T Bridge S.p.A.

MODELLO DI ORGANIZZAZIONE

(ai sensi del D.L.vo 231/2001)

primo aggiornamento giugno 2016

secondo aggiornamento luglio 2020

terzo aggiornamento settembre 2023

T BRIDGE S.p.A. a socio unico soggetta a direzione e coordinamento di BV TECH S.p.A
Via G. Garibaldi, 7/10, 16124, Genova
Tel. +39 010 5769111
Fax +39 010 5531185
PEC: tbridge@legalmail.it

Capitale sociale € 400.000,00 i.v.
C.F. e P. IVA n.01201580998
Registro delle Imprese di Genova n. 01201580998

T BRIDGE
BV'TECH

PARTE GENERALE

IL DECRETO LEGISLATIVO N. 231/2001

PREMESSA

Il presente documento viene redatto ai sensi di quanto previsto:
dalla Convenzione di Bruxelles del 26 luglio 1995 sulla protezione degli interessi finanziari della Comunità Economica Europea,
dalla Convenzione di Bruxelles del 26 maggio 1997 sulla lotta contro la corruzione dei pubblici ufficiali nell'ambito della Comunità Economica Europea e degli Stati Membri;
dalla Convenzione OECD del 21 novembre 1997 per la lotta contro la corruzione dei pubblici ufficiali esteri nelle transazioni internazionali;
dal decreto legislativo n. 231/2001 così come emanato ed integrato dalla successiva legislazione (d'ora innanzi il Decreto) ed in particolare per individuare un modello di organizzazione societaria finalizzato alla prevenzione dei reati individuati nel Decreto e nelle Convenzioni.
L'aggiornamento, conformemente a come previsto dal d.lgs 231/01, si è reso necessario per recepire da un lato le novità legislative e dall'altro la nuova struttura organizzativa di T Bridge S.p.A. Si è provveduto a aggiornare l'elenco e la descrizione delle fattispecie di reato presupposto previste dalla normativa vigente al 31/06/2016. In relazione alle ridefinite e/o nuove fattispecie di reato, introdotte dalle intervenute modifiche ed integrazioni al d.lgs 231/01, si ritiene che i principi generali di comportamento e i protocolli di controllo già adottati nella parte speciale del modello organizzativo, alla quale pertanto si rinvia, siano adatti alla loro prevenzione.
Ad inizio 2020, è emersa l'esigenza di aggiornare il presente modello per adeguarlo all'evoluzione normativa del D. Lgs. 231/2001 intervenuta e ad oggi in vigore. L'aggiornamento ha riguardato l'adeguamento del Modello all'evoluzione normativa introdotta dalla L. n. 179 del 30 novembre 2017, che ha introdotto nuovi principi ed obblighi in relazione al Modello adottato, l'aggiornamento dell'elenco reati presupposto, la valutazione del rischio commissione dei nuovi reati presupposto da parte di soggetti ''collegati" a T Bridge s.p.a., l'aggiornamento delle aree/attività a rischio commissione reati, dei principi generali di comportamento, dei protocolli aziendali e del sistema sanzionatorio in relazione ai nuovi reati presupposto. (Postilla aggiornamento 2020)

T BRIDGE
BV*TECH

STRUTTURA DEL DOCUMENTO

Il presente documento è composto di una Parte Generale e una Parte Speciale.

La Parte Generale descrive: la disciplina contenuta nel D. Lgs. 231/2001ed i reati rilevanti per la Società, indica i destinatari del Modello ed i principi di funzionamento dell'Organismo di Vigilanza, definisce un sistema sanzionatorio dedicato al presidio delle violazioni del Modello, gli obblighi di comunicazione dello stesso e di formazione del personale.

La Parte Speciale ha ad oggetto l'indicazione delle attività "sensibili" – cioè, delle attività che sono state considerate dalla Società a rischio di reato, in esito alle analisi dei rischi condotte – ai sensi del Decreto, i principi generali di comportamento, gli elementi di prevenzione a presidio delle suddette attività e le misure di controllo essenziali deputate alla prevenzione o alla mitigazione degli illeciti.

Costituiscono inoltre parte integrante del Modello:

il Codice Etico, che definisce i principi e le norme di comportamento della Società;

Il Codice Sanzionatorio

Tutte le disposizioni, i provvedimenti interni, gli atti e le procedure operative aziendali che del presente documento costituiscono attuazione (ad esempio statuto, poteri, organigrammi, job description, procedure). Tali atti e documenti sono reperibili secondo le modalità previste per la loro diffusione all'interno dell'azienda.

T BRIDGE
BV'TECH

PARTE GENERALE

LA SOCIETA'

La T Bridge S.p.A. (d'ora innanzi anche indicata come la società) è una società di consulting, attiva nella consulenza direzionale, nella formazione manageriale e nella consulenza ICT. I mercati di sbocco di T Bridge sono quelli dei servizi e delle utilities (settori sanità, retailing e grande distribuzione, cultura e turismo, servizi all'industria, enti pubblici), dell'industria (prevalentemente impiantistica e manifatturiera), del trasporto merci e passeggeri, della mobilità e della logistica. La società ha sede legale in Genova e sede operativa in Milano. La stessa fa parte del gruppo BV Tech S.p.A., con sede in Milano. Il gruppo ad oggi raggruppa circa 500 dipendenti e sviluppa un volume d'affari di circa 60 milioni di euro. Il 70% circa dell'organico è costituito da personale tecnico laureato altamente specializzato con età non superiore a 40 anni. La clientela di T Bridge è composta sia da primarie aziende private operanti nei mercati sopra descritti che da amministrazioni pubbliche.

