MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

TAGETIK SOFTWARE S.r.l.

Ai sensi dell'art. 6 del D.Lgs. 231/01

Revisioni

Rev.	Natura della revisione	Data delibera CDA
0	Prima emissione	20.02.2012
1	Revisione generale	07.11.2017
2	Revisione per aggiornamento normativo e introduzione parte speciale H – Reati Tributari	10.10.2022
3	Revisione per aggiornamento del paragrafo 3.3 Parte generale con recepimento della procedura della Whistleblowing a seguito della pubblicazione in G.U. del D.Lgs. 24/2003 del 10 marzo 2023 n. 24 di "Attuazione della direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio, del 23 ottobre 2019	12.07.2023

INDICE

1. DEFINIZIONI

TAGETIK (o la Società)	Sta ad indicare la società Tagetik Software S.r.l.
Decreto	indica il D. Lgs. 8 giugno 2001 n. 231;
Destinatari	indica tutti i soggetti tenuti al rispetto delle prescrizioni contenute nel Modello, in particolare: tutti coloro che operano in nome e per conto di TAGETIK SOFTWARE S.R.L., inclusi gli amministratori, i sindaci, i membri degli altri eventuali organi sociali, i dipendenti, i collaboratori anche occasionali, i partner commerciali, i fornitori, nonché i componenti dell'organismo di Vigilanza.
Enti o Ente	ai sensi dell'art. 1 del Decreto, indica gli enti forniti di personalità giuridica, le società e le associazioni anche prive di personalità giuridica cui si applicano le disposizioni del Decreto ed in particolare la responsabilità amministrativa dallo stesso introdotta;
Linee Guida	indica le Linee Guida per la costruzione dei Modelli di organizzazione, gestione e controllo ex D. Lgs. 231/2001 pubblicate da Confindustria nella più recente revisione (marzo 2014);
Modello	indica il Modello di organizzazione, gestione e controllo previsto dal Decreto;
Reati Presupposto	indica i reati per i quali il Decreto ha introdotto la responsabilità amministrativa dell'Ente. si tratta, in particolare, delle fattispecie di reato individuate dagli artt. 24 e 25 e segg. del Decreto;
Testo Unico	indica il D. lgs. 9 aprile 2008 n. 81. (c.d. Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro) e successive modifiche ed integrazioni
TUF	indica il D. lgs. 24 febbraio 1998 n. 58, Testo Unico in materia di intermediazione finanziaria e successive modifiche ed integrazioni

2. INTRODUZIONE

2.1 Il regime di responsabilità amministrativa degli Enti

L'adeguamento della legislazione italiana ad alcune convenzioni internazionali ha portato, in esecuzione della legge delega del 29 settembre 2000 n. 300, alla promulgazione del D. lgs. 8 giugno 2001 n. 231, entrato in vigore il 4 luglio 2001, "*Disciplina della responsabiità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*".
Il Decreto ha introdotto nell'ordinamento italiano il regime della responsabilità amministrativa degli Enti per alcuni reati (indicati dagli artt. 24 e ss. del Decreto, i c.d. Reati Presupposto) commessi, o semplicemente tentati, nell'interesse o a vantaggio degli Enti medesimi, o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, da parte di:

(i) soggetti che abbiano la rappresentanza, l'amministrazione o la direzione o, anche di fatto, esercitino la gestione o il controllo dell'Ente o di una sua unità organizzata (i soggetti apicali ai sensi dell'art. 5 del Decreto, comma 1, lett. a); o

(ii) soggetti sottoposti alla direzione o vigilanza dei soggetti di cui alla lettera (i) che precede (i soggetti sottoposti all'altrui direzione ai sensi dell'art. 5 del Decreto, comma primo, lett. b).

La responsabilità amministrativa dell'Ente è diretta e distinta dalla responsabilità dell'autore materiale del reato ed è tesa a sanzionare gli Enti per i reati commessi a loro vantaggio o nel loro interesse.
In virtù della responsabilità introdotta dal Decreto, l'Ente subisce pertanto un autonomo procedimento ed è passibile di sanzioni che possono giungere al punto di bloccare l'ordinaria attività d'impresa.
Infatti, oltre alle sanzioni pecuniarie, l'eventuale confisca e la pubblicazione della sentenza di condanna, il Decreto prevede che l'Ente possa essere sottoposto anche a sanzioni di carattere interdittivo (art. 9, comma secondo), quali:

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

In base a quanto stabilito dall'art. 4, gli Enti con sede principale in Italia possono essere perseguiti anche per reati commessi all'estero, qualora la legislazione del paese straniero non preveda una forma analoga di responsabilità.
La responsabilità amministrativa dell'Ente si fonda su una "*colpa di organizzazione*": l'Ente è ritenuto, cioè, responsabile in via amministrativa del reato commesso dal suo esponente, se ha omesso di darsi un'organizzazione in grado di impedirne efficacemente la realizzazione e, in particolare, se ha omesso di dotarsi di un sistema di controllo interno e di adeguate procedure per lo svolgimento delle attività a maggior rischio di commissione dei reati previsti dal Decreto.
Al contrario, ai sensi dell'art. 5 comma 2 del Decreto, l'Ente non risponde se le persone suindicate hanno agito nell'interesse esclusivo proprio o di terzi.
I processi attraverso cui dotarsi di un simile sistema di organizzazione e controllo interno sono indicati agli artt. 6 e 7 del Decreto, e cioè:

- l'approvazione, adozione, ed efficace attuazione, anteriormente alla commissione di un reato, di un Modello idoneo a prevenire la commissione dei Reati Presupposto previsti dal Decreto. In linea generale, ed in estrema sintesi, il Modello è ritenuto "idoneo" quando i soggetti che hanno posto in essere il reato abbiano agito in modo deliberato e fraudolento al fine di eludere i relativi presidi posti in essere dal Modello stesso;
- la creazione di un Organismo di Vigilanza interno, con poteri autonomi di iniziativa e controllo, deputato (i) al controllo dell'effettivo funzionamento del Modello e del rispetto delle previsioni in esso contenute da parte di tutti i destinatari; (ii) alla costante verifica della reale efficacia preventiva del Modello; e (iii) al suo aggiornamento.

Il Modello, in base alle previsione del Decreto, con riferimento ai poteri delegati ed al possibile rischio di commissione dei reati deve peraltro:

- individuare le attività nel cui ambito possono essere commessi reati;

- prevedere specifici controlli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

L'adozione del Modello, pur se non obbligatoria, ma meramente facoltativa, ha efficacia esimente ai fini della responsabilità amministrativa solo se accompagnata dall'efficace e concreta attuazione dello Modello stesso e dal suo costante aggiornamento ed adeguamento.
Il Giudice del procedimento penale, infatti, è chiamato a valutare, nell'ambito del procedimento volto a verificare la responsabilità amministrativa dell'Ente, l'idoneità del Modello a prevenire la commissione di reati, e la sua concreta applicazione ed efficacia.

2.2 Storia, attività e governance di TAGETIK SOFTWARE S.R.L.

La società Tagetik Software S.r.l. ha la propria sede legale, operativa e amministrativa in LUCCA, Via Roosevelt, 103 e proprie sedi operative/unità locali in Italia nelle città di Lucca (Via Borgo Giannotti, 37/U), Milano (Largo Richini Francesco, 6), Roma (Via Goito, 39) e Torino (Via Confienza, 10).
Tagetik viene fondata nel 1986 come società di consulenza per occuparsi di processi di Performance Management.
Sebbene ai suoi esordi non fosse che una piccola società sulle colline toscane, è divenuta rapidamente il "software vendor" di soluzioni CPM con la crescita più rapida sul mercato
Negli anni 90 Tagetik si espande in Italia e sviluppa la sua prima suite di applicazioni, costituita da 4 prodotti per il consolidamento, il budgeting, la pianificazione finanziaria, le chiusure e allocazioni.
Nel 1994 con Costa Crociere prima e nel 1997 con Ifil poi, TAGETIK SOFTWARE S.R.L. comincia ad annoverare tra i propri clienti una serie di nomi che fanno parte dell'aristocrazia del business.
Nell'anno 2002 UniCredit, la sesta banca mondiale per grandezza, sceglie Tagetik per il consolidamento civilistico. In questo progetto, Tagetik collabora con UniCredit e inizia lo sviluppo di Tagetik CPM.
Nel 2005 Tagetik lancia Tagetik CPM (ora Tagetik 5), il primo prodotto completamente unificato per tutti i processi di CPM e inizia a espandere la sua attività in altri paesi europei.
Nel 2008 Tagetik continua la sua espansione mondiale e apre due uffici in Nord America. Poco dopo Gartner la inserisce nel Visionary Quadrant del suo "Magic Quadrant for CPM Suites".
Oggi Tagetik è un'azienda globale e offre un prodotto di CPM unificato on-premise o sul cloud. Con oltre 50.000 utenti in 40 mercati diversi, annovera fra i suoi clienti alcune delle più grandi aziende del mondo citate in Fortune 1000.
In data 6 aprile 2017 la totalità delle quote societarie è stata acquisita da Wolters Kluver International Holding B.V. che risulta quindi, a oggi, socio unico di Tagetik Software S.r.l.
Il management di Tagetik Software S.r.l. è attualmente strutturato con un Consiglio di Amministrazione formato di nr. 5 Consiglieri tra i quali sono individuati Consiglieri dotati di specifici poteri (da esercitarsi in firma singola) e membri muniti della Legale Rappresentanza della società.
Operativamente, la società è organizzata mediante 6 Direzioni che fattivamente gestiscono l'organizzazione e la quotidianità nonché lo sviluppo delle attività, nell'ambito degli indirizzi forniti dal Consiglio di Amministrazione.
Tra gli incaricati di Direzione risultano anche riconoscibili alcuni procuratori in particolare per la Salute e Sicurezza nei luoghi di lavoro, la prevenzione dei reati ambientali, la tutela dei dati e il rispetto delle normative in materia di privacy nonché la gestione amministrativo/finanziaria.
Dal 2012 Tagetik Software applica il Modello di Organizzazione Gestione e Controllo ivi descritto e, come previsto ai sensi dell'art. 6 del D.Lgs. 231/01, ha nominato l'Organismo di Vigilanza atto a monitorare l'efficace attuazione del Modello stesso.
Il Modello di Organizzazione Gestione e Controllo è integrato con i sistemi di gestione aziendali e in particolare TAGETIK SOFTWARE S.r.l. ha ottenuto le seguenti certificazioni dall'Organismo internazionale DEKRA CERTIFICATION S.r.l.:
UNI EN ISO 9001 – Sistema di Gestione per la Qualità
ISO 45001:2018 – Sistema di Gestione per la Salute e Sicurezza nei luoghi di lavoro

UNI CEI ISO/IEC 27001 – Sistema di Gestione della Sicurezza delle Informazioni (applicabile ai servizi cloud)
UNI EN ISO 22301 – Business Continuity Management

3. MODELLO DI ORGANIZZAZIONE E DI GESTIONE

3.1 Funzione del Modello

Il Modello ha lo scopo di porre in essere un sistema strutturato di protocolli e di procedure, unitamente ad una serie di attività di controllo e verifica, idoneo a prevenire, o quanto meno a ridurre, il rischio di commissione dei Reati Presupposto da parte dei Destinatari del Modello.
Il Modello ha, tra l'altro, il fine di:

- ribadire che tali forme di comportamento illecito sono fortemente condannate da TAGETIK SOFTWARE S.R.L. in quanto contrarie, oltre che alle disposizioni di legge, anche ai principi etico-sociali cui TAGETIK SOFTWARE S.R.L. ispira lo svolgimento della propria attività d'impresa;
- permettere a TAGETIK SOFTWARE S.R.L., grazie ad un'azione di individuazione delle aree di attività nel cui ambito possono essere commessi i reati, e all'attuazione delle procedure, di intervenire tempestivamente per prevenire o comunque contrastare la commissione di reati.

Ne consegue che aspetti qualificanti del Modello sono, oltre a quanto sopra evidenziato:

- la sensibilizzazione e la formazione di tutti i Destinatari delle previsioni di comportamento e delle procedure volte a garantire il rispetto del Modello;
- la mappatura delle aree di attività di TAGETIK SOFTWARE S.R.L. in relazione alle quali possono essere commessi i Reati Presupposto;
- la dotazione ed attribuzione all'Organismo di Vigilanza di TAGETIK SOFTWARE S.R.L. di specifici poteri autonomi di iniziativa e di vigilanza sull'efficacia e sul buon funzionamento del Modello;
- il controllo e la documentazione delle operazioni a rischio;
- il rispetto del principio di separazione delle funzioni;
- la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
- la verifica dei comportamenti aziendali dei Destinatari, nonché del funzionamento e dell'aggiornamento del Modello.

3.2 Struttura del Modello

Il Modello è composto da una "Parte Generale" e da più "Parti Speciali", redatte in relazione alle tipologie dei Reati, presupposto per i quali TAGETIK SOFTWARE S.R.L. ha ritenuto sussistere un rischio di commissione da parte dei Destinatari in virtù dell'Attività dalla stessa svolta.
TAGETIK SOFTWARE S.R.L. è consapevole della circostanza che l'implementazione del Modello si accompagna nella prassi all'adozione anche di un Codice Etico, in cui l'Ente normalmente formalizza i principi cui ispira l'esercizio della propria attività aziendale.
Non è intenzione di TAGETIK SOFTWARE S.R.L. sottrarsi a tale prassi, tanto più che la Società ha sempre uniformato la propria attività d'impresa ad un insieme di principi e di regole di condotta ispirati ai valori della correttezza, della trasparenza e della buona fede.
Il testo originario del Decreto si limitava a individuare, come Reati Presupposto, alcuni delitti contro la Pubblica Amministrazione ed altri contro il patrimonio mediante frode (artt. 24 e 25). Successivi interventi legislativi hanno ampliato il numero dei Reati Presupposto per i quali è configurabile la responsabilità amministrativa dell'Ente, che è stata pertanto via via estesa alle seguenti fattispecie:

- delitti informatici (art. 24-*bis*);
- Falsità in monete, in carte di pubblico credito e in valori di bollo (art. 25-*bis*);
- reati contro l'industria e il commercio (art. 25 *bis 1*);
- reati societari e corruzione tra privati (art. 25-*ter*);

- delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, nonché alle pratiche di mutilazione degli organi genitali femminili (art. 25-*quater*);
- reati contro la personalità individuale (art. 25-*quinquies*);
- reati di abuso di informazioni privilegiate e di manipolazione del mercato (art. 25-*sexies*);
- reati di omicidio colposo e lesioni personali gravi e gravissime commessi in violazione delle norme tutela della salute o sicurezza sul lavoro (art. 25-*septies*);
- reati di riciclaggio, ricettazione e di impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25–*octies*);
- reati in materia di violazione del diritto d'autore (art. 25 *novies*);
- reati contro l'attività giudiziaria (art. 25 *decies*)
- Reati ambientali (art. 25 *undecies*)
- Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare (art. 25 *duodecies*)
- Reati di razzismo e xenofobia (art. 25 *terdecies*)
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25-*quaterdecies*)
- Reati tributari (Art. 25-quinquiesdecies)
- Contrabbando (Art. 25-sexiesdecies)

Sono previsti nel prossimo futuro ulteriori ampliamenti dei reati espressamente previsti dal Decreto.
Per questa ragione, il Consiglio di Amministrazione di TAGETIK SOFTWARE S.R.L., anche su richiesta dell'Organismo di Vigilanza, dovrà adottare apposite delibere per integrare il Modello con l'inserimento di nuove *Parti Speciali* relative ai reati che, per effetto di ulteriori interventi legislativi, dovessero ampliare l'ambito della responsabilità amministrativa dell'Ente.

3.3 Parte Generale

Secondo quanto stabilito dall'art. 6, comma 3, del Decreto (e secondo le menzionate Linee Guida), la Parte Generale del Modello deve mirare a quattro fondamentali finalità:

I) Individuazione delle Attività Aziendali nel cui ambito possano essere commessi i Reati: mappatura dei rischi

L'art. 6, comma 2, lett. a) del Decreto richiede anzitutto che il Modello provveda alla cosiddetta mappatura dei rischi: è necessaria, pertanto, l'analisi della complessiva attività svolta da TAGETIK SOFTWARE S.R.L. e l'individuazione delle fasi operative o decisionali che comportino il rischio di commissione dei Reati Presupposto.
Dati gli interventi legislativi che hanno portato ad una progressiva estensione dei Reati Presupposto, e dati anche i mutamenti che possono intervenire tanto sulla struttura societaria di TAGETIK SOFTWARE S.R.L., quanto sulle attività dalla stessa svolte, la mappatura dei rischi non potrà mai dirsi definitiva e immodificabile, ma, al contrario, deve essere sottoposta ad una continua attività di controllo e revisione e deve essere allo stesso modo costantemente aggiornata.
TAGETIK SOFTWARE S.R.L., con il supporto dell'Organismo di Vigilanza provvederà pertanto a revisionare e integrare, ove occorra, la mappatura dei rischi ogni qual volta ciò si renda necessario in ragione di ulteriori interventi legislativi, di modifiche dell'assetto societario di TAGETIK SOFTWARE S.R.L., o anche solo in considerazione di modifiche delle circostanze e/o delle modalità con cui TAGETIK SOFTWARE S.R.L. svolge la propria attività d'impresa.

