto sono quelli previsti dal codice penale e dalle leggi speciali e i delitti posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo conclusa a New York il 9.12.1999.
- ✓ **Pratiche di mutilazione degli organi genitali femminili (art.25-*quater*.1)** – il cui Reato presupposto è: pratiche di mutilazione degli organi genitali femminili (art. 583 bis c.p.).
- ✓ **Delitti contro la personalità individuale (art. 25 - *quinquies*)** – i cui reati presupposto sono: riduzione in schiavitù (art. 600 c.p.), prostituzione minorile (art. 600-bis c.p.), pornografia minorile (art. 600-ter, primo e secondo comma, c.p.), detenzione di materiale pornografico (art. 600-quater, c.p.), iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 - quinquies, c.p.), tratta e commercio di schiavi (art. 601 c.p.), alienazione e acquisto di schiavi (art. 602 c.p.), Intermediazione illecita e sfruttamento del lavoro (art. 603 c.p.).
- ✓ **Abusi di mercato (art. 25-*sexies*)** – i cui reati presupposto sono: abuso di informazioni privilegiate (art. 184 T.U.F.), manipolazione di mercato (art. 185 T.U.F.) previsti dalla parte V, titolo I-*bis*, capo II, del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.
- ✓ **Omicidio colposo o lesioni colpose gravi o gravissime, commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-*septies*)** – i cui reati presupposto sono: Omicidio colposo (art. 589 c.p.) e lesioni colpose gravi o gravissime (art. 590 c.p.), commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (Legge 123 / 2007).
- ✓ **Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio (art. 25-*octies*)** – i cui reati presupposto sono: ricettazione (art. 648 c.p.), riciclaggio (art. 648 bis c.p.), impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.), autoriciclaggio (art. 648 ter.1).

- ✓ **Delitti in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies.1)** – i cui reati presupposto sono: Indebito utilizzo e falsificazione di carte di credito e di pagamento (art. 493-ter, c.p.), Detenzione e diffusione di apparecchiature, dispositivi, programmi informatico diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater, c.p.), Frode informatica (art 640-ter, c.p).
- ✓ **Delitti in materia di violazione del diritto d'autore (art. 25-*novies*)** – i cui reati presupposto sono: messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, l. 633/1941 comma 1 lett a) bis), reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, l. 633/1941 comma 3), abusiva duplicazione, per trarneprofitto, di programmi per elaboratore, importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis l. 633/1941 comma 1), riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis l. 633/1941 comma 2), abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter l. 633/1941), mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies l. 633/1941), fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies l. 633/1941).
- ✓ **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 *decies*)** – il cui Reato presupposto è: induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.).
- ✓ **Reati transnazionali (art. 10, L. 16 Marzo 2006 n.146)** - i cui reati presupposto sono: associazione a delinquere (art. 416 c.p.), associazione di stampo mafioso (art. 416 bis c.p.), associazione per delinquere

finalizzata al contrabbando di tabacchi lavorati esteri (art. 291 quater del DPR 43/1973), associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del DPR 309/1990), Reato concernente il traffico di migranti (art. 12 D.lgs. 286/1998), Induzione a rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.), favoreggiamento personale (art. 378 c.p.).

- ✓ **Reati ambientali (art. 7, Decreto Legislativo 7 luglio 2011, n. 121)** – i cui reati presupposto sono: Inquinamento ambientale (Art. 452-*Bis* c.p.), Disastro ambientale (art. 452-*Quater* c.p.), Delitti colposi contro l'ambiente (art. 452-*Quinquies* c.p.), Traffico e abbandono di materiale ad alta radioattività (art. 452-*sexies* c.p.), Circostanze aggravanti (art. 452-*Octies* c.p.), Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (Art. 727-Bis c.p.), il danneggiamento di habitat (art. 733-bis c.p.), l'apertura o scarico di acque reflue industriali (D.lgs. n. 152/2006, art. 137), la gestione di rifiuti non autorizzata e il traffico illecito di rifiuti (D.lgs. n. 152/2006, art. 256 e artt. 259 e 260), l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio (D.lgs. n. 152/2006, art. 258), violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D.lgs. n. 152/2006, art. 257), sanzioni (D.lgs. n. 152/2006, art. 279), la produzione il consumo, l'importazione, l'esportazione, la detenzione e la commercializzazione di sostanze lesive dell'ozono stratosferico (legge n. 549/1993, art. 3), lo scarico di sostanze inquinanti provocato da natanti (D.lgs. n. 202/2007 - attuazione della direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e conseguenti sanzioni), rati legge n. 159/1992.
- ✓ **Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 *duodecies*)** – la cui condotta presupposto è prevista dall'art. 22 – commi 3, 3 bis, 3 ter, 5 e 12 bis del D.lgs. 52 luglio 1998 n. 286 – testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero.
- ✓ **Razzismo e xenofobia (art. 25-terdecies)** - articolo 3, comma 3 bis, della legge 13 ottobre 1975, n. 654 - Ratifica ed esecuzione della convenzione internazionale sull'eliminazione di tutte le forme di discriminazione razziale, aperta alla firma a New York il 7 marzo 1966.
- ✓ **Frode in competizioni sportive - Esercizio abusivo - Gioco - Scommessa - Giochi d'azzardo - Apparecchi vietati (art. 25-quaterdecies) –** introdotto dalla Legge 3 Maggio 2019, n. 39, pubblicata sulla GU del 16/05/2019, in vigore dal 17/05/2019 – la previsione normativa dispone che in relazione alla commissione dei reati di cui agli articoli 1 e 4 della legge 13 dicembre 1989, n. 401, si applicano all'ente le seguenti sanzioni pecuniarie: a) per i delitti, la sanzione pecuniaria fino a cinquecento quote; b) per le contravvenzioni, la sanzione pecuniaria fino a duecentosessanta quote. Nei casi di condanna per uno dei delitti indicati nel comma 1, lettera a), del presente articolo, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a un anno.
- ✓ **Reati tributari – (art. 25-quinquiesdecies) -** 1. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, si applicano all'ente le seguenti sanzioni pecuniarie: a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto

dall'articolo 2, comma 1, la sanzione pecuniaria fino a cinquecento quote; b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 2, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote; c) per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote; d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, la sanzione pecuniaria fino a cinquecento quote; e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote; f) per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote; g) per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote.