II) Articolazione di un sistema di controllo preventivo

Ai sensi dell'art. 6, comma 2 lett. b) del Decreto, una volta compiuta la mappatura dei rischi, occorre prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente nelle individuate aree di rischio.
A tal fine, nelle singole Parti Speciali del presente Modello sono indicate le specifiche misure definite (anche con rinvio a procedure interne espressamente precisate) in grado di prevenire o comunque ridurre fortemente il rischio di commissione dei reati.
In aggiunta a tali procedure, che hanno finalità preventiva, è espressamente riconosciuto all'Organismo di Vigilanza il potere/dovere di effettuare verifiche a posteriori su singole operazioni o singoli comportamenti aziendali.
Come la mappatura dei rischi, anche le procedure e i rimedi adottati non potranno mai dirsi definitivi: la loro efficacia e completezza devono, al contrario, essere oggetto di continua rivalutazione da parte dell'azienda e dell'Organismo

di Vigilanza, che ha anche il compito precipuo di proporre al Consiglio di Amministrazione i miglioramenti, le integrazioni e le modifiche che riterrà di volta in volta necessari.

III) Designazione dell'Organismo di Vigilanza.

Terza finalità della Parte Generale è l'individuazione di un Organismo di Vigilanza che provveda, in base al Decreto:
- al controllo costante del rispetto delle prescrizioni del Modello, nonché delle specifiche disposizioni e delle procedure predisposte in attuazione dello stesso, da parte di tutti i Destinatari;
- all'attività di valutazione costante e continuativa dell'adeguatezza della mappatura dei rischi e delle procedure descritte ai punti I) e II);
- alla proposta al Consiglio di Amministrazione di tutte le modifiche necessarie.

L'Organismo di Vigilanza è collegiale, interno a TAGETIK SOFTWARE S.R.L., ma del tutto autonomo e indipendente, come meglio precisato al punto 4 del presente Modello.

IV) Whistleblowing

Quarta finalità della parte generale è definire un sistema di garanzia della riservatezza delle segnalazioni e tutela dei segnalanti. Infatti, con la Legge n. 179 del 2017 (G.U. Serie Generale n. 291 del 14-12-2017), recante "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", il Legislatore ha apportato modiche all'articolo 6 del D.Lgs. 231/01 disponendo che il Modello di Organizzazione Gestione e Controllo deve prevedere:

a) uno o più canali che consentano alle persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso o da persone sottoposte alla loro direzione o vigilanza, di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali devono garantire la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;

b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;

c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;

d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

Ha disposto inoltre che l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui sopra può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. È onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

E' stato pubblicato recentemente in G.U. il D.Lgs. 24/2003 del 10 marzo 2023 n. 24 di "Attuazione della direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali".

Il presente modello organizzativo, al fine di rispondere risponde agli adempimenti previsti dal Decreto Whistleblowing, dalla Direttiva Whistleblowing e dal D.Lgs. n. 231/2001, recepisce la procedura Whisleblowing adottata da Wolters Kluwer Italia srl,

Tale Procedura si applica sia per la gestione delle Segnalazioni rilevanti ai sensi del Decreto Whistleblowing sia per la gestione delle Segnalazioni Ordinarie e si basa sui seguenti pilastri: (i) la protezione dalle Segnalazioni in malafede; (ii) la protezione del Segnalante; (iii) la tutela della riservatezza della Segnalazione.

Le persone coinvolte nella presente Procedura operano nel rispetto del sistema normativo e organizzativo, dei poteri e delle deleghe interne e sono tenute ad operare in conformità con le normative di legge ed i regolamenti vigenti e nel rispetto dei principi di seguito riportati:
CONOSCENZA E CONSAPEVOLEZZA – La Procedura rappresenta un elemento fondamentale al fine di garantire piena consapevolezza per un efficace presidio dei rischi e delle loro interrelazioni e per orientare i mutamenti della strategia e del contesto organizzativo.

PROTEZIONE DEL SEGNALATO DALLE SEGNALAZIONI IN "MALAFEDE" – Tutti i soggetti sono tenuti al rispetto della dignità, dell'onore e della reputazione di ciascuno. A tal fine, è fatto obbligo al soggetto Segnalante dichiarare se ha un interesse privato collegato alla Segnalazione. Più in generale, la Società garantisce adeguata protezione dalle Segnalazioni in "malafede", censurando simili condotte ed informando che le Segnalazioni inviate allo scopo di danneggiare o altrimenti recare pregiudizio, nonché ogni altra forma di abuso del presente documento sono fonte di responsabilità, in sede disciplinare e nelle altre sedi competenti. Nell'ambito delle Segnalazioni rilevante ai sensi del Decreto Whistleblowing i Soggetti Segnalati godono delle tutele previste dal Decreto Whistleblowing.

IMPARZIALITÀ, AUTONOMIA E INDIPENDENZA DI GIUDIZIO – Tutti i soggetti che ricevono, esaminano e valutano le Segnalazioni sono in possesso di requisiti morali e professionali e assicurano il mantenimento delle necessarie condizioni di indipendenza e dovuta obiettività, competenza e diligenza nello svolgimento delle loro attività.

L'OdV viene costantemente informato in merito alla gestione delle Segnalazioni sulla base delle previsioni di cui al paragrafo 8 della procedura Whistleblowing sopra richiamata.

L'OdV è destinatario del Report Semestrale Segnalazioni e delle relazioni periodiche (almeno su base annuale) di cui al paragrafo 10 della procedura Whistleblowing sopra richiamata.

L'OdV si occupa della gestione delle Segnalazioni ai sensi del paragrafo 8 della procedura Whistleblowing sopra richiamata, in presenza di conflitti di interesse da parte del Comitato Whistleblowing.

L'OdV, una volta ricevuta la relazione scritta conclusiva della Segnalazione, può decidere di svolgere ulteriori approfondimenti e valutazioni indipendenti anche mediante l'utilizzo del proprio budget.

3.4 Parti Speciali

Il presente Modello si articola, oltre che della Parte Generale come sopra descritta, anche di alcune Parti Speciali dedicate ciascuna ad una specifica categoria di Reati Presupposto, per i quali, sulla base della mappatura dei rischi effettuata ai sensi del Decreto, TAGETIK SOFTWARE S.R.L. ha ritenuto sussistere un rischio di commissione al suo interno.
Ogni Parte Speciale, oltre alla descrizione delle fattispecie delittuose esaminate, contiene l'individuazione delle aree aziendali ritenute particolarmente a rischio, nonché l'indicazione precisa delle procedure adottate per evitare o quanto meno ridurre la commissione degli illeciti.
Nelle Parti Speciali che seguono verranno pertanto esaminate le seguenti fattispecie:
i) Reati contro la Pubblica Amministrazione (Parte Speciale "A");
II) Reati informatici e trattamento illecito di dati nonché delitti in materia di diritto d'autore (Parte Speciale "B");
iii) reati c.d. societari e di corruzione tra privati (Parte Speciale "C");
iv) abusi di mercato (Parte Speciale "D");
v) omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche, sulla tutela dell'igiene e della salute sul lavoro (Parte Speciale "E");

vi) reati di riciclaggio, ricettazione e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (Parte Speciale "F")
vii) impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare (Parte Speciale "G")
viii) reati tributari (Parte Speciale "H")
All'esito della mappatura dei rischi effettuata inizialmente nel 2012, poi aggiornata nell'anno 2017 e, infine, nel presente anno 2020, TAGETIK SOFTWARE S.R.L. ha ritenuto di non ricomprendere nel presente Modello i reati con finalità di terrorismo o di eversione dell'ordine democratico così come quelli di criminalità organizzata, nonché i delitti contro l'industria e il commercio, i reati ambientali, le frodi sportive nonché l'esercizio abusivo del gioco d'azzardo e i reati di contrabbando – per i quali comunque è prevista la responsabilità amministrativa dell'Ente – in considerazione del fatto che non sussistono, per tali fattispecie, reali e concreti/significativi rischi di commissione di tali reati, tenuto conto delle specifiche attività aziendali svolte dalla Società.

3.5 L'attuazione del Decreto da parte di TAGETIK SOFTWARE S.R.L.

Alla luce della volontà di operare in modo trasparente e corretto, anche a presidio della propria reputazione aziendale, così come dei propri soci, amministratori, e dipendenti, TAGETIK SOFTWARE S.R.L. ha ritenuto opportuno, ed il linea con la propria filosofia aziendale, procedere all'adozione e all'attuazione del presente Modello, ed al suo successivo costante aggiornamento.
Il Modello ha anche il fine di sensibilizzare tutti i Destinatari, in modo da orientare a principi di correttezza e trasparenza il loro operare e, allo stesso tempo, evitare e prevenire ogni rischio di commissione di reati nell'ambito delle attività aziendali.
Il Modello è stato predisposto da TAGETIK SOFTWARE S.R.L. avendo come riferimento la propria specifica organizzazione, dimensione e struttura, le prescrizioni e le norme del Decreto, le pronunce giurisprudenziali in materia, nonché le Linee Guida elaborate dalle associazioni di categoria e, in particolare, quelle elaborate da Confindustria (nella versione pubblicata sul sito di Confindustria nel mese di marzo 2014).
Il presente Modello è stato adottato dal Consiglio di Amministrazione di Tagetik Software S.r.l con apposita delibera.
Inoltre il Consiglio di Amministrazione, ha nominato l'Organismo di Vigilanza, attualmente composto da nr. 2 membri e dotato di autonomi poteri, con compiti di vigilanza, controllo ed iniziativa in relazione al Modello stesso ed in particolare alla sua concreta applicazione, rispetto ed aggiornamento.

3.6 Mappatura dei rischi

Sulla base delle disposizioni del Decreto e delle indicazioni fornite dalle Linee Guida, TAGETIK SOFTWARE S.R.L. ha provveduto alla mappatura dei rischi, individuando, all'interno della propria realtà aziendale, le aree che risultano particolarmente al rischio di commissione di alcuno dei Reati Presupposto.
In questa sede, verrà brevemente illustrata la metodologia utilizzata per la mappatura dei rischi.
TAGETIK SOFTWARE S.R.L. ha anzitutto proceduto all'analisi degli elementi costitutivi dei Reati Presupposto, allo scopo di individuare e definire le condotte concrete che, all'interno delle attività aziendali, potrebbero realizzare le varie fattispecie delittuose.
In secondo luogo, TAGETIK SOFTWARE S.R.L. ha proceduto all'analisi della realtà aziendale, al fine di individuare le aree ed i settori maggiormente a rischio. L'individuazione di tali aree a rischio è stata compiuta inizialmente con il supporto di un avvocato e di un consulente esterno esperto in organizzazione aziendale appositamente incaricati allo scopo e analizzando la realtà di TAGETIK SOFTWARE S.R.L. sulla base di interviste agli Amministratori, ai Responsabili di Processo e all'analisi di alcuni documenti a campione di fra quanti utilizzati per la gestione delle attività aziendali. L'aggiornamento della mappatura dei rischi è stato attuato, nel 2016, con il supporto operativo dell'Organismo di Vigilanza.
Infine, TAGETIK SOFTWARE S.R.L. ha proceduto alla stesura, all'interno delle aree a rischio individuate nel corso dell'analisi valutativa iniziale, delle procedure e dei protocolli ritenuti opportuni al fine di assicurare l'adeguatezza e l'efficienza del modello in relazione alle disposizioni del Decreto. Gli esiti delle predette attività di mappatura dei rischi verranno dettagliatamente descritti nelle singole Parti Speciali, dove verranno anche illustrate le procedure e le misure predisposte da TAGETIK SOFTWARE S.R.L. al fine di evitare o comunque di ridurre al minimo il rischio di commissione dei Reati Presupposto.

3.7 Destinatari del Modello

Destinatari delle norme e delle prescrizioni contenute nel presente Modello, e tenuti, quindi, alla sua integrale osservanza, sono, in generale, tutti coloro che operano in nome e per conto di TAGETIK SOFTWARE S.R.L., ivi inclusi gli amministratori, i membri degli altri eventuali organi sociali, i dipendenti, i collaboratori anche occasionali, i partner commerciali, i fornitori, e i componenti dell'Organismo di Vigilanza.

4. ORGANISMO DI VIGILANZA

4.1 Identificazione dell'Organismo di Vigilanza

L'Organismo di Vigilanza di TAGETIK SOFTWARE S.R.L. è un organo interno dotato di autonomi poteri di iniziativa e di controllo con il compito di vigilare sul funzionamento e sull'osservanza del Modello e provvedere al relativo aggiornamento.
L'Organismo di Vigilanza di TAGETIK SOFTWARE S.R.L. è composto da due membri, da scegliersi tra soggetti dotati di comprovata competenza e professionalità, che, in occasione della prima riunione, adotteranno un apposito regolamento per il funzionamento dello stesso.
Alla luce delle esperienze maturate nella prassi, e nel rispetto delle disposizioni del Decreto, TAGETIK SOFTWARE S.R.L. ha ritenuto di individuare, quali componenti del proprio Organismo di Vigilanza, due professionisti esterni esperti delle tematiche del Decreto, ovvero un commercialista e revisore legale già in precedenza destinatario dell'incarico di Presidente del Collegio Sindacale di Tagetik Software Srl e un esperto di Organizzazione Aziendale con conoscenza pluriennale della società.
Tale soluzione è ritenuta da TAGETIK SOFTWARE S.R.L. la scelta ottimale, perché consente all'Organismo di Vigilanza di operare efficacemente, in considerazione proprio del fatto che è composto da membri esterni ma tali da conoscere in maniera approfondita tanto la struttura societaria e organizzativa di TAGETIK SOFTWARE S.R.L. quanto le modalità con cui la stessa svolge la propria attività d'impresa.
L'Organismo di Vigilanza è nominato dal Consiglio di Amministrazione di TAGETIK SOFTWARE S.R.L. e resta in carica per la durata indicata all'atto della nomina, o in mancanza di tale termine per tre anni. I suoi membri possono ricoprire la carica per più mandati, senza limite di mandati.
Costituiscono cause di ineleggibilità o di revoca quali componenti dell'Organismo di Vigilanza:
i) la condanna, anche con sentenza non definitiva o applicazione della pena su richiesta delle parti, per i delitti puniti a titolo di dolo, con l'esclusione quindi dei delitti colposi, eccettuati quelli previsti e puniti dagli articoli 589 e 590 comma 3 c.p., commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sui luoghi di lavoro, nonché le contravvenzioni che comportino l'applicazione di una pena accessoria di cui all'art. 19 c.p., o previste da specifiche disposizioni di legge;
ii) in ogni caso, qualsiasi condanna, anche non definitiva, che comporti l'applicazione di una pena accessoria di cui all'art. 19 c.p. o previste da specifiche disposizioni di legge;
iii) l'applicazione di una misura di sicurezza, personale o patrimoniale, l'applicazione di una misura di prevenzione personale o patrimoniale o l'applicazione di una misura di prevenzione antimafia personale o patrimoniale;
iv) la dichiarazione di interdizione o di inabilità ai sensi del codice civile, come pure il conflitto di interessi con TAGETIK SOFTWARE S.R.L..
Costituisce inoltre causa di sospensione dalla carica, per tutta la durata della misura, l'applicazione di una misura cautelare personale (custodia cautelare in carcere o in luogo di cura, arresti domiciliari, divieto e obbligo di dimora, obbligo di presentarsi alla Polizia Giudiziaria, divieto di espatrio) e l'applicazione di una misura interdittiva (sospensione dall'esercizio di un pubblico ufficio o servizio, divieto temporaneo di esercitare determinate attività professionali e imprenditoriali).
All'Organismo di Vigilanza ed ai suoi membri si applicheranno le norme del Codice civile in tema di mandato.

4.2 Prerogative e risorse dell'Organismo di Vigilanza

L'Organismo di Vigilanza potrà avvalersi della collaborazione di soggetti appartenenti alle diverse attività aziendali, qualora si rendano necessarie le loro conoscenze e competenze specifiche per particolari analisi, e per la valutazione di specifici passaggi operativi e decisionali dell'attività di TAGETIK SOFTWARE S.R.L..
In ogni caso, l'Organismo di Vigilanza avrà la facoltà, laddove si manifesti la necessità di avvalersi di professionalità non presenti al proprio interno, o comunque nell'organigramma di TAGETIK SOFTWARE S.R.L., di utilizzare la consulenza di professionisti esterni.

L'Organismo di Vigilanza, all'inizio del proprio mandato, e successivamente con cadenza annuale, potrà presentare al Consiglio di Amministrazione di TAGETIK SOFTWARE S.R.L. una richiesta di budget di spesa annuale da erogarsi da parte della stessa TAGETIK SOFTWARE S.R.L. ed in particolare:
• l'Organismo di Vigilanza presenterà al Consiglio di Amministrazione la richiesta di disponibilità dell'importo corrispondente al budget annuale con sufficiente dettaglio delle spese e dei costi da sostenere per il corretto adempimento del mandato;
• Il Consiglio di Amministrazione non potrà ragionevolmente rifiutarsi di provvedere all'erogazione di tale importo, fermo restando che l'Organismo di Vigilanza lo potrà utilizzare, in via autonoma e senza obbligo di preventiva autorizzazione, per gli scopi previsti dal presente Modello;
• tale importo dovrà coprire le spese che, secondo le stime, l'Organismo di Vigilanza dovrà sostenere nell'esercizio delle proprie funzioni (fermo restando che gli eventuali costi relativi alle risorse umane o materiali messi a disposizione da TAGETIK SOFTWARE S.R.L. non fanno parte del budget);
Qualora, in ragione di eventi o circostanze straordinarie (cioè al di fuori dell'ordinario svolgimento dell'attività dell'Organismo di Vigilanza) si rendesse necessaria per l'Organismo di Vigilanza la disponibilità di somme ulteriori rispetto all'importo sopra indicato, il Presidente dell'Organismo di Vigilanza dovrà formulare richiesta motivata al Consiglio di Amministrazione di TAGETIK SOFTWARE S.R.L. indicando con ragionevole dettaglio le ragioni ed i fatti posti a base di tale richiesta. La richiesta degli ulteriori fondi non potrà essere respinta dal Consiglio di Amministrazione senza fondato motivo.

4.3 Funzioni e poteri dell'Organismo di Vigilanza

All'Organismo di Vigilanza di TAGETIK SOFTWARE S.R.L. è affidato il compito di:
- vigilare sull'osservanza delle prescrizioni del Modello e dei documenti ad esso ricollegabili da parte dei Destinatari, assumendo ogni iniziativa necessaria;
- vigilare sulla reale efficacia, efficienza ed effettiva capacità delle prescrizioni del Modello, in relazione alla struttura aziendale, di prevenire la commissione dei Reati Presupposto;
- verificare l'opportunità di aggiornamento ed adeguamento delle procedure disciplinate dal Modello, formulando al Consiglio di Amministrazione le opportune relative proposte;
- segnalare al Consiglio di Amministrazione le violazioni accertate del Modello perché possa assumere i provvedimenti conseguenti.
Fermo restando l'obbligo di vigilanza sul rispetto del Modello e delle procedure ivi indicate attribuito all'Organismo di Vigilanza, il suo operato non è sindacabile da parte del Consiglio di Amministrazione, se non per motivi attinenti ad inadempimenti del mandato conferito.
In particolare, l'Organismo di Vigilanza di TAGETIK SOFTWARE S.R.L. realizzerà le predette finalità attraverso:
- le ricognizioni delle attività aziendali, ai fini della verifica periodica dell'attuazione di quanto previsto dal Modello nonché per aggiornamento della mappatura delle aree di rischio nell'ambito del contesto aziendale;
- la richiesta di informazioni periodiche o specifiche a singole funzioni aziendali in relazione alle attività considerate a rischio. Le informazioni richieste dall'Organismo di Vigilanza dovranno essere prontamente fornite a cura delle funzioni coinvolte senza omissioni o alterazioni di sorta per assicurare all'Organismo stesso una visione certa e concreta delle attività oggetto di monitoraggio; a tal fine si precisa anche che l'Organismo di Vigilanza deve ricevere costantemente informazioni sull'evoluzione delle aree di rischio, e ha libero accesso a tutta la relativa documentazione aziendale.
- il coordinamento con le altre funzioni aziendali (anche attraverso apposite riunioni) per il migliore monitoraggio delle attività nelle aree individuate a rischio di commissione dei reati presupposto;
- il coordinamento con i responsabili delle funzioni aziendali per i diversi aspetti attinenti all'attuazione del Modello;
- il controllo dell'effettiva presenza e della regolare tenuta della documentazione richiesta in conformità a quanto previsto nelle singole Parti Speciali del Modello per le diverse tipologie di reati;
- ogni altro controllo, sia periodico che mirato, sul concreto svolgimento di singole operazioni, procedure o attività all'interno di TAGETIK SOFTWARE S.R.L. che si renda opportuno;
Inoltre, l'Organismo di Vigilanza provvederà a:

- verificare l'adeguatezza delle norme in essere in relazione ad eventuali trasformazioni, modifiche ed allargamenti dell'attività aziendale;
- segnalare al Consiglio di Amministrazione le eventuali carenze del Modello e le relative proposte di modifica o miglioramento.
- curare conseguentemente l'aggiornamento delle norme di condotta delle singole Parti Speciali;
- verificare la validità delle clausole standard finalizzate all'attuazione di meccanismi sanzionatori (ad es. quelle di risoluzione dei contratti nei riguardi di partner commerciali, collaboratori o fornitori), se si accertino violazioni delle prescrizioni di cui al Decreto;

l'Organismo di Vigilanza dovrà predisporre una relazione informativa destinata al Consiglio di Amministrazione, con cadenza perlomeno annuale.

Infine, e conformemente alle disposizioni di cui all'art. all'art. 6, comma 1 lett. b) del Decreto, i compiti di monitoraggio e di aggiornamento del Modello assegnati all'Organismo di Vigilanza d il Modello si articolano su tre differenti tipi di verifiche:

- *verifiche sugli atti:* periodicamente l'Organismo di Vigilanza procederà a una verifica dei principali atti societari e di eventuali contratti di significativa rilevanza conclusi da TAGETIK SOFTWARE S.R.L. nell'ambito delle aree di rischio;
- *verifiche sulle procedure:* periodicamente l'Organismo di Vigilanza verificherà l'effettiva attuazione del presente Modello;
- *verifiche sulle segnalazioni e le misure:* l'Organismo di Vigilanza esaminerà ogni segnalazione ricevuta nel corso dell'anno, le azioni intraprese in proposito, gli eventi e gli episodi considerati maggiormente rischiosi, nonché l'effettività della conoscenza tra tutti i Destinatari del contenuto del Modello e delle ipotesi di reato per le quali è prevista la responsabilità amministrativa dell'ente.

Dei risultati di questa attività di verifica l'Organismo di Vigilanza dovrà dare conto, seppure sommariamente, nella relazione annualmente predisposta dall'Organismo di Vigilanza per il Consiglio di Amministrazione, il Collegio Sindacale e l'Assemblea dei Soci.

5. FLUSSI INFORMATIVI INTERNI

5.1 Comunicazioni e segnalazioni all'Organismo di Vigilanza

E' possibile contattare l'Organismo di Vigilanza di TAGETIK SOFTWARE S.R.L. mediante 3 modalità:

- Contatto personale con uno dei membri ed eventuale stesura congiunta di un documento diretto all'Organismo di Vigilanza
- Comunicazione @-mail alla casella di posta elettronica organismodivigilanza@tagetik.com
- segnalazioni scritte, anche eventualmente in forma anonima, in busta chiusa spedita all'indirizzo: Organismo di Vigilanza c/o Tagetik Software S.r.l., Via Roosevelt, 103 55100 LUCCA.

L'organismo di vigilanza è tenuto a condurre indagini interne in seguito a segnalazioni di eventuali violazioni del presente Modello e, qualora siano ritenute serie e fondate, a formulare pareri non vincolanti sulla tipologia e l'entità degli interventi da adottare nonché sulle possibili sanzioni nei confronti dei responsabili. L'attuazione degli interventi e delle possibili sanzioni sono a carico del Consiglio di Amministrazione che ne decide l'entità tenendo conto dei pareri e delle indicazioni dell'Organismo di Vigilanza. L'Organismo di Vigilanza è tenuto a garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione eventuali segnalanti in buona fede.

5.2 Obblighi informativi nei confronti dell'Organismo di Vigilanza

Oltre alla documentazione espressamente indicata da ogni singola Parte Speciale del Modello secondo le procedure in esse contemplate, dovrà essere portata a conoscenza dell'Organismo di Vigilanza ogni altra informazione attinente all'attuazione del Modello nelle aree di rischio, nonché quella relativa ad eventuali violazioni delle prescrizioni del Modello stesso.
Dovranno sempre essere comunicate all'Organismo di Vigilanza tutte le informazioni riguardanti:
- le decisioni relative alla richiesta, erogazione e utilizzo di finanziamenti pubblici;
- le richieste di assistenza legale inoltrate dai dipendenti (ivi inclusi i dirigenti) nei confronti dei quali la magistratura proceda per taluno dei Reati Presupposto;
- i provvedimenti e/o le notizie provenienti dalla Magistratura e dagli organi di Polizia Giudiziaria o da qualsiasi altra autorità, dai quali risulti lo svolgimento di indagini, anche nei confronti di ignoti, per fatti in cui siano potenzialmente interessate le attività aziendali di TAGETIK SOFTWARE S.R.L.;
- i risultati e le conclusioni di commissioni di inchiesta o altre relazioni interne dalle quali emergano ipotesi di responsabilità per i Reati Presupposto;
- notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello;
- procedimenti disciplinari svolti, eventuali sanzioni irrogate ovvero provvedimenti di archiviazione di tali procedimenti con relative motivazioni;
- prospetti riepilogativi degli appalti a seguito di gare pubbliche ovvero di trattative private;
- commesse attribuite da enti pubblici, dalla Comunità Europea o da soggetti che svolgano funzioni di pubblica utilità.
- infortuni e incidenti sul lavoro considerabili quali gravi o molto gravi (indicativamente con prognosi iniziale superiore a gg. 40)

Il Consiglio di Amministrazione è tenuto a dare piena informazione all'Organismo di Vigilanza sulle questioni che rientrano nella competenza dell'Organismo di Vigilanza medesimo.
Al fine di consentire all'Organismo di Vigilanza l'efficace adempimento dei compiti che gli sono demandati, TAGETIK SOFTWARE S.R.L. garantisce a tutti i Destinatari del Modello, nonché ad eventuali terzi, la facoltà di segnalare a tale organo qualsiasi illecito, anomalia o attività sospetta, in relazione alla commissione o al rischio di commissione di uno dei Reati Presupposto, di cui siano venuti a conoscenza per qualsivoglia ragione.
A tutti coloro che invieranno comunicazioni o segnalazioni all'Organismo di Vigilanza TAGETIK SOFTWARE S.R.L. garantisce espressamente l'esclusione di qualsiasi forma di ritorsione, discriminazione o penalizzazione, ed in ogni caso assicura la riservatezza sull'identità del segnalante.
Tutti i dipendenti della società hanno quindi la facoltà, oltre che il dovere, di comunicare, in forma scritta, ogni informazione relativa a possibili anomalie interne od attività illecite.
L'Organismo di Vigilanza potrà anche ricevere e valutare segnalazioni e comunicazioni, allo stesso modo scritte, provenienti da estranei alla società.

L'Organismo di Vigilanza potrà richiedere ogni genere di informazione e/o documentazione, utile agli accertamenti e ai controlli ad esso demandati, al Consiglio di Amministrazione ed ai dipendenti, facendo obbligo ai soggetti indicati di ottemperare con la massima cura, completezza e sollecitudine ad ogni richiesta dell'Organismo di Vigilanza.
L'Organismo di Vigilanza di TAGETIK SOFTWARE S.R.L. deve ricevere dal Consiglio di Amministrazione informazioni dettagliate circa eventuali modifiche dei poteri definiti e delle deleghe attribuite.
L'Organismo di Vigilanza verifica ed analizza le informazioni e le comunicazioni ricevute e i provvedimenti da attuare; una volta attuati, i provvedimenti dovranno essere in linea e conformi alle previsioni dettate dal sistema disciplinare del presente Modello.
L'Organismo di Vigilanza può richiedere al Consiglio di Amministrazione l'emissione di sanzioni disciplinari a carico di coloro che si sottraggono agli obblighi di informazione.
L'Organismo di Vigilanza comunicherà al Consiglio d'Amministrazione per le proprie determinazioni se, all'esito degli accertamenti svolti sulle comunicazioni e segnalazioni pervenute, le stesse furono redatte con dolo o colpa grave finalizzate al nocumento della società, dei propri amministratori, dirigenti e dipendenti.

5.3 Obblighi informativi dell'Organismo di Vigilanza nei confronti degli organi societari

L'Organismo di Vigilanza è tenuto a specifici obblighi informativi nei confronti del Consiglio di Amministrazione e dell'Assemblea dei Soci.
L'Organismo di Vigilanza avrà inoltre l'obbligo specifico di fornire tempestive informazioni su ogni modifica, integrazione o aggiornamento che possa interessare il Decreto. L'Organismo di Vigilanza ha altresì il dovere di comunicare al Consiglio di Amministrazione ogni violazione accertata nell'ambito dello svolgimento della propria attività.
L'Organismo di Vigilanza di TAGETIK SOFTWARE S.R.L. potrà essere convocato in qualsiasi momento dal Consiglio di Amministrazione o potrà a sua volta richiedere di essere da questo sentito, per riferire in merito al funzionamento del Modello o a situazioni specifiche.
Annualmente, inoltre, come già sopra definito, l'Organismo di Vigilanza trasmette al Consiglio di Amministrazione (e all'Assemblea dei Soci) una relazione scritta sull'attuazione del Modello.

5.4 Raccolta e conservazione delle informazioni

Le informazioni e i *report* predisposti o ricevuti in base al Decreto devono essere conservati a cura dell'Organismo di Vigilanza in un archivio apposito, informatico o cartaceo che, previa autorizzazione scritta dello stesso Organismo di Vigilanza, potrà essere reso accessibile a soggetti esterni in base a procedure da delineare a cura dello stesso Organismo di Vigilanza.
Tale documentazione sarà, ovviamente, a disposizione dell'Organismo di Vigilanza e di chiunque abbia interesse a prenderne visione.
Per propria scelta, l'Organismo di Vigilanza ha deciso di utilizzare un libro verbali a pagine vidimate

6. SISTEMA DISCIPLINARE

6.1 Principi generali

L'art. 6, comma 2 lettera e), del Decreto stabilisce che deve essere introdotto un sistema disciplinare idoneo a sanzionare le violazioni intervenute.
La definizione di un sistema disciplinare (da commisurarsi alla tipologia delle infrazioni) da applicarsi in caso di violazione delle previsioni del Modello, rende efficace l'azione di vigilanza e prevenzione affidata all'Organismo di Vigilanza e ha lo scopo di garantire l'efficacia del Modello stesso.
Il sistema disciplinare è stato redatto anche sulla base dei seguenti principi:
• differenziazione in base ai Destinatari del Modello;
• individuazione delle sanzioni disciplinari da adottarsi nei confronti dei destinatari nel rispetto delle disposizioni previste dai CCNL e delle prescrizioni legislative applicabili;
• individuazione di procedure di accertamento delle violazioni, infrazioni, elusioni, imperfette o parziali applicazioni, nonché di una apposita procedura di irrogazione delle sanzioni applicabili, individuando il soggetto preposto alla loro irrogazione ed in generale a vigilare sulla osservanza, applicazione ed aggiornamento del sistema disciplinare.
In particolare, il sistema disciplinare è rivolto:
- a tutti coloro che rivestono, anche di fatto, funzioni di rappresentanza, di amministrazione o di direzione (inclusi anche eventuali liquidatori) di TAGETIK SOFTWARE S.R.L. o di una sua unità organizzativa dotata di autonomia finanziaria e gestionale;
- alle persone sottoposte alla direzione o vigilanza di uno dei soggetti di cui sopra, ed in generale a tutti i dipendenti così come a tutti coloro che, a qualsiasi titolo ed ai vari livelli di responsabilità, operano nell'ambito di TAGETIK SOFTWARE S.R.L. concorrendo, con i propri atti, allo svolgimento della complessiva attività aziendale, compresi i collaboratori, i partner commerciali, i fornitori.
Il presente sistema disciplinare è suddiviso in sezioni specifiche ognuna riferita ad una categoria di destinatari, tenuto conto dello *status* giuridico dei diversi soggetti.
È affidato all'Organismo di Vigilanza il compito di sorvegliare sull'osservanza e sulla corretta applicazione del sistema disciplinare e sulla sua effettività, nonché di adottare gli opportuni provvedimenti affinché il Consiglio di Amministrazione di TAGETIK SOFTWARE S.R.L. provveda ad aggiornare, modificare e/o integrare il sistema disciplinare stesso.
L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, poiché le regole di condotta imposte dal Modello sono assunte dall'azienda in piena autonomia, indipendentemente dall'illecito penale che le stesse condotte possano integrare.
L'Organismo di Vigilanza potrà proporre al Consiglio di Amministrazione di TAGETIK SOFTWARE S.R.L. l'adozione di misure disciplinari commisurate all'entità ed alla gravità delle violazioni accertate.

6.2 Sanzioni disciplinari nei confronti dei dipendenti

Le condotte tenute dai lavoratori dipendenti in violazione delle singole regole di comportamento indicate nel presente Modello, costituiranno illeciti disciplinari.
Le sanzioni irrogabili nei riguardi dei lavoratori dipendenti rientrano tra quelle previste dal CCNL applicato in azienda, nel rispetto delle procedure previste dall'articolo 7 della Legge 30 maggio 1970, n. 300 (c.d. Statuto dei Lavoratori) ed eventuali normative speciali applicabili.
In particolare, la sanzioni irrogate, a seconda della gravità della violazione, potranno essere quelle previste dal CCNL del Commercio, nonché dal CCNL Dirigenti del Commercio.
Le sanzioni saranno irrogate, nel rispetto delle procedure previste dal CCNL applicabile, dal Consiglio di Amministrazione, di propria iniziativa o su proposta dell'Organismo di Vigilanza.
In materia di tutela della salute e della sicurezza nei luoghi di lavoro, l'applicazione di sanzioni disciplinari può essere proposta dal RSPP e/o dal Datore di lavoro.
Le misure disciplinari qui di seguito elencate, irrogabili nei confronti del personale non dirigente sono quelle previste dall'apparato sanzionatorio del CCNL e delle eventuali modifiche e rinnovi di tale contratto e saranno adottate tenuto conto:

- dell'intenzionalità del comportamento e del grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
- del comportamento complessivo del lavoratore con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo nei limiti consentiti dalla legge;
- delle mansioni del lavoratore;
- della posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- delle altre particolari circostanze che accompagnano la violazione disciplinare.