1-bis. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, si applicano all'ente le seguenti sanzioni pecuniarie:

a) per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote;

b) per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattro- cento quote;

c) per il delitto di indebita compensazione previsto dall'articolo 10-quater, la sanzione pecuniaria fino a quattrocento quote.

2. Se, in seguito alla commissione dei delitti indicati ai commi 1 e 1 - bis, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

3. Nei casi previsti dai commi 1, 1 - bis e 2, si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e).

- ✓ **Contrabbando – (art. 25-sexiesdecies)** - 1. In relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, si applica all'ente la sanzione pecuniaria fino a duecento quote. 2. Quando i diritti di confine dovuti superano centomila euro si applica all'ente la sanzione pecuniaria fino a quattrocento quote. 3. Nei casi previsti dai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

ALLEGATO – 2

MODULO DI SEGNALAZIONE ALL'ORGANISMO DI VIGILANZA di C.R. TECHNOLOGY SYSTEMS S.p.A.

Il presente modulo può essere utilizzato da chiunque voglia comunicare o segnalare all'Organismo di vigilanza di C.R. TECHNOLOGY SYSTEMS S.p.A. la commissione o il tentativo di commissione di uno dei comportamenti in violazione ai principi del Codice Etico, del Modello di organizzazione, gestione e controllo di Parte Generale e di Parte Speciale di C.R. TECHNOLOGY SYSTEMS S.p.A., alle procedure, alle istruzioni, alla modulistica o al sistema delle deleghe di C.R. TECHNOLOGY SYSTEMS S.p.A., per comunicare la commissione o i tentativi di commissione di uno dei reati presupposto di cui al D.lgs. 8 giugno 2001 n. 231, nonché nei casi di ***Whistleblowing*** *di cui alla Legge 30 novembre 2017 n. 179.*

Dati dell'autore del comportamento oggetto della segnalazione

Nome _____

Cognome _____

Unità Organizzativa di appartenenza _____

Telefono _____ (se noto)

E_mail _____ (se noto)

Descrizione dettagliata del comportamento che ha generato la segnalazione con indicazione del fatto accaduto del luogo e dell'ora in cui è accaduto e di quant'altro possa essere utile a meglio descriverlo.

Dati del segnalante

Numero di matricola _____

Unità Organizzativa di appartenenza _____

Telefono _____

E_mail _____

Informativa ai sensi dell'art. 13 Reg. UE 679/2016 – Ai sensi e per gli effetti del (i) Regolamento UE 679/2016 "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*" (il "RGPD") e del (ii) D.lgs. 196/2003, "*Codice in materia di protezione dei dati*", come modificato (iii) dal D.lgs. 101/2018 recante disposizioni di adeguamento della normativa nazionale al RGPD, C.R. TECHNOLOGY SYSTEMS S.p.A.**,** in veste di titolare del trattamento dei dati personali *ex* art. 4 par. 1 n. 7 del RGPD, le rende noto che i suoi dati personali acquisiti mediante la presente segnalazione saranno trattati esclusivamente per le finalità connesse al rispetto degli obblighi derivanti dal D.lgs. 231 del 2001, nonché utilizzabili, ed in seguito conservati, sia in forma cartacea che informatica. Il segnalante resta, in ogni caso, personalmente responsabile del contenuto eventualmente diffamatorio delle comunicazioni trasmesse; l'Organismo di vigilanza, si riserva di non prendere in considerazione le segnalazioni prodotte in evidente *"mala fede"*. Si ricorda che i dati da Lei forniti devono essere pertinenti rispetto alle finalità della segnalazione, cosicché l'Organismo di vigilanza di C.R. TECHNOLOGY SYSTEMS S.p.A. sarà libero di non dare seguito alle segnalazioni riguardanti condotte o soggetti estranei agli obblighi derivanti dal D.lgs. 231 del 2001. Salvo l'espletamento di obblighi derivanti dalla legge, i dati personali da Lei forniti non avranno alcun ambito di comunicazione e diffusione. Il titolare del trattamento la informa inoltre che, in qualità di soggetto interessato, potrà ogni momento esercitare i diritti espressamente riconosciuti agli articoli 15-22 del Reg. UE 679/2016, ed in particolare il diritto di accedere ai propri dati personali, di chiederne la rettifica, l'aggiornamento o la cancellazione, se incompleti, erronei o raccolti in violazione della legge, la limitazione o la portabilità, nonché di opporsi al loro trattamento per motivi legittimi, rivolgendo le sue richieste direttamente ad C.R. TECHNOLOGY SYSTEMS S.p.A., tramite casella di posta elettronica odvcrtechnologysystems@gmail.com o tramite posta ordinaria in busta chiusa all'indirizzo via Rossaro n. 9, Treviglio 24047 BG.

Con la sottoscrizione del presente documento autorizzo il trattamento dei dati ai sensi del Reg. UE 679/2016.

Data _____ Firma _____