Restano ferme e si intendono qui richiamate, tutte le disposizioni di cui all'art. 7 della Legge 300/1970 in relazione sia all'esposizione dei codici disciplinari, ed in particolare all'obbligo di preventiva contestazione dell'addebito al dipendente, anche al fine di consentire allo stesso di approntare una idonea difesa e di fornire eventuali giustificazioni, nonché ai fini della rilevanza della recidiva.

Per cui, i provvedimenti disciplinari irrogabili nei confronti di detti lavoratori, nel rispetto delle disposizioni previste dall'art. 7 dello Statuto dei Lavoratori (L. 20 maggio 1970, n. 300) e delle eventuali normative speciali applicabili, sono quelli previsti dall'apparato sanzionatorio del CCNL del settore del commercio, e precisamente:

1. Biasimo inflitto verbalmente: si applica in caso di lieve inosservanza dei principi e delle regole di comportamento previsti dal Modello Organizzativo e/o dal Codice Etico, o in violazione delle procedure o norme interne.
2. Biasimo inflitto per iscritto: si applica nei casi di recidiva delle infrazioni di cui al precedente punto 1.
3. Multa in misura non eccedente l'importo di 4 ore della normale retribuzione: si applica in caso di inosservanza dei principi e delle regole di comportamento previste dal Modello Organizzativo e/o dal Codice Etico ovvero in caso di violazione delle procedure e norme interne, in misura tale da poter essere considerata ancorché non lieve, comunque, non grave, correlandosi detto comportamento ad una negligente inosservanza delle norme e/o delle procedure e/o delle direttive ed istruzioni impartite dalla direzione o dai superiori.
4. Sospensione dalla retribuzione e dal servizio per un massimo di giorni 10: si applica in caso di inosservanza dei principi e delle regole di comportamento previste dal Modello Organizzativo e/o Codice Etico ovvero in caso di violazione delle procedure e norme interne, in misura tale da essere considerata di una certa gravità, anche se dipendente da recidiva in qualsiasi illecito disciplinare sanzionato con la multa.
5. Licenziamento disciplinare senza preavviso e con le altre condizioni di ragione e di legge: si applica in caso di adozione, nell'espletamento delle attività ricomprese nelle Attività Sensibili, di un comportamento caratterizzato da notevole inadempimento delle prescrizioni e/o delle procedure e/o delle norme interne stabilite dal Modello Organizzativo e/o dal Codice Etico, anche se sia solo suscettibile di configurare uno dei reati o degli illeciti amministrativi sanzionati dal Decreto o, in caso di recidiva in un qualsiasi illecito disciplinare sanzionato con la sospensione.

In caso di inosservanza da parte dei dirigenti dei principi e delle regole di comportamento previsti dal Modello Organizzativo e dal Codice Etico ovvero in caso di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle Attività Sensibili, di un comportamento non conforme o non adeguato alle suddette prescrizioni, si provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti del Commercio. Costituisce illecito anche la mancata vigilanza del personale dirigente sulla corretta applicazione, da parte dei lavoratori gerarchicamente subordinati, delle regole e delle procedure previste dal Modello Organizzativo e dal Codice Etico, così come la diretta violazione degli stessi, o più in generale l'assunzione di comportamenti, tenuti nell'espletamento delle attività connesse alle proprie mansioni, che non siano conformi a condotte ragionevolmente attese da parte di un dirigente, in relazione al ruolo rivestito ed al grado di autonomia riconosciuto.

Il presente sistema disciplinare viene costantemente monitorato dall'OdV e dal Consiglio di Amministrazione. Il Modello Organizzativo e il Codice Etico sono considerati vincolanti per tutti i destinatari. Pertanto tali documenti e i loro eventuali successivi aggiornamenti vengono resi noti da parte della Società ai destinatari attraverso l'invio di una circolare interna secondo quanto previsto dall'art. 7 dello Statuto dei Lavoratori, ponendo in particolare evidenza le sanzioni collegate alle violazioni.

6.3 Misure nei confronti degli amministratori e dei sindaci

In caso di violazioni del Modello da parte degli amministratori di TAGETIK SOFTWARE S.R.L. l'Organismo di Vigilanza ne informerà l'intero Consiglio di Amministrazione e se ritenuto opportuno l'Assemblea dei Soci, che provvederanno ad assumere le opportune iniziative previste ai sensi della normativa vigente.

6.4 Misure nei confronti di collaboratori, partner commerciali e fornitori

Ogni comportamento posto in essere da collaboratori, da partner commerciali o da fornitori in contrasto con le linee di condotta indicate dal presente Modello e tale da comportare il rischio di commissione di un Reato Presupposto potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di *partnership*, la risoluzione del rapporto contrattuale, fatta salva la richiesta di risarcimento qualora da tale comportamento derivino danni a TAGETIK SOFTWARE S.R.L. come nel caso di applicazione da parte del Giudice delle misure previste dal Decreto.

7. DIFFUSIONE E CONOSCENZA DEL MODELLO

Presupposto perché il Modello possa costituire esimente della responsabilità amministrativa dell'Ente è la sua efficacia, nonché la sua concreta ed effettiva applicazione.
Condizione indispensabile per garantire il concreto e costante rispetto del Modello e delle procedure dallo stesso descritte è la conoscenza dello stesso da parte di tutti i Destinatari.
TAGETIK SOFTWARE S.R.L. ha pertanto adottato le iniziative che verranno descritte qui di seguito al fine di assicurare una corretta divulgazione del Modello non soltanto all'interno ma anche all'esterno della propria realtà aziendale.

7.1 Formazione del personale

TAGETIK SOFTWARE S.R.L. promuove la conoscenza del Modello tra tutti i Destinatari, che sono pertanto tenuti a conoscerne il contenuto, ad osservarlo e a contribuire alla sua migliore attuazione.
Ai fini dell'attuazione del Modello la formazione del personale (a cui vanno aggiunti anche i consulenti esterni) sarà articolata secondo le seguenti modalità:

- Formazione iniziale attraverso riunioni specifiche nel periodo immediatamente successivo all'approvazione del Modello e di ogni sua successiva revisione sostanziale.
- Diffusione di una nota informativa interna esplicativa del Modello e delle sue funzioni;
- Pubblicazione sul sito internet e nell'intranet di TAGETIK SOFTWARE S.R.L. del presente Modello e del Codice Etico ad esso collegato;
- Pubblicazione nell'intranet di TAGETIK SOFTWARE S.R.L. delle procedure interne collegate al presente Modello;
- Diffusione tramite circolare interna di materiale informativo dedicato all'argomento, con comunicazione costante e tempestiva di eventuali aggiornamenti e modifiche;
- Informativa in sede di assunzione.

7.2 Informazione dei collaboratori, dei partner commerciali e dei fornitori

TAGETIK SOFTWARE S.R.L. promuove la conoscenza e l'osservanza del Modello anche tra i partner commerciali, i collaboratori ed i fornitori, attraverso la pubblicazione del presente Modello nel sito internet aziendale.

7.3 Clausole contrattuali

Al fine di assicurare il rispetto delle prescrizioni e delle procedure di cui al presente Modello anche da parte di soggetti terzi che partecipano, anche in via indiretta, all'esercizio dell'attività di impresa di TAGETIK SOFTWARE S.R.L., la Società inserirà nei contratti e nelle lettere di incarico sottoscritti con partner commerciali, fornitori e collaboratori apposite clausole contrattuali attraverso le quali i sottoscrittori si impegneranno al rispetto delle norme del Modello, accettando altresì che la loro violazione possa costituire motivo di risoluzione del relativo contratto da parte di TAGETIK SOFTWARE S.R.L..
La Società ritiene infatti che tale rimedio contrattuale costituisca l'unico strumento che consenta di tutelare il rispetto delle procedure e dei principi elaborati dal Modello anche da parte di soggetti (quali i collaboratori, i partner commerciali ed i collaboratori) che, non sono esposti al rischio delle sanzioni disciplinari previste espressamente per i dipendenti.

PARTE SPECIALE "A"

Rapporti con la Pubblica Amministrazione

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

Per quanto concerne la presente Prima Parte Speciale, si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati negli artt. 24 e 25 del Decreto:

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

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

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

Tale ipotesi di reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione Europea.

In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316-bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato (di seguito descritta), nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

Concussione (art. 317 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio, abusando della propria posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli.

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

Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318-319 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere o ritardare atti del suo ufficio (determinando un vantaggio in favore dell'offerente).

L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetti denaro per garantire l'aggiudicazione di una gara).

Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

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

Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale rifiuti l'offerta illecitamente avanzatagli.

Corruzione in atti giudiziari (art. 319-ter)

Tale ipotesi di reato si configura nel caso in cui la Società sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere, un teste od altro funzionario).

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

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea), determinandolo a fornire una determinata prestazione patrimoniale.

Tale reato può realizzarsi, ad esempio, nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta), al fine di ottenere l'aggiudicazione della gara stessa.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)

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

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

Frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640-ter c.p.)

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto da parte dello Stato o di altro ente pubblico, arrecando danno a terzi.

In concreto, potrebbe, ad esempio, integrarsi il reato in esame qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

Frode nelle pubbliche forniture (art. 356 c.p.)

Il reato si configura laddove venga attuata una frode nel corso di erogazione di una fornitura (sia essa di prodotti e/o servizi) nei confronti dello Stato, di un ente locale o comunque di un soggetto della Pubblica Amministrazione, intendendo incluse anche le società a prevalente partecipazione pubblica.

Il reato presuppone la sussistenza di un contratto nell'ambito del quale vengono erogate forniture diverse da quelle pattuite. Trattandosi di dolo generico, non sono necessari raggiri né vizi della cosa fornita, ma è sufficiente la malafede nell'esecuzione del contratto.

Frode ai danni del Fondo europeo agricolo (art. 2. L. 23/12/1986, n.898)

Il reato si realizza quando chiunque, mediante l'esposizione di dati o notizie false, consegua indebitamente, per sé o per altri, aiuti, premi, indennità, restituzioni, contributi o altre erogazioni a carico totale o parziale del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale.

Peculato (art. 314 c.p.)

Il reato si configura qualora un pubblico ufficiale o l'incaricato di un pubblico servizio, si appropri di denaro o altri beni di proprietà altrui delle quali risulta in possesso o in disponibilità in ragione del suo ufficio o servizio.

Peculato mediante profitto dell'errore altrui (art. 316 c.p.)

Il reato si realizza qualora un pubblico ufficiale o l'incaricato di un pubblico servizio, nell'esercizio delle proprie funzioni riceva o trattenga denaro o ottenga altre utilità, giovandosi dell'errore altrui a favore di sé stesso o di terzi.

Abuso d'Ufficio (art. 323 c.p.)

Commette detto reato il pubblico ufficiale o l'incaricato di un pubblico servizio che, nello svolgimento delle proprie funzioni, procuri a se stesso o ad altri un indebito vantaggio patrimoniale ovvero arrechi ad altri un danno ingiusto, violando le norme di legge o i regolamenti dell'ente, o anche omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto.

2. Valutazione delle Aree di Rischio

A prescindere dal fatto che il rischio di commissione di delitti contro la Pubblica Amministrazione è presente in ogni attività di impresa (qualsiasi società infatti si trova, nel corso della propria ordinaria attività, ad interfacciarsi in più di un'occasione con differenti enti pubblici e per differenti ragioni quali in primis la costituzione della società, con riferimento agli adempimenti formali di iscrizione e di pubblicità richiesti), il rischio di illeciti nei confronti della Pubblica Amministrazione è stato ritenuto non irrilevante in TAGETIK SOFTWARE S.R.L. per il fatto che pur essendo la clientela di TAGETIK SOFTWARE S.R.L. costituita prevalentemente da società private, in alcuni casi i destinatari dei servizi di TAGETIK SOFTWARE S.R.L. sono aziende pubbliche e/o a prevalente partecipazione pubblica (es. aziende c.d. municipalizzate) a seguito di tale valutazione i principi etici nell'ambito della gestione dei rapporti con la pubblica amministrazione sono stati inseriti nel codice etico aziendale e sono state previste apposite procedure per la riduzione ed il controllo del rischio di illecito.

3. Individuazione delle attività a Rischio

I reati considerati, come detto, trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione (intesa in senso lato e tale da ricomprendere anche la Pubblica Amministrazione di Stati esteri, così come esponenti di enti privati o soggetti privati che tuttavia esercitano attività regolate da norme di diritto pubblico e, in generale, di pubblico interesse).
Sono pertanto da considerarsi a rischio tutte quelle attività aziendali che implichino l'instaurazione di un rapporto con la Pubblica Amministrazione (attività di rischio diretto).
Sono poi da considerarsi allo stesso modo a rischio le aree aziendali che, pur non implicando direttamente l'instaurazione di rapporti con la Pubblica Amministrazione, gestiscono strumenti di tipo finanziario e di pagamento e altre attività che potrebbero consentire di attribuire vantaggi e utilità a pubblici ufficiali (o a soggetti ad essi collegati) nella commissione di reati contro la Pubblica Amministrazione (attività di rischio indiretto).
Costituiscono, in particolare, aree di rischio indiretto (con riferimento alla possibilità che esse possano essere impiegate per la formazione di riserve occulte di danaro o da impiegare in ipotesi per illecite dazioni o per dissimulare simili illecite dazioni):

- le attività di amministrazione, finanza, contabilità e fiscale;
- le attività di pagamento, con riferimento all'ipotesi che i soggetti selezionati possano essere ricollegabili ad amministratori e pubblici ufficiali locali che quindi l'attribuzione dell'incarico possa essere la contropartita di un patto corruttivo o comunque di un illecito vantaggio;
- l'assegnazione di contratti di consulenza e prestazione professionale, in particolare quando il soggetto selezionato abbia operi a contatto con l'area amministrativa pubblica cui TAGETIK SOFTWARE S.R.L. si stia in quel momento rivolgendo;
- la selezione del personale;
- la nomina di dirigenti e di membri organi sociali.

4. Principi di comportamento nella gestione delle attività a rischio diretto

La presente Parte Speciale prevede l'espresso divieto - a carico di tutti i Destinatari - di:
I) porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto);
II) porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo o comunque presentarsi in modo non cristallino ed essere oggetto di fraintendimento;
III) porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.
Nell'ambito di ogni rapporto con la Pubblica Amministrazione è fatto divieto in particolare di:
a) effettuare elargizioni in denaro a pubblici funzionari;
b) distribuire omaggi e regali a funzionari pubblici italiani ed esteri (anche in quei Paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società. Sono consentiti eccezionalmente omaggi di esiguo valore quali *gadgets* e prodotti espressamente approvati da TAGETIK SOFTWARE S.R.L..
c) accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al precedente punto b);
d) effettuare prestazioni in favore dei partner commerciali che intrattengono rapporti con la pubblica amministrazione e che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con i partner stessi;
e) riconoscere compensi in favore dei collaboratori che operano a contatto con la pubblica amministrazione e che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere;
f) presentare dichiarazioni non veritiere o incomplete o parziali a organismi pubblici nazionali o comunitari al fine di risultare assegnatari di gare pubbliche o di ottenere contratti da parte di aziende pubbliche e/o a prevalente partecipazione pubblica, conseguire erogazioni pubbliche, contributi o finanziamenti agevolati o qualsiasi altro risultato;
g) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.

La gestione di ogni rapporto con la Pubblica Amministrazione deve essere improntata ai principi fondamentali elencati nel Codice Etico aziendale e deve sempre prevedere le seguenti caratteristiche:
- *formalità*: è opportuno seguire sempre le procedure formali previste dalle norme del procedimento amministrativo ed evitare quanto più possibile rapporti informali, men che meno confidenziali con esponenti di pubbliche amministrazioni;
- *tracciabilità*: è necessario lasciare tracce scritte delle principali fasi e dei contatti nel corso di un procedimento amministrativo.
- *controllo:* le attività di partecipazione a gare, ottenimento di contratti ed erogazione di servizi vs. la pubblica amministrazione deve essere verificata preventivamente e durante la sua erogazione da parte delle funzioni ad esso deputate e per quanto necessario, da parte dell'Organismo di Vigilanza.

5. Principi di comportamento nella gestione delle attività a rischio indiretto

Come detto, il Modello deve prevedere ulteriori controlli su alcune aree di attività che possono fornire l'occasione per predisporre somme di denaro da impiegare a scopi corruttivi o di conferire incarichi e vantaggi che possono mascherare illecite dazioni. In particolare:

- Partecipazione a bandi di gare pubbliche e/o stipula di contratti con aziende a prevalente partecipazione pubblica

Ogni partecipazione a gare pubbliche così come l'ottenimento di contratti da parte di aziende pubbliche e/o a prevalente partecipazione pubblica e la relativa esecuzione dei servizi deve avvenire con scrupolosa attenzione alla trasparenza, al rispetto delle regole di correttezza e veridicità delle dichiarazioni

- Attività di gestione dei pagamenti

L'attività di pagamento segue l'apposita procedura interna che implica l'intervento e/o l'autorizzazione di almeno due soggetti. Nessuna fattura, con la sola esclusione di quelle di importi esigui può essere o pagata con modalità diverse rispetto alla procedura prevista.

- Selezione del personale

La selezione del personale è compiuta dalla funzione interessata in accordo con il Responsabile Risorse Umane, nel rispetto della relativa procedura interna.

- Incarichi a consulenti e professionisti esterni

Gli incarichi a liberi professionisti, consulenti e collaboratori esterni sono assegnati con lettera di incarico e/o contratto scritto, che ne indica il contenuto e l'importo degli onorari riconosciuti. Il coinvolgimento di consulenti e professionisti esterni deve anche prevedere, in forma preventiva, la verifica del fornitore, così come previsto dall'apposita procedura relativa alla gestione dei servizi vs. la Pubblica Amministrazione.

6. Procedure e documenti interni di riferimento

In relazione alla presente parte speciale sono di riferimento le seguenti procedure e documenti interni:

1- Codice Etico
2- Procedura Acquisti IT
3- Procedura Acquisti Marketing
4- Procedura Acquisti Beni e Servizi
5- Procedura Gestione procacciatori
6- Procedura Commerciale
7- Procedura Pagamenti e rimborsi spese
8- Procedura HR
9- Procedura gare d'appalto ed erogazione dei servizi nella Pubblica Amministrazione

Tali procedure sono da considerarsi integrative ed esplicative delle prassi definite nella presente Parte Speciale.

PARTE SPECIALE "B"

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

1. La tipologia degli illeciti informatici rilevanti (art. 24-bis del Decreto)

La legge n. 48 del 2008 ha ratificato e dato esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001.
La legge n. 48 ha introdotto nel codice penale una serie di nuove fattispecie di reato.
Al tempo stesso, ha introdotto nel Decreto l'art 24-*bis*, che ha stabilito la responsabilità amministrativa degli Enti anche nel caso di commissione di delitti informatici nel loro interesse o a loro vantaggio.
Questo, in particolare, il testo della norma: "*(Delitti informatici e trattamento illecito di dati). – 1.* In relazione alla commissione dei delitti di cui agli articoli 615-*ter*, 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote. *2.* In relazione alla commissione dei delitti di cui agli articoli 615-*quater* e 615-*quinquies* del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote. *3.* In relazione alla commissione dei delitti di cui agli articoli 491- *bis* e 640-*quinquies* del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote. *4.* Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere *a)*, *b)* ed *e)*. Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere *b)* ed *e)*. Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere *c), d)* ed *e)*".
Si provvede ad una breve descrizione degli illeciti indicati in questa norma.
Accesso abusivo ad un sistema informatico (art. 615-ter c.p.)
La norma sanziona il fatto di chi, similmente a quanto avviene per la violazione fisica del domicilio, si introduce abusivamente o si trattiene contro la volontà espressa dell'avente diritto in un sistema informatico protetto da misure di sicurezza.
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
La norma si riferisce al fatto di chi fraudolentemente intercetta comunicazioni telematiche o volontariamente le interrompe e le impedisce.
Installazione di apparecchiature atte ad intercettare impedire o interrompere comunicazioni telematiche (art. 617-quinquies)
La norma, anticipando la tutela della riservatezza delle comunicazioni telematiche, sanziona la mera installazione di apparecchiature atte ad intercettare, anche quando non sia seguita da alcuna effettiva attività di intercettazione, interruzione o impedimento.
Fattispecie di danneggiamento (635-bis – 635-quinquies c.p.)
Gli art. 635-bis e seguenti sanzionano una serie articolata di fattispecie che hanno il proprio elemento comune in condotte di danneggiamento volontario di dati e sistemi informatici.
L'art. 635-bis, anzitutto, sanziona il danneggiamento volontario programmi o dati informatici. La norma sanziona infatti chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui con la reclusione da sei mesi a tre anni.
L'art. 635-ter colpisce più gravemente chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.
L'art. 635-quater colpisce il danneggiamento di sistemi informatici o telematici ed in particolare il fatto di chi, ponendo in essere una delle condotte di cui all'art. 635-bis finalizzate al danneggiamento di programmi e dati, danneggia più in generale il funzionamento di un intero sistema informatico.
L'art. 635-quinquies colpisce ancor più gravemente i fatti di cui all'art. precedente se relativi a sistemi di pubblica utilità.
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematica (art. 615-quater c.p.)

La norma sanziona la condotta di chi, al fine di ottenerne un profitto od arrecare un danno, diffonde, comunica, consegna, riproduce o si procura codici, parola chiave o altri mezzi idonei a consentire l'accesso ad un sistema informatico protetto da misure di sicurezza.

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-quinquies c.p.)

La norma sanziona la condotta di chi diffonde cd. virus informatici, ossia programmi destinati ad entrare in sistemi informatici e ad impedirne o danneggiarne il funzionamento a produrre la distruzione dei dati in esso contenuti.

Falsità in documenti informatici (art. 491-bis c.p.)

La norma in questione estende le fattispecie di reato previste dal capo dedicato alle falsità in atti, ai casi in cui esse si realizzino su documenti di tipo informatico.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.)

L'articolo sanziona il fatto del soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Relativamente al diritto d'autore la Legge 99/09 del 23 luglio 2009 "Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia"ha introdotto nel D.Lgs. 231/01 il seguente dettato normativo:

("Delitti in materia di violazione del diritto d'autore") In relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a-bis), e terzo comma, 171-bis, 171-ter, 171- septies e 171-octies della legge 22 aprile 1941, n. 633, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.

2. Nel caso di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore ad un anno. Resta fermo quanto previsto dall'articolo 174- quinquies della citata legge n. 633 del 1941.

Si provvede ad una breve descrizione degli illeciti indicati in questa norma.

Diffusione in tutto o in parte di un'opera dell'ingegno protetta attraverso l'utilizzo di reti telematiche (art. 171, i comma, lettera a-bis della legge 633/1941)

La fattispecie di reato in oggetto si concretizza quando un soggetto viola il diritto di autore, diffondendo - attraverso l'utilizzo di reti telematiche – in tutto o in parte opere dell'ingegno protette.

Gestione abusiva di programmi per elaboratori e di banche dati protette (art. 171- bis della legge 633/1941)

Il reato in questione si realizza quando, al fine di trarne profitto, sono integrate condotte finalizzate a duplicare abusivamente, importare, distribuire, vendere, concedere in locazione, diffondere/trasmettere al pubblico, detenere a scopo commerciale - o comunque per trarne profitto - programmi per elaboratori e contenuti di banche dati protette.

Gestione abusiva di opere a contenuto letterario, musicale, multimediale, cinematografico, artistico (art. 171- ter della legge 633/1941)

Il reato in questione si realizza quando, al fine di lucro, sono integrate condotte finalizzate a duplicare abusivamente, importare, distribuire, vendere, noleggiare, diffondere/trasmettere al pubblico, detenere a scopo commerciale - o comunque per trarne profitto - qualsiasi opera protetta dal diritto d'autore e da diritti connessi, incluse opere a contenuto letterario, musicale, multimediale, cinematografico, artistico.

Gestione impropria di supporti esenti da obblighi di contrassegno ovvero non assolvimento fraudolento degli obblighi di contrassegno (art. 171-septies della legge 633/1941)

Il reato in questione si realizza quando i produttori o importatori dei supporti non soggetti al contrassegno SIAE, non comunicano alla stessa società entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi ovvero quando questi soggetti dichiarano falsamente di aver assolto agli obblighi di contrassegno.

Gestione abusiva o comunque fraudolenta di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato (art. 171- octies della legge 633/1941)

Il reato in questione si realizza quando, a fini fraudolenti, sono integrate condotte finalizzate a produrre, porre in vendita, importare, promuovere, installare, modificare, utilizzare per uso pubblico e privato 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.

2. Aree a rischio

Devono ritenersi, astrattamente, aree a rischio, tutte le attività di soggetti che accedono, nell'ambito delle loro competenze aziendali, alla rete informatica e ne facciano uso.
In concreto, la tipologia delle fattispecie delittuose in esame consente di limitare le possibili attività illecite nell'interesse di TAGETIK SOFTWARE S.R.L. o di sue controllate alle seguenti attività:
- alterazioni e falsificazioni di documenti elettronici pubblici o privati;
- attività di spionaggio o sabotaggio per via informatica dirette a concorrenti, pubblici o privati (creazione, modifica, alterazione di dati altrui; accesso abusivo in altrui sistemi; modifiche non autorizzate e programmi altrui e loro danneggiamento; detenzione indebita di *password* di accesso a sistemi altrui; intercettazione fraudolenta di altrui comunicazioni informatiche; installazione di dispositivi volti a tale illecita attività; diffusione di virus…).
- divulgazione di software privi delle necessarie licenze e conseguentemente violazione delle norme sul diritto d'autore
Vista la natura delle società di TAGETIK SOFTWARE S.R.L. operanti primariamente (e in modo pressoché esclusivo) nel settore informatico, nonché a contatto diretto con Banche Dati e, in generale, con la struttura informatica dei clienti, l'avvenimento di delitti in tali aree è stata valutata rilevante, in sede di analisi e mappatura del rischio.

3. Regole di condotta e procedure

In generale, tutti i Destinatari:
- devono impiegare la rete informatica aziendale esclusivamente per scopi, operazioni e comunicazioni professionali;
- devono accedere connettersi e scambiare dati con reti informatiche di terzi solo per ragioni professionali, nei casi e per il tempo strettamente necessari;
- devono tutelare i dati dei clienti di cui possono entrare in possesso per ragioni di sviluppo delle attività e devono mantenere su di essi il più stretto riserbo in base agli accordi di riservatezza stipulati con la società cliente e anche all'eventuale termine dei rapporti commerciali con il cliente stesso.
- devono tutelare gli strumenti informatici, i dati aziendali e i dati dei clienti in ogni situazione considerando incluse le eventuali attività svolte presso i clienti stessi nonché l'utilizzo e la tutela dei PC portatili e degli altri dispositivi mobili.
- devono evitare di utilizzare software e più in generale programmi per elaboratore in violazione delle norme sul diritto d'autore
- devono provvedere a comunicare al Responsabile IT e/o alla Direzione Aziendale qualsiasi fatto, evento, anomalia che possa rendere fondato il sospetto che sia in corso un abuso informatico
Con riferimento alla tipologia dei reati di cui alla presente Parte Speciale, una loro reale prevenzione può e deve fondarsi su due punti:
- la certa identificazione dell'identità del soggetto che di volta in volta accede ed agisce sulla rete informatica;
- idonee misure di prevenzione di accessi alla rete da parte di soggetti terzi e non titolati, perché sia escluso che taluno possa agire in modo anonimo sulla rete informatica aziendale.
- il periodico controllo della liceità dei software installati nei PC e nella rete informatica aziendale
Su questi punti, vi è da rilevare che TAGETIK SOFTWARE S.R.L. mantiene volontariamente un Documento Programmatico della Sicurezza nonché si è dotata di un Sistema di Gestione della Sicurezza delle Informazioni ai sensi della norma UNI CEI ISO/IEC 27001:2013 (certificato dall'Organismo di parte terza DEKRA CERTIFICATION S.r.l.), in cui sono stati indicate tutte le misure di sicurezza atti a prevenire accessi abusivi (fisici o informatici) ai dati sensibili che sono trattati dall'azienda: a quelle misure, documenti e sistemi (in quanto compatibili con l'aspetto dell'accesso e della sicurezza della rete informatica), la Parte Speciale fa rinvio, rendendole parte integrante anche del presente Modello.

Inoltre sono stati individuati a livello Direzionale, Amministratori Delegati con specifici poteri in fatto di tutela dei dati rispettivamente nelle fasi di consulenza e nelle fasi di elaborazione del software.

4. Procedure e documenti interni di riferimento

In relazione alla presente parte speciale sono di riferimento le seguenti procedure e documenti interni:

- Tutte le procedure e i documenti del sistema di gestione della sicurezza delle informazioni ai sensi della norma UNI CEI ISO/IEC 27001:2013
- Documento Programmatico della Sicurezza
- Regolamento informatico aziendale

Tali procedure e documenti sono da considerarsi integrative ed esplicative delle prassi definite nella presente Parte Speciale.

PARTE SPECIALE "C"

I Reati societari

1. Introduzione

Il D. Lgs. n. 61 del 2002 ha riformato la materia dei cd. reati societari, riformulando gli artt. 2621 e ss. c.c. Lo stesso decreto ha introdotto nel testo del Decreto l'articolo (art. 25-*ter*), che ha esteso la configurabilità della responsabilità amministrativa degli Enti anche al caso di commissione di *"reati in materia societaria previsti dal codice civile, se commessi nell'interesse della società, da amministratori, direttori generali o liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si fosse realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica".*

2. La tipologia dei Reati societari

Si provvede qui di seguito a fornire una breve descrizione dei principali reati rilevanti ai fini della presente Seconda Parte Speciale.

2.1 IPOTESI DI FALSITÀ

False comunicazioni sociali (artt. 2621 e 2622 c.c.)

Le fattispecie delineate dagli artt. 2621 e 2622 c.c. mirano a colpire l'esposizione, nelle comunicazioni sociali previste dalla legge, di false notizie o l'omissione di notizie dovute da parte di amministratori, direttori generali, sindaci e liquidatori, in modo tale da indurre in inganno i destinatari delle comunicazioni stesse.

La condotta, perché sia penalmente rilevante, deve essere posta in essere con il duplice intento di ingannare i soci, i creditori o il pubblico, da un lato, e di ottenere per sé o per altri un ingiusto profitto, dall'altro.

Falso in prospetto (art. 2623 c.c.)

La fattispecie individuata dall'art. 2623 è posta a tutela della veridicità e della completezza delle informazioni indirizzate al mercato, nei casi in cui la società voglia sollecitare l'investimento o voglia procedere alla quotazione su mercati regolamentati ovvero a offerte pubbliche di acquisto o di scambio. La norma, infatti, sanziona la condotta di chi, in tali occasioni, diffonda false informazioni, o ne occulti di vere, con l'intento di indurre in errore il pubblico.

Anche in questo caso, come nel precedente, la condotta non solo deve essere indirizzata allo scopo di ingannare i destinatari delle informazioni, ma deve anche mirare a produrre un ingiusto profitto per il soggetto attivo o per altri soggetti.

Anche in questo caso, il reato si configura come contravvenzione o delitto a seconda che dalla condotta sia derivato o meno un danno patrimoniale ai destinatari del prospetto informativo.

Falsità nelle relazioni e nelle comunicazioni della società di revisione (art. 2624 c.c.)

In questo caso, tutelate sono la veridicità e la completezza delle comunicazioni dei soggetti incaricati della revisione contabile della società.

Come in precedenza, se dalla condotta è scaturito un danno patrimoniale ai destinatari delle comunicazioni la sanzione è aggravata e il reato da contravvenzione diviene delitto.

Il reato di cui all'art. 2624 è reato proprio, potendo essere commesso dai soggetti responsabili della revisione contabile; ciò non toglie che gli amministratori e tutti gli altri soggetti indicati dall'art. 25-*ter* del Decreto, vi possano essere coinvolti a titolo di concorso.

2.2 TUTELA DEL CAPITALE SOCIALE

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

La norma risulta violata quando, fuori dai casi di legittima riduzione del capitale sociale, vi sia la restituzione, anche simulata, dei conferimenti a uno o più soci o la liberazione di uno di essi dall'obbligo di eseguirli.

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

La condotta individuata dalla norma è integrata quando vi sia la ripartizione di utili o di acconti su utili non effettivamente conseguiti o destinati dalla legge a riserva, ovvero sia ripartita altra riserva che per legge non potrebbe essere ripartita.

La norma prevede tuttavia che la restituzione degli utili o la reintegrazione delle riserve prima del termine per l'approvazione del bilancio d'esercizio estinguono il reato.

Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)

Il reato si perfeziona con l'acquisto o la sottoscrizione di azioni o quote sociali della società o della società controllante che intacchi l'integrità del capitale sociale o delle riserve non distribuibili.
Come nel caso dell'illegale ripartizione degli utili, la ricostituzione del capitale sociale o delle riserve prima del termine per l'approvazione del bilancio d'esercizio estinguono il reato.
Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
La fattispecie tutela la garanzia dei creditori e vieta il compimento di operazioni come la riduzione del capitale, la fusione con altra società o la scissione, quando esse provochino un danno ai creditori della società.
Qualora, prima del giudizio, intervenga il risarcimento del danno da essi patito, il reato si estingue.
Omessa comunicazione del conflitto di interessi (2629 bis c.c.)
La norma è stata introdotta dalla L. 262/2005 contenente le "*Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari*".
L'art 2629 *bis* del codice civile prevede la violazione dell'art. 2391, 1 comma, c.c. (che sancisce l'obbligo di comunicazione del conflitto di interessi) realizzata dagli amministratori di una società con titoli ammessi alla negoziazione in mercati regolamentari o diffusi tra il pubblico in misura rilevante ovvero da un soggetto sottoposto a vigilanza ai sensi del TUF.
Formazione fittizia del capitale (art. 2632 c.c.)
La norma prevede tre possibili condotte, accomunate dal medesimo effetto di provocare la formazione di quote fittizie di capitale:
- attribuzione di quote o azioni sociali per una somma inferiore al loro valore nominale;
- sottoscrizione reciproca di azioni o quote;
- sopravvalutazione rilevante di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.
Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)
Tale fattispecie riguarda il caso in cui, in fase di liquidazione, i liquidatori provvedano a ripartire i beni sociali tra i soci prima del pagamento dei creditori o dell'accantonamento della somme necessarie per la loro soddisfazione, con conseguente danno per i creditori stessi.
Il reato è estinto se, prima del giudizio, vi sia il risarcimento.

2.3 TUTELA DEL CORRETTO FUNZIONAMENTO DELLA SOCIETÀ
Impedito controllo (art. 2625 c.c.)
Il reato consiste nell'ostacolare le attività di controllo che la legge attribuisce a determinati soggetti – soci, organi sociali, eventuale società di revisione – attraverso l'occultamento di documenti o altri idonei artifici.
La concreta causazione di un danno comporta un aggravamento della sanzione.
Corruzione tra privati (art. 2635 c.c.)
Il reato consiste nella dazione di denaro e/o utilità (anche solo promessa) che comporti una violazione degli obblighi d' ufficio o di fedeltà, cagionando danno alla società.
Illecita influenza sull'assemblea (art. 2636 c.c.)
La norma individua e sanziona la condotta di chi, con atti simulati o con frode, determini la formazione della maggioranza assembleare, per procurare a sé o ad altri un ingiusto profitto.

2.4 TUTELA CONTRO LE FRODI
Aggiotaggio (art. 2637 c.c.)
La fattispecie prevista dall'art. 2637 è integrata dalla condotta di chi diffonda notizie false ovvero ponga in essere operazioni simulate o altri artifici concretamente idonei a influenzare in modo sensibile il prezzo di strumenti finanziari non quotati oppure incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o di gruppi bancari.
È opportuno sottolineare espressamente che la norma, a far data dal 2005, sanziona solo le condotte di aggiotaggio che influiscono sul valore di titoli non quotati. Da quell'anno, infatti il legislatore ha introdotto gli artt. 184 e 185 nel TUF, con cui ha separatamente disciplinato gli abusi di mercato su titoli di società quotate. La stessa legge, ha introdotto un nuovo art. 25 *sexies* nel Decreto, con cui è stata espressamente prevista la responsabilità amministrativa degli Enti anche per queste due nuove figure di reati.
A queste due fattispecie di abuso di mercato sarà dedicata la successiva Parte Speciale "D".

2.5 TUTELA DELLE FUNZIONI PUBBLICHE DI VIGILANZA

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)

La norma prevede due differenti condotte, distinte per modalità di condotta e momento offensivo.

La prima si realizza o con l'esposizione di fatti materiali non rispondenti al vero sulla situazione patrimoniale, economica e finanziaria, anche se oggetto di valutazione, nelle comunicazioni previste dalla legge nei confronti di Autorità Pubbliche di Vigilanza o con l'occultamento di fatti, sempre relativi alla situazione economica, patrimoniale e finanziaria, che avrebbero dovuto essere comunicati.

La seconda si realizza con ogni altra forma di ostacolo, attuata consapevolmente, alle attività di vigilanza delle Autorità Pubbliche.

3. Aree a Rischio

Alla luce dei reati e delle condotte sopra richiamate, l'analisi delle attività di impresa di TAGETIK SOFTWARE S.R.L. ha rivelato l'esistenza di un modesto rischio di commissione dei reati societari descritti.

TAGETIK SOFTWARE S.R.L. non è una società quotata, non ricorre al pubblico risparmio, non è sottoposta alla relativa Autorità Pubblica di Vigilanza (CONSOB): questi dati escludono l'esistenza di un rischio specifico di commissione di quelli, tra gli illeciti indicati, relativi a questi profili (prospetti, rapporti con il mercato, rapporti con Autorità di Vigilanza).

I rischi di commissione di illeciti societari, si ricollegano, quindi, a quelli fisiologici esistenti in ogni persona giuridica che eserciti attività di impresa e sono, in particolare individuabili nelle seguenti aree di attività:

A) attività di predisposizione di comunicazioni dirette ai soci o al pubblico e, in particolare, redazione e predisposizione del bilancio d'esercizio; In particolare, va però anche in tale caso sottolineato che i soci coincidono sostanzialmente con gli amministratori e pertanto anche tale ipotesi di reato risulta ridotta.

B) operazioni che incidono sul capitale sociale e di gestione della *corporate governance*;

C) attività di promozione commerciale e gestione dei rapporti commerciali in genere, anche tra privati

L'elenco è suscettibile di ogni integrazione futura; sarà, quindi, sempre possibile l'individuazione di ulteriori aree di rischio (con conseguente predisposizione di norme comportamentali specifiche e di relative procedure).

A tal proposito, l'Organismo di Vigilanza potrà proporre al Consiglio di Amministrazione ogni opportuno intervento sul testo della presente Parte Speciale. Il Consiglio di Amministrazione potrà, peraltro, assumere in autonomia analoghe iniziative.

Oltre alle specifiche indicazioni e principi di comportamento che di seguito saranno indicati, resta fermo il richiamo a tutti i principi generalmente accolti da TAGETIK SOFTWARE S.R.L. nonché dalla Parte Generale del presente Modello.

4. Regole di comportamento generali

Ai Destinatari è fatto espresso obbligo:

- di tenere un comportamento corretto, scrupolosamente trasparente e collaborativo, nel rispetto delle norme di legge e di tutte le procedure aziendali, in tutte le attività correlate e finalizzate alla preparazione del bilancio e della altre comunicazioni sociali, con lo scopo di fornire sempre ai soci e ai terzi un'informazione veritiera, completa e corretta sulla situazione economica, finanziaria e patrimoniale di TAGETIK SOFTWARE S.R.L. nel suo complesso;
- porre la massima attenzione e cautela, attraverso il rispetto delle norme di legge e delle procedure interne a essa indirizzate, alla tutela dell'integrità ed effettività del capitale e del patrimonio sociali, nel rispetto totale delle garanzie dei creditori e dei terzi in genere;
- aver cura e tutelare il regolare funzionamento degli organi sociali di TAGETIK SOFTWARE S.R.L., garantendo e agevolando ogni forma di controllo sulla gestione sociale e garantendo la libera formazione della volontà assembleare;
- aver cura di effettuare, nella piena veridicità, con tempestività e correttezza, tutte le comunicazioni previste dalla disciplina applicabile nei confronti delle Autorità competenti, evitando di frapporre qualsivoglia ostacolo all'esercizio delle loro attività di controllo e verifica;

- non diffondere notizie in merito alle iniziative e le scelte di partner commerciali (conclusione di accordi da parte di TAGETIK SOFTWARE S.R.L., collaborazioni con la Società e quant'altro), se non quando strettamente necessarie e con l'accordo del partner stesso.
- attuare prassi di etica nei rapporti commerciali atte a evitare il possibile reato di corruzione tra privati

5. Regole di comportamento particolari, relative alle specifiche aree di Rischio

5.1 Comunicazioni ai Soci e al pubblico

Bilanci ed altre comunicazioni sociali

TAGETIK SOFTWARE S.R.L. ha elaborato una specifica procedura per la redazione del proprio bilancio di esercizio, in cui sono state individuate tutte le funzioni aziendali e quindi i soggetti che devono contribuire a tale attività.
Le Funzioni coinvolte sono:
• amministrazione di gruppo;
• amministratori delle società italiane ed estere;
• • consulente fiscale esterno.
La Società risulta inoltre dotata di uno scrupoloso sistema di controllo che consente di monitorare, in tempo reale, la situazione contabile di TAGETIK SOFTWARE S.R.L., e consente pertanto di ritenere che, riguardo a questi, il rischio della commissione di taluno dei reati in esame sia fortemente ridotto.

5.2 Tutela del Capitale Sociale

Tutte le operazioni che, anche indirettamente, possono influire sul capitale sociale di TAGETIK SOFTWARE S.R.L., quali in particolare l'acquisto o la cessione di partecipazioni o rami d'azienda, di fusione, scissione o scorporo, devono prevedere:
- la precisa attribuzione delle responsabilità decisionali e di quelle operative nell'ambito dei singoli progetti, nonché i meccanismi di coordinamento tra le funzioni così individuate;
- l'informazione all'Organismo di Vigilanza, fin dal principio del progetto, in modo che sia possibile che questo segua l'intero *iter* decisionale;
- la messa a disposizione allo stesso Organismo di Vigilanza dell'intera documentazione relativa a ogni progetto;
Per quanto riguarda l'eventuale conflitto di interessi, l'obbligo per gli amministratori di comunicare al Consiglio di Amministrazione e all'Organismo di Vigilanza, che ne cura l'archiviazione e l'aggiornamento, tutte le informazioni relative alle cariche assunte o alle partecipazioni di cui sono titolari, direttamente o indirettamente, in altre società o imprese, nonché le cessazioni o le modifiche delle medesime, le quali, per la natura o la tipologia, possono lasciar ragionevolmente prevedere l'insorgere di conflitti di interesse ai sensi dell'art. 2391 c.c.

5.3 Rapporti con le Autorità competenti

Per quanto riguarda eventuali rapporti con le Autorità competenti, sono tre i potenziali ambiti di attività rilevanti:
- la predisposizione e la trasmissione delle informazioni, periodiche e non, richieste dalla legge e dai regolamenti;
- la predisposizione e la trasmissione di ogni altra informazione che sia ulteriormente richiesta dalle Autorità competenti;
- le condotte da tenere nel caso di verifiche ispettive delle stesse Autorità.
In questi casi, le attività dovranno essere rette ai seguenti principi:
- i termini e i modi della trasmissione e della circolazione interna dei dati necessari alla predisposizione delle informazioni alle Autorità competenti, con la previsione di meccanismi e procedure che assicurino la massima veridicità e completezza degli stessi;
- l'individuazione di responsabili, che curino il rispetto delle procedure previste e rilascino una dichiarazione di veridicità e completezza delle informazioni raccolte e predisposte;
- nel caso di verifiche ispettive, la massima collaborazione da parte di tutte le unità aziendali coinvolte, la tempestiva individuazione di un responsabile delle attività necessarie, che possa assicurare il massimo coordinamento tra le unità aziendali coinvolte e la massima rapidità nella messa a disposizione delle informazioni richieste dagli ispettori;
- in generale, la possibilità, per tutti i responsabili individuati, di rivolgersi e riferire all'Organismo di Vigilanza in merito allo svolgimento delle attività relative ai rapporti con le Autorità competenti, segnalando altresì eventuali carenze delle procedure e dei metodi operativi predisposti;

- per quanto riguarda il responsabile individuato nel caso di verifiche ispettive la redazione di una relazione all'Organismo di Vigilanza sull'indagine avviata, che dovrà essere periodicamente aggiornata in relazione agli sviluppi dell'indagine stessa e al suo esito.

6. Procedure e documenti interni di riferimento

In relazione alla presente parte speciale sono di riferimento le seguenti procedure e documenti interni:

1. Codice etico
2. Procedura per la redazione del bilancio
3. Procedura commerciale

Tali procedure e documenti sono da considerarsi integrative ed esplicative delle prassi definite nella presente Parte Speciale.

PARTE SPECIALE "D"

Abusi di mercato

1. I Delitti di cui agli artt. 184 e 185 TUF (art. 25 sexies del Decreto)

L'art. 9 della legge 18 aprile 2005, n. 62, recependo le indicazioni della direttiva 2003/6/CE del Parlamento Europeo e del Consiglio del 28 gennaio 2003, ha introdotto nel Decreto l'art. 25-*sexies*. Questa norma estende l'ambito di applicazione della disciplina della responsabilità amministrativa degli Enti anche a condotte di esponenti aziendali che integrino una delle due fattispecie di abuso di mercato previste nel TUF.

La stessa legge, infatti, ha provveduto a ridelineare il quadro degli illeciti di abuso di mercato, introducendo, agli artt. 184 e 185 nel TUF, due distinti delitti.

L'art. 184 sanziona il cd. abuso di informazioni privilegiate con la reclusione da due a dodici anni e con la multa da euro quarantamila ad euro sei milioni: il reato si realizza quando taluno, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, o della partecipazione al capitale della emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio, 1) compie operazioni su strumenti finanziari giovandosi di quelle informazioni oppure 2) comunica tali informazioni ad altri oppure 3) raccomanda o induce altri a compiere operazioni.

Secondo il comma 2 della norma, lo stesso reato può essere commesso da ogni soggetto che, pur privo di una della qualità indicate dal primo comma, sia venuto in possesso di un'informazione sensibile in ragione delle preparazione di un reato.

Inoltre l'art. 181 del TUF definisce espressamente la nozione di informazione privilegiata: si intende un'informazione di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari.

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

Per informazione che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di strumenti finanziari si intende un'informazione che presumibilmente un investitore ragionevole utilizzerebbe come uno degli elementi su cui fondare le proprie decisioni di investimento.

L'art. 185 del TUF, invece, sanziona le condotte di manipolazione del mercato.

Questa norma, in particolare, sanziona con la pena della reclusione da due a dodici anni e la multa da euro quarantamila ad euro dieci milioni, tre tipologie di condotta:

1) la diffusione di notizie false;
2) il compimento di operazioni simulate;
3) la realizzazione di altri artifici

nel caso in cui simili condotte siano idonee a provocare una sensibile alterazione del prezzo di strumenti finanziari quotati.

2. Aree a rischio

TAGETIK SOFTWARE S.R.L. non è una società quotata: tale dato elimina il rischio che, nell'ambito della sua attività, possano essere compiuti abusi di mercato che siano relativi a titoli della medesima società. Inoltre TAGETIK SOFTWARE S.R.L. non detiene partecipazioni in società quotate e non opera modo mercato borsistico.

E' invece da considerare, come area di rischio, la gestione delle informazioni relative a società clienti che risultano essere quotate: nell'ambito delle proprie quotidiane attività, i consulenti di TAGETIK SOFTWARE S.R.L. sono a diretto contatto con dati relativi ai bilanci e/o ai consolidati di gruppo di primarie società quotate nella Borse italiane ed estere.

Le aree della Società ritenute maggiormente a rischio di commissione di attività di abusi di mercato sono così individuabili:

a. gestione delle informazioni relative ad eventuali rapporti con clienti quotati o collegati con altri soggetti quotati, prima della loro formalizzazione/ufficializzazione;

b. attività di comunicazione relativa a nuovi accordi, nuovi servizi e nuove *partnership* che coinvolgano clienti quotati o collegati a terzi quotati.

3. Regole generali di comportamento

Per norma generale espressamente formalizzata, tutte le informazioni relative alla gestione dell'azienda, ai clienti, a dati di bilancio, a conclusioni di accordi ecc. devono essere trattate e gestite come informazioni riservate e diffuse solo tra i soggetti strettamente necessari e coinvolti nelle specifiche attività di progetto.
Con specifico riferimento alle attività di consulenza, TAGETIK SOFTWARE S.R.L. indica le seguenti norme di condotta:
- ogni forma di comunicazione con terzi deve essere improntata a principi di massima riservatezza;
- ogni consulente che intervenga in progetti nel corso dei quali potranno essere ricevute o rese reperibili informazioni privilegiate dovrà aver sottoscritto preventivamente un impegno generale alla riservatezza e uno impegno specifico alla tutela dei dati del cliente riscontrati durante le attività progettuali;
- è fatto obbligo a tutti i Destinatari di segnalare prontamente ogni comportamento ed ogni fatto che possa lasciar intendere lo sfruttamento o le rivelazioni di notizie riservate, se non anche la commissione di un abuso di mercato.

6. Procedure e documenti interni di riferimento

In relazione alla presente parte speciale sono di riferimento le seguenti procedure e documenti interni:

1- Codice Etico
2- Procedura Consulting
3- Procedura HR

Tali procedure e documenti sono da considerarsi integrative ed esplicative delle prassi definite nella presente Parte Speciale.

PARTE SPECIALE "E"

Reati in violazione delle norme sulla tutela della salute e sicurezza sul lavoro

1. Omicidio colposo e Lesioni personali gravi e gravissime in violazione delle norma in tutela della Salute e Sicurezza si Lavoro (art. 25 septies del Decreto)

L'art. 25-*septies* del Decreto, introdotto dalla L. 23 agosto 2007 n. 123, e sostituito dall'art. 300 del D.Lgs. 81/2008 (c.d. Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro), ha esteso la responsabilità amministrativa dell'Ente anche ai reati di omicidio colposo e lesioni gravi e gravissime, commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

In proposito, si deve evidenziare che il citato decreto, oltre a riformare e riorganizzare in maniera sistematica la vasta disciplina esistenti in materia di tutela della salute e della sicurezza sui luoghi di lavoro, ha appunto esteso la responsabilità amministrativa dell'ente alle ipotesi di reato in esame, e dettato alcune norme specifiche in merito alla predisposizione del Modello.

Omicidio colposo (art. 589 c.p.)

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

Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione sul lavoro la pena è della reclusione da due a sette anni.

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

Lesioni personali colpose (art. 590 c.p.)

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

Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da Euro 123 a Euro 619; se è gravissima, della reclusione da tre mesi a due anni o della multa da Euro 309 a Euro 1.239.

Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da Euro 500 a Euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni. Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque.

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

*****

È opportuno precisare che non tutti gli episodi di omicidio colposo o di lesioni personali colpose gravi o gravissime possono essere il presupposto della responsabilità amministrativa: infatti, ai sensi dell'art. 25-*septies* in esame, rilevano solo quei fatti in cui la condotta colposa che abbia determinato il danno all'incolumità fisica di qualcuno sia consistita nel mancato rispetto di una o più norme di legge o regolamento poste a tutela della salute e della sicurezza sul lavoro.

È altresì necessario precisare, ai sensi dell'art. 583 comma 1 c.p., la lesione personale è da considerarsi "*grave*" se: (i) dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore a 40 giorni; (ii) il fatto produce l'indebolimento permanente di un senso o di un organo.

La lesione è invece considerata "*gravissima*", ai sensi del medesimo art. 583 comma 2 c.p., se dal fatto deriva: (i) una malattia certamente o probabilmente insanabile; (ii) la perdita di un senso; (iii) la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà dell'uso della parola; (iv) la deformazione, ovvero lo sfregio permanente del viso.

Per quanto attiene al regime sanzionatorio introdotto dal Decreto in relazione ai reati in esame, si distinguono tre diversi gradi di gravità dell'illecito, e quindi della sanzione applicabile all'ente. In particolare:

(i) nel caso di omicidio colposo determinato dalle violazioni più gravi indicate dall'art. 55 comma 2 del Testo Unico (consistenti, sommariamente, nell'omessa redazione o nell'inadeguata redazione del documento di valutazione dei

rischi imposto dalla legge in aziende le cui attività sono caratterizzate da particolare pericolosità), la sanzione pecuniaria è di 1000 quote; la sanzioni interdittive vanno da un minimo di tre mesi a un massimo di un anno;
(ii) nel caso di omicidio colposo commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, la sanzione pecuniaria va da 250 a 500 quote; quelle interdittive da un minimo di tre mesi ad un massimo di un anno;
(iii) nel caso di lesione colposa grave o gravissima, la sanzione pecuniaria massima è di 250 quote; le sanzioni interdittive non superano i sei mesi.

*****

2. Destinatari della presente parte speciale

In considerazione della finalità delle fattispecie in esame, risulta di tutta evidenza come ogni attività di impresa costituisca un rischio, sotto tale profilo, tanto per chi la esegue quanto per la collettività in generale.
Immediata conseguenza di tali premesse è che devono ritenersi destinatari della presente Parte Speciale, in aggiunta ai Destinatari del Modello:
- tutti i soggetti che svolgono funzioni e ricoprono incarichi in materia di salute e sicurezza nei luoghi di lavoro (a titolo esemplificativo, i delegati del datore di lavoro, i responsabili per la sicurezza, i medici competenti, gli addetti alle emergenze, ecc.);
- i prestatori esterni di servizi che operino all'interno delle aree aziendali;
- i lavoratori di imprese appaltatrici che operino all'interno delle aree aziendali;
- altri collaboratori, anche solo occasionali;
- i visitatori degli uffici e altre aree aziendali.

3. Finalità della presente parte speciale

Si deve anzitutto evidenziare che i delitti di cui alla presente Parte Speciale, a differenza di tutti gli altri previsti dal Decreto, non consistono in condotte illecite volontarie; essi sono integrati da condotte meramente colpose, e quindi involontarie.
Nel caso di lesioni colpose, quindi, nessuno persegue la realizzazione dell'evento lesivo: esso avviene per causa di un'omissione precedente circa il rispetto delle norme antinfortunistiche determinata da colpa (ossia da negligenza o imprudenza o imperizia), non certo dalla volontà di causare l'evento.
La presente Parte Speciale ha quindi la finalità di prevenire questo tipo di reati, attraverso la previsione di una serie di misure organizzative interne che mirino all'assunzione puntuale ed esaustiva di tutti i rimedi e di tutte le misure imposte dalla legge e dai regolamenti per la piena tutela della sicurezza del lavoro e la riduzione al minimo del rischio che si possano verificare omissioni e carenze in questo ambito di attività.
Nel perseguire le finalità di prevenzione, l'art 30 del D.Lgs. 81/2008 precisa che il modello Organizzativo, in relazione agli specifici reati di cui all'art. 25-septies deve essere finalizzato a:
a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
d) alle attività di sorveglianza sanitaria;
e) alle attività di informazione e formazione dei lavoratori;
f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.
Va per contro precisato che nella specifica realtà di TAGETIK SOFTWARE S.R.L., la cui struttura è formata sostanzialmente di uffici e di lavoratori che effettuano attività prevalentemente intellettuali, i rischi di reato ai sensi del sopra citato art. 25-septies sono decisamente limitati anche se, chiaramente, non escludibili.
Il presente Modello si propone pertanto ed espressamente di:
- prevedere misure e metodi idonei a monitorare l'applicazione delle attività previste dal D.lgs. 81/2008 e s.m.i. in relazione agli adempimenti obbligatori per la realtà di TAGETIK SOFTWARE S.R.L.;

- a prevedere l'estensione del sistema disciplinare già esistente anche alle carenze, alle omissioni ed alle violazioni in materia antinfortunistica.

4. Soggetti dedicati a compiti in materia di sicurezza

I soggetti che hanno un ruolo di rilevo per la tutela della sicurezza e della salute del lavoro sono:
1. Datore di lavoro, per i compiti da questo non delegabili;
2. Responsabile del Servizio di Prevenzione e Protezione (RSPP);
4. Addetti antincendio e primo soccorso;
5. Preposti all'osservanza delle norme in materia di sicurezza;
6. Rappresentante dei lavoratori per la sicurezza (RLS);
7. Medico competente;
8. Lavoratori.

Il datore di lavoro ai fini della Salute e Sicurezza nei luoghi di lavoro è stato individuato e appositamente delegato dal Consiglio di Amministrazione in uno degli Amministratori Delegati della Società. Ad egli spetta il compito di adempiere ai propri compiti indelegabili con riferimento in primis alla valutazione dei rischi e alla nomina del Responsabile del Servizio di Prevenzione e Protezione aziendale (RSPP), attualmente individuato in un consulente esterno che affianca la società e che ha assunto tale incarico in forma personale.
Sono stati poi individuati i lavoratori addetti al servizio antincendio ed i lavoratori addetti al servizio di primo soccorso, che hanno frequentato i relativi corsi di formazione e/o aggiornamento periodico e si è provveduto alla nomina del Medico Competente.
Ai soggetti sin qui richiamati devono aggiungersi infine tutti i lavoratori: il contributo conoscitivo, informativo in merito ai rischi per la sicurezza di tutti i soggetti coinvolti nell'attività dell'impresa è infatti fondamentale per un sistema interno che miri ad una tutela quanto più efficace della sicurezza, anche con riferimento al più rapido e tempestivo rilevamento di eventuali carenze, eventuali punti scoperti ed eventuali esigenze di adeguamento, in caso di modifiche organizzative.

5. Pianificazione e organizzazione del Sistema

Per dare attuazione concreta ai principi della propria gestione della sicurezza, TAGETIK SOFTWARE S.R.L. ha adottato uno specifico sistema di gestione della salute e sicurezza nei luoghi di lavoro ai sensi della norma internazionale BS OHSAS 18001:2007 e ne ha ottenuto la certificazione da parte dell'Organismo di parte terza DEKRA CERTIFICATION S.r.l.

6. Valutazione dei rischi esistenti

Presupposto necessario ed imprescindibile per un'efficace attività di prevenzione dei rischi per la salute e per la sicurezza del lavoro è un'effettiva, adeguata e continuativa rilevazione e valutazione dei rischi per la salute e sicurezza esistenti nell'organizzazione aziendale.
il documento fondamentale risultante è il Documento di Valutazione dei rischi previsto dal Testo Unico. Esso è redatto, aggiornato e perfezionato dal Datore di lavoro con il supporto tecnico del RSPP.
A questo documento si affiancano ulteriori e più specifici documenti, riguardanti particolari tipologie di rischio quali, in primis, la valutazione del rischio d'incendi e la valutazione del rischio stress lavoro correlato.
A fronte delle risultanze delle valutazioni dei rischi per la salute e sicurezza nei luoghi di lavoro TAGETIK SOFTWARE S.R.L. ha provveduto ad attuare le necessarie misure di riduzione del rischio volte a prevenire gli infortuni e le malattie professionali, nonché ad adottare le procedure definite nel sistema di gestione della salute e sicurezza.
Altro profilo fondamentale è dato dalla valutazione di eventuali rischi sanitari. Ruolo fondamentale, al riguardo, è ovviamente svolto dal Medico Competente e dall'archivio della documentazione medica. La documentazione sanitaria è conservata, nel rispetto delle normative in tema di tutela della privacy, in appositi archivi aziendali.
Il Medico Competente provvede a redigere ogni anno una relazione della loro attività, con la segnalazione di particolari patologie o eventi infortunistici che abbiano avuto particolare impatto nell'anno precedente.

7. Casi particolari e/o straordinari rispetto all'attività aziendale ordinaria

Ulteriore elemento decisivo per un'efficace prevenzione è che essa fondi le proprie misure e le proprie iniziative non solo sull'esame dell'ordinaria attività, ma anche sui casi e sulle situazioni che da essa esulino: sono proprio i casi in cui ad essere coinvolti siano soggetti non direttamente appartenenti all'organizzazione di persone della Società, o che riguardino situazioni in senso lato di emergenza quelli che portano con sé i maggiori rischi di attività che si rivelano pericolose o di un abbassamento del livello delle cautele di prevenzione.
Per questa ragione, TAGETIK SOFTWARE S.R.L. ha provveduto a disciplinare anche la materia della salute e sicurezza in caso di appalti conferiti ad imprese terze.

8. Informazione e formazione

Aspetto fondamentale per un'efficace attività di tutela della salute e della sicurezza sul lavoro è costituito dalla corretta formazione ed informazione dei lavoratori e di ogni altro soggetto interessato sui temi della salute e sicurezza nei luoghi di lavoro.
TAGETIK SOFTWARE S.R.L., con il supporto del RSPP, stabilisce le forme ed i modi per garantire:
1. l'efficace formazione ed informazione dei lavoratori e di tutti gli altri soggetti coinvolti nell'attività aziendale;
2. il contributo conoscitivo e di esperienza da parte dei lavoratori, quotidianamente impiegati nelle lavorazioni e nelle attività aziendali.
Quanto al primo punto, sono già state previste ed espressamente disciplinate, anche in relazione agli obblighi cogenti in materia, attività di:
- formazione collettiva su base periodica o specifica;
- formazione individuale, all'ingresso in azienda ed in caso di cambio di mansioni;
- accesso di tutti i soggetti interessati all'archivio documentale in materia di sicurezza.
Quanto al secondo punto, invece, TAGETIK SOFTWARE S.R.L. prevede forme di coinvolgimento sulla base di attività di formazione ed informazione dei lavoratori deve essere data prova scritta, su apposita scheda, che deve essere sottoscritta dal lavoratore interessato.
- riunioni periodiche con i lavoratori ed i loro rappresentanti;
- possibilità di segnalazioni di disfunzioni e carenze.
Le segnalazioni di disfunzioni possono essere indirizzate al Responsabile del Servizio Prevenzione e Protezione (RSPP).

6. Procedure e documenti interni di riferimento

In relazione alla presente parte speciale sono di riferimento le seguenti procedure e documenti interni:

1- Tutte le procedure del sistema di gestione della salute e sicurezza nei luoghi di lavoro ai sensi della norma BS OHSAS 18001;2007.
2- Documento di Valutazione dei Rischi aziendali (e documenti collegati in materia di salute e sicurezza nei luoghi di lavoro)

Tale sistema formato di procedure e documenti è da considerarsi integrativo ed esplicativo delle prassi definite nella presente Parte Speciale.

PARTE SPECIALE "F"

Reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o altra utilità di provenienza illecita, nonché autoriciclaggio

I reati di cui all'art-25–octies sono stati introdotti nel D.Lgs. 231/01 dal D. Lgs. 21 novembre 2007, n. 231 di "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, nonché della direttiva 2006/70/CE che ne reca misure di esecuzione". Da ciò si deduce che la finalità del Decreto n. 231/2007 consiste nella protezione del sistema finanziario dal suo utilizzo ai fini del riciclaggio o di finanziamento del terrorismo.
Si tratta di reati che colpiscono con sanzioni di natura sia pecuniaria che interdittiva.
La sanzione pecuniaria varia da un minimo di 200 ad un massimo di 1000 quote.
Nel caso di condanna, si applicano all'ente anche le sanzioni interdittive previste dall'art. 9, comma 2° del D. Lgs. 231/2001 per una durata non superiore a due anni.

Ricettazione (art. 648 C.P.)

Commette il reato di ricettazione chiunque, allo scopo di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, alla cui commissione non ha partecipato, o comunque si intromette nel farli acquistare, ricevere od occultare. Per tale reato è richiesta la presenza di dolo specifico da parte di chi agisce, e cioè la coscienza e la volontà di trarre profitto, per sé stessi o per altri, dall'acquisto, ricezione od occultamento di beni di provenienza delittuosa.
E' inoltre richiesta la conoscenza della provenienza delittuosa del denaro o del bene; la sussistenza di tale elemento psicologico potrebbe essere riconosciuta in presenza di circostanze gravi ed univoche - quali ad esempio la qualità e le caratteristiche del bene, le condizioni economiche e contrattuali inusuali dell'operazione, la condizione o la professione del possessore dei beni - da cui possa desumersi che nel soggetto che ha agito poteva formarsi la certezza della provenienza illecita del denaro o del bene.

Riciclaggio (art. 648 bis C.P.)

Tale ipotesi di reato si configura nel caso in cui il soggetto agente, che non abbia concorso alla commissione del delitto sottostante, sostituisca o trasferisca denaro, beni o altre utilità provenienti da un delitto non colposo, ovvero compia in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.
La norma va interpretata come volta a punire coloro che - consapevoli della provenienza delittuosa di denaro, beni o altre utilità - compiano le operazioni descritte, in maniera tale da creare in concreto difficoltà alla scoperta dell'origine illecita dei beni considerati.
Non è richiesto, ai fini del perfezionamento del reato, l'aver agito per conseguire un profitto o con lo scopo di favorire gli autori del reato sottostante ad assicurarsene il provento. Costituiscono riciclaggio le condotte dinamiche, atte a mettere in circolazione il bene, mentre la mera ricezione od occultamento potrebbero integrare il reato di ricettazione.

Impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter C.P.)

La condotta criminosa si realizza attraverso l'impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto, fuori dei casi di concorso nel reato d'origine e dei casi previsti dagli articoli 648 (ricettazione) e 648 bis (riciclaggio) C.P..
Rispetto al reato di riciclaggio, pur essendo richiesto il medesimo elemento soggettivo della conoscenza della provenienza illecita dei beni, l'art. 648 ter circoscrive la condotta all'impiego di tali risorse in attività economiche e finanziarie. Peraltro, in considerazione della ampiezza della formulazione della fattispecie del reato di riciclaggio, risulta difficile immaginare condotte di impiego di beni di provenienza illecita che già non integrino di per sé il reato di cui all'art. 648 bis C.P..

Autoriciclaggio (art. 648 ter-1 C.P.)

Il reato di autoriciclaggio punisce "chiunque, avendo commesso o concorso a commettere un delitto non colposo, sostituisce, trasferisce ovvero impiega in attività economiche o finanziarie denaro beni o altre utilità provenienti dalla commissione di tale delitto in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa". La pena prevista è la reclusione da 2 a 8 anni e la multa da euro 5.000 a euro 25.000. La pena viene

ridotta alla reclusione da 1 a 4 anni se il reato presupposto della condotta di riciclaggio prevede la reclusione inferiore, nel massimo, a 5 anni.
La pena è aumentata quando i fatti sono commessi nell'esercizio di un'attività bancaria, finanziaria o di altra attività professionale; è invece diminuita se il soggetto si è adoperato per "evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto".
Le condotte di autoriciclaggio non sono punite "quando il denaro, i beni o le altre utilità vengono destinate all'utilizzazione o al godimento personale" purché non ci sia stata intenzione, in tal modo, di occultare i frutti del reato.
Le norme sull'autoriciclaggio non si applicano a chi aderisce alla procedura di "voluntary disclosure", ovvero collabora volontariamente al rientro di capitali detenuti illegalmente all'estero.

2. Finalità della presente parte speciale

La presente parte speciale si riferisce a comportamenti posti in essere dagli Organi Sociali, dai Dipendenti, nonché dai Consulenti, come meglio definiti nella parte generale, coinvolti nella fattispecie di attività sensibile.
Obiettivo della presente parte speciale è garantire che i soggetti sopra individuati mantengano condotte conformi ai principi di riferimento di seguito enunciati, al fine di prevenire la commissione del reato indicato nel paragrafo precedente.

Nella parte generale sono stati richiamati i principi ispiratori della normativa e i presidi principali per l'attuazione delle vigenti disposizioni in materia.
In questa parte speciale sono individuati i principi di riferimento per la costruzione del Modello, specificamente previsti in relazione alle fattispecie di attività sensibile individuata al fine di prevenire la commissione del reato di "autoriciclaggio".

3. Principi di riferimento generali

Nell'espletamento di tutte le operazioni direttamente o indirettamente connesse alle tematiche inerenti al reato di "autoriciclaggio", i Dipendenti e gli Organi Sociali devono adottare e rispettare:

- il sistema di controllo interno, e quindi le procedure aziendali, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale e organizzativa;
- il sistema disciplinare;
- in generale, la normativa applicabile.

4. Principi generali di comportamento

La presente parte speciale prevede l'espresso divieto a carico degli Organi Sociali (in via diretta) e dei lavoratori dipendenti di Tagetik Software. (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che considerati individualmente o collettivamente - integrino, direttamente o indirettamente, la fattispecie di reato di cui all' art. 25-octies del D.Lgs. 231/2001 (autoriciclaggio);
- violare i principi e le procedure aziendali applicabili alla presente parte speciale.

5. Le attività sensibili relative al reato di autoriciclaggio ai fini del d. lgs. 231/2001

Le attività sensibili individuate, in riferimento al reato di autoriciclaggio di cui all' artt. 25-octies del D.Lgs. 231/2001, sono le seguenti:

- GESTIONE ADEMPIMENTI ED OPERAZIONI IN MATERIA SOCIETARIA
- GESTIONE DEI PROCESSI AMMINISTRATIVO CONTABILI E DEI FLUSSI FINANZIARI

In riferimento alla fattispecie di autoriciclaggio, occorre tenere in considerazione che, oltre alle attività sopra elencate, l'autoriciclaggio potrebbe trovare realizzazione anche in conseguenza di altre fattispecie presupposto ai sensi del D.Lgs. 231/01 di natura non-colposa (solo a titolo di esempio si pensi alla corruzione, alla truffa ai danni dello stato, alla frode in commercio ai reati contro la proprietà intellettuale e industriale, ai delitti informatici, ecc., i cui proventi potrebbero essere oggetto di "autoriciclaggio" nel caso di condotte mirate ad ostacolare concretamente l'identificazione della provenienza delittuosa).

6. Principi generali di controllo

I Principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo possono essere sintetizzati come segue:

- SEGREGAZIONE DELLE ATTIVITÀ: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- ESISTENZA DI PROCEDURE/NORME/CIRCOLARI: devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- POTERI AUTORIZZATIVI E DI FIRMA: i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere chiaramente definiti e conosciuti all'interno della Società;
- TRACCIABILITÀ: ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

7. Gestione adempimenti ed operazioni in materia societaria

La regolamentazione dell'attività deve prevedere quanto stabilito in maniera dettagliata dai Principi di riferimento relativi alla regolamentazione delle attività sensibili "Operazioni relative al capitale sociale: gestione dei conferimenti, dei beni sociali, degli utili e delle riserve, operazioni sulle partecipazioni e sul capitale" e "Gestione dei flussi finanziari".

8. Gestione dei processi amministrativo contabili e dei flussi finanziari

La regolamentazione dell'attività deve prevedere quanto stabilito in maniera dettagliata dai Principi di riferimento relativi alla regolamentazione delle attività sensibili "Predisposizione di bilanci, relazioni, comunicazioni sociali in genere", nonché "Gestione dei flussi finanziari".

9. I controlli dell'organismo di vigilanza

Fermo restando il potere discrezionale di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza non effettua controlli periodici sulle attività di Tagetik Software S.r.l. potenzialmente a rischio di compimento dei reati, in funzione della valutazione del rischio assegnata in sede di predisposizione del Modello e nel corso dei suoi successivi aggiornamenti.

Si ribadisce tuttavia che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le fattispecie di Attività Sensibili.

All'Organismo di Vigilanza deve essere indirizzato un flusso informativo sintetico, ogni qualvolta venga posta in essere un'operazione che per caratteristiche, rilevanza dimensionale, o natura non ordinaria rispetto ai normali flussi d'operatività aziendale, possa afferire ai profili trattati nel presente capitolo, quali, ad esempio:

- operazioni societarie di natura straordinaria;
- attivazione di finanziamenti da parte di soci o terzi di natura non bancaria, ovvero finanziamenti Intercompany;
- operazioni sul capitale (es. aumenti di capitale, anche mediante conferimenti);
- altre operazioni o flussi finanziari di natura straordinaria;
- operazioni di investimento di particolare rilevanza.

10. Procedure e documenti interni di riferimento

In relazione alla presente parte speciale sono di riferimento le seguenti procedure e documenti interni:

1- Codice Etico
2- Procedura Redazione del bilancio di esercizio
3- Procedura Pagamenti e rimborsi spese
4- Procedura Acquisti IT
5- Procedura Acquisti Marketing
6- Procedura Acquisti Beni e Servizi

Tali procedure e documenti sono da considerarsi integrative ed esplicative delle prassi definite nella presente Parte Speciale.

PARTE SPECIALE "G"

Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare

1. I Delitti di cui all' art. 22 comma 12 del D.Lgs. 286/1998 (art. 25 duodecies del Decreto)

Il D.Lgs. 109/2012 ha ampliato il catalogo dei reati previsti dal D.Lgs. 231/01: l'art. 25-*duodecies* prevedendo come reato "*L'impiego di cittadini di paesi terzi il cui soggiorno è irregolare*".

Tale reato si verifica quando il datore di lavoro occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dall' art. 22 del d.lgs. 286/98 ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge il rinnovo, revocato o annullato.

L'articolo 25-duodecies estende l'applicazione del decreto alle aziende che si sono avvalse di lavoratori stranieri privi del permesso di soggiorno o con permesso scaduto, superando i limiti stabiliti dal D.lgs. n. 268/1998 "Testo Unico Immigrazione" in termini di:

1- numero di lavoratori
2- età
3- condizioni lavorative.

Il D.lgs. n. 109/2012 prevede che le pene disciplinate dall'articolo 22, comma 12 del decreto legislativo 25 luglio 1998, n. 286 che riporta:"...Il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, é punito con *la reclusione da sei mesi a tre anni e con la multa di 5.000 euro per ogni lavoratore impiegato*".

Il D.Lgs. n. 109/2012 (pubblicato sulla G.U. n. 172 del 25 luglio 2012) ha inserito nel D.Lgs. 231/01 l'art. 25-duodecies "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare" con il seguente testo dispositivo:

"1. In relazione alla commissione del delitto di cui all'articolo 22, comma 12-bis, del decreto legislativo 25 luglio 1998, n. 286, si applica all'ente la sanzione pecuniaria da 100 a 200 quote, entro il limite di 150.000 euro."

2. Aree a rischio

TAGETIK SOFTWARE S.R.L. è una società che applica puntualmente ogni previsione normativa in materia di lavoro; ciò nonostante, è stato considerato un profilo di rischio in relazione all'art. 25-duodecies, data la significativa internazionalizzazione dell'azienda che controlla varie società in Paesi Terzi e alla conseguente non irrilevante presenza di personale che opera in trasferta e/o proveniente da differenti Paesi e Nazionalità.

3. Regole generali di comportamento

Per norma generale è chiaramente fatto divieto di impiegare personale proveniente da Paesi Terzi che non risulti in regola con le previsioni del D.Lgs. 286/1998.

Conseguentemente tutto il personale che sia assunto o che comunque collabori con Tagetik Software S.r.l. e che provenga da Paesi Terzi ma risulti domiciliato, anche temporaneamente, in Italia con permesso di soggiorno soggetto a scadenz, deve consegnare all'Ufficio Risorse Umane copia del proprio permesso di soggiorno in vigore sia all'atto di assunzione e/o inizio della collaborazione che ad ogni successivo rinnovo.

L'Ufficio risorse umane deve verificare periodicamente che tutto il personale con permesso di soggiorno soggetto a scadenza risulti in regola rispetto alle previsioni di cui al D.Lgs. 286/1998

4. Procedure e documenti interni di riferimento

In relazione alla presente parte speciale sono di riferimento le seguenti procedure e documenti interni:

1- Codice Etico
2- Procedura HR

Tali procedure e documenti sono da considerarsi integrative ed esplicative delle prassi definite nella presente Parte Speciale.

PARTE SPECIALE "H"

Reati tributari

1. I Reati Tributari (art. 25 quinquiesdecies del Decreto)

Il D.Lgs. Fiscale 2020 (D.L 124 del 26 ottobre 2019, convertito in legge dalla L. 19 dicembre 2019 nr. 157) ha ampliato il catalogo dei reati previsti dal D.Lgs. 231/01: l'art. 25-quinquesdecies inserendo "I reati tributari" tra i reati sanzionabili ai sensi del D.Lgs. 231/01.

Le fattispecie di reato previste sono le seguenti:

dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000)

Il reato si configura laddove il soggetto, al fine di evadere le imposte sul valore aggiunto o sui redditi, indichi elementi passivi fittizi nelle dichiarazioni annuali, avvalendosi di fatture o altri documenti per operazioni inesistenti.

Il delitto viene commesso quando il soggetto registra nelle scritture contabili le fatture o comunque le detiene ai fini di prova nei confronti dell'Amministrazione finanziaria. In ogni caso, è escluso che il reato possa ritenersi commesso fino al momento in cui tali elementi sono indicati nella dichiarazione annuale.

Va precisato che la definizione di "fatture o altri documenti" include qualsiasi documento con cui il soggetto possa provare l'esistenza di costi deducibili o imposte detraibili.

dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000)

Il delitto viene commesso dal soggetto che, al fine di evadere le imposte sul valore aggiunto o sui redditi, indica elementi passivi fittizi o indica elementi attivi inferiori a quelli effettivi nelle dichiarazioni annuali, sulla base di una falsa rappresentazione nelle scritture contabili e avvalendosi di mezzi fraudolenti idonei ad ostacolare l'accertamento.

Le soglie di punibilità penale che devono essere congiuntamente superate, sono attualmente le seguenti:

- l'importo evaso deve superare (per singola imposta) euro 30.000,00;
- gli elementi attivi sottratti all'imposizione e gli elementi passivi fittizi devono superare il 5% degli elementi attivi dichiarati o comunque € 1.000.000,00.

Costituiscono elementi necessari di questo reato:

a. l'infedeltà della dichiarazione derivante dall'indicazione di elementi attivi inferiori al reale o elementi passivi fittizi;
b. la presenza di una falsa indicazione nelle scritture contabili;
c. l'uso di mezzi fraudolenti, che debbono essere diversi dalle fatture false, altrimenti si ricade nel delitto di dichiarazione fraudolenta mediante utilizzo di fatture false.

emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000)

Il reato si configura laddove il soggetto, al fine di consentire a terzi l'evasione delle imposte sul valore aggiunto o sui redditi, emette fatture o altri documenti per operazioni inesistenti. L'emissione e il rilascio di più fatture o altri documenti per operazioni inesistenti relative al medesimo periodo d'imposta, si considera come un unico reato.

Per il momento della commissione del delitto rileva la registrazione in dichiarazione del documento emesso da parte di chi lo ha ricevuto.

occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000)

Per il reato in oggetto viene punita la condotta di distruzione o occultamento di documenti contabili, la cui tenuta è obbligatoria per legge, al fine di impedire la ricostruzione della contabilità da parte delle autorità preposte, il reato per tali motivi può essere commesso solo da coloro che sono obbligati alla tenuta della contabilità.

Ai fini della punibilità è richiesto il dolo specifico, cioè il reo deve avere specifica finalità di evadere le imposte sui redditi o sul valore aggiunto o di consentire a terzi di evadere le stesse imposte.

Non è previsto il superamento di alcuna soglia di punibilità al fine della commissione del reato.

sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000)

commette il reato di sottrazione fraudolenta al pagamento di imposte, il soggetto che, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva.

Per la sussistenza del delitto, trattandosi di reato di pericolo concreto, è sufficiente che vi sia un debito non inferiore a cinquantamila euro e non è richiesto che sia posta in essere una procedura di riscossione coattiva, ma che siano compiuti atti volti a inficiare il buon esito di una eventuale riscossione forzata.

Successivamente alla L. 19 dicembre 2019 nr. 157, il Decreto Legislativo 14 luglio 2020, n. 75 "Attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale" ha esteso l'elenco dei reati tributari alle seguenti fattispecie:

Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000)

La dichiarazione infedele è un reato tributario, attuabile con dolo specifico, in materia di imposte sui redditi ed IVA. Per la configurazione del reato è necessario che ricorrano congiuntamente due condizioni, ovvero: l'imposta evasa in riferimento alla singola imposta deve essere di ammontare superiore ad euro 150.000,00; il totale degli elementi attivi non indicati nella dichiarazione e/o gli elementi passivi inesistenti devono essere di ammontare superiore al 10% del totale degli elementi attivi indicati in dichiarazione, o, comunque, il loro importo deve superiore ad euro 3.000.000,00. Il Legislatore, in aggiunta alle sopra citate "soglie" di punibilità sopra evidenziate, ha identificato alcune cause di non punibilità nei seguenti casi :

- le violazioni che scaturiscono da interpretazioni di norme, quando queste sono obiettivamente incerte;
- la violazione delle norme sulla competenza economica è frutto di comportamenti contabili costanti ed evidenziati in bilancio, (viene infatti a mancare il dolo);
- le valutazioni estimative, se la stima corretta non differisce di più del 10% da quella effettuata: l'importo di tali differenze non concorre nemmeno al calcolo dell'imposta evasa o degli elementi sottratti a tassazione ai fini delle soglie di punibilità.

Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000)

L'omessa dichiarazione si configura qualora il soggetto, al fine di evadere le imposte sui redditi o sul valore aggiunto non presenta la dichiarazione ai fini delle imposte sul reddito o dell'Iva, pur essendovi tenuto.
La soglia di punibilità del reato di omessa dichiarazione è attualmente pari a euro 30.000,00.

Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000)

Il reato si configura laddove il soggetto non versi le somme dovute, utilizzando in compensazione, crediti inesistenti o non spettanti.
Il reato si consuma nel momento in cui le indebite compensazioni eccedono € 50.000 in un periodo d'imposta.
-

Destinatari della presente parte speciale

In considerazione della finalità delle fattispecie in esame, devono ritenersi destinatari della presente Parte Speciale:
- il Consiglio di Amministrazione
- gli organi incaricati della Revisione
- le funzioni incaricate della predisposizione del bilancio, inclusi i consulenti dell'azienda in materia fiscale e tributaria
- tutti i soggetti che svolgono funzioni e ricoprono incarichi in materia amministrativa, quali in particolare, la gestione del ciclo attivo e l'emissione delle fatture di vendita.
- le funzioni incaricate della gestione del ciclo passivo e, in particolare, la ricezione, verifica, registrazione delle fatture da fornitori per il successivo pagamento.

2. Finalità della presente parte speciale

La presente Parte Speciale ha la finalità di prevenire i reati sopra indicati, attraverso la previsione di una serie di misure organizzative interne che mirino alla verifica periodica o specifica del rispetto delle normative in materia fiscale.

3. Aree a rischio

TAGETIK SOFTWARE Srl è una società che applica ogni previsione normativa in materia tributaria; ciò nonostante, è stato comunque considerato un profilo di rischio, in relazione all'art. 25-*quinquiesdecies*, derivante da possibili erronee registrazioni di contabilità e/o valorizzazioni di bilancio, significative ai sensi del calcolo e conseguente versamento delle imposte.
Inoltre sono considerate operazioni a rischio eventuali attività di rimozione/distruzione di documenti validi ai fini fiscali, inclusa la gestione dei documenti conservati informaticamente a titolo di archiviazione sostitutiva.

4. Regole generali di comportamento

Nell'espletamento delle attività di gestione amministrativa devono essere rispettate le procedure predisposte a controllo del ciclo attivo e passivo dell'azienda, oltre che il rispetto della procedura di predisposizione del bilancio di esercizio e delle normative cogenti in materia.
È quindi necessario:

- attenersi a quanto espressamente previsto dal Codice Etico della Società in materia di trasparenza, rapporto con gli organi societari e rispetto della legalità;
- conoscere e applicare le previsioni delle norme fiscali anche richiedendo specifiche consulenze o supporti in materia
- rispettare puntualmente quanto previsto dalle procedure interne e dai contratti aziendali in fatto di:
  - emissione delle fatture di vendita
  - verifica, autorizzazione, registrazione e pagamento delle fatture passive
  - predisposizione del bilancio di esercizio
  - eliminazione dei documenti obsoleti
- porre la massima attenzione ad ogni attività di registrazione contabile, potenzialmente atta a creare erronee poste di bilancio e/o a violare le normative cogenti in materia;
- porre la massima attenzione al rispetto delle normative di legge in ogni eventuale attività di eliminazione di documenti obsoleti (sia cartacei che informatici) validi a fini fiscali.

5. I controlli dell'organismo di vigilanza

Per monitorare il rispetto delle procedure e misure atte ad evitare, per quanto possibile, la violazione, anche incidentale, delle norme relative ai reati tributari dovranno essere attuati specifici audit di verifica interna, con cadenza pianificata, con e/o senza preavviso, a cura dell'Organismo di Vigilanza e/o di suoi incaricati qualificati.
A tal fine, si ribadisce che all'Organismo di Vigilanza e ad eventuali incaricati dell'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le fattispecie di attività sensibili.

6. Procedure e documenti interni di riferimento

In relazione alla presente parte speciale sono di riferimento le seguenti procedure e documenti interni:

- Codice Etico
- Procedura emissione delle fatture di vendita
- Procedura pagamenti e rimborsi spese
- Procedura per la redazione del bilancio

Tali procedure e documenti sono da considerarsi integrative ed esplicative delle prassi definite nella presente Parte Speciale.