IL REGIME DI RESPONSABILITÀ PREVISTO DAL DECRETO LEG.VO 231/2001

Con il Decreto Legislativo n. 231 dell'8 giugno 2001 (di seguito il "Decreto"), recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, entrato in vigore il 4 luglio successivo è stato introdotto nell'ordinamento, a carico delle persone giuridiche (di seguito denominate Enti), un regime di responsabilità amministrativa (equiparabile sostanzialmente alla responsabilità penale), che va ad aggiungersi alla responsabilità della persona fisica che ha materialmente commesso determinati fatti illeciti e che mira a coinvolgere, nella punizione degli stessi, gli Enti nel cui interesse o vantaggio i reati in discorso siano stati compiuti.
Un simile ampliamento della responsabilità a carico degli Enti mira ad estendere la punizione degli illeciti penali individuati nel Decreto agli Enti che abbiano tratto vantaggio o nel cui interesse siano stati commessi i reati. La responsabilità prevista dal Decreto si configura anche in relazione a reati commessi all'estero, purché per gli stessi non proceda lo Stato nel cui luogo è stato commesso il reato.
I punti chiave del Decreto riguardano:
a) le persone coinvolte nella commissione del reato, che sono:

I) persone fisiche che rivestono posizioni c.d. “apicali” (rappresentanza, amministrazione o direzione dell’Ente o di altra unità organizzativa o persone che ne esercitino, di fatto, la gestione ed il controllo);
II) persone fisiche sottoposte alla direzione o vigilanza da parte di uno dei soggetti sopraindicati;
b) la tipologia di reati prevista, che riguarda, in generale,
I) alcuni reati contro la Pubblica Amministrazione
II) alcuni reati contro la circolazione delle monete con corso legale
III) alcuni reati societari
IV) alcuni reati di carattere terroristico
V) alcuni reati contro la libertà personale e contro i minori
VI) alcuni reati contro il corretto andamento del mercato
VII) alcuni reati connessi con la tutela della sicurezza nei luoghi di lavoro
VIII) alcuni reati informatici
Dalla sua entrata in vigore il decreto 231 ha subito continui aggiornamenti normativi relativi alle fattispecie di reato.
Di seguito si riportano i principali aggiornamenti:
Il D.L. 25 settembre 2001, n. 350, convertito con L. 23 novembre 2001, n. 409 ha disposto (art. 6) l'introduzione dell'art. 25–bis.
Il D.Lgs. 11 aprile 2002, n. 61 ha disposto (art. 3) l'introduzione dell'art. 25–ter e la seguente modifica nel Capo I, Sezione III: la partizione "Responsabilità amministrativa per reati previsti dal codice penale" è sostituita dalla seguente: “Responsabilità amministrativa da reato”.
Il D.P.R. 30 maggio 2002, n. 115 ha disposto (art. 299) l'abrogazione dell'art. 75.
Il D.P.R. 14 novembre 2002, n. 313 ha disposto (art. 52) la modifica dell'art. 85 e l'abrogazione degli artt. 80, 81 e 82.
La L. 14 gennaio 2003, n. 7 ha disposto (art. 3) l'introduzione dell'art. 25–quater.
Il D. 26 giugno 2003, n. 201 precisa che (art. 8), rispetto ai termini stabiliti dall'art. 6 del d.lgs. 231/01, “Per i codici di comportamento inviati al Ministero della giustizia fino alla data di entrata in vigore del presente regolamento, il termine di trenta giorni di cui all'articolo 6, comma 3, del decreto legislativo n. 231 del 2001, decorre da tale data.”
La L. sto 2003, n. 228 ha disposto (art. 5) l'introduzione dell'art. 25–quinquies.
La L. 18 aprile 2005, n. 62 ha disposto (art. 9) l’introduzione dell'art. 25–sexies.
La L. 28 dicembre 2005, n. 262 ha disposto (art. 31) la modifica dell'art. 25–ter.
La L. 9 gennaio 2006, n. 7 ha disposto (art. 8) l'introduzione dell'art. 25–quater.1.
La L. 6 febbraio 2006, n. 38 ha disposto (art. 10) la modifica dell'art. 25–quinquies.
La L. 16 marzo 2006 n.146 che ha introdotto la fattispecie dei reati transnazionali.
La L. 3 agosto 2007, n. 123 ha disposto (art. 9) l'introduzione dell'art. 25–septies.
Il D.Lgs. 21 novembre 2007, n.231 ha disposto (art. 63) l'introduzione dell'art. 25–octies.
La L. 18 marzo 2008, n. 48 ha disposto (art. 7) l'introduzione dell'art. 24–bis.

Il D.Lgs. 9 aprile 2008, n. 81 ha disposto (art. 300) la modifica dell'art. 25–septies.
La L. 15 luglio 2009, n. 94 ha disposto (art. 2) l'introduzione dell'art. 24–ter.
La L. 23 luglio 2009, n. 99 ha disposto (l'art. 15, comma 7) la modifica dell'art. 25–bis, commi 1, 2 e rubrica, l'introduzione degli artt. 25–bis.1 e 25–novies.
La L. 3 agosto 2009, n. 116 ha disposto (art. 4) l'introduzione di un "secondo" art. 25–novies. (che è stato rinominato decies).
Il D.lgs. n. 121 del 7 luglio 2011 che ha introdotto l'art. 25 – undecies.
Il D.lgs. n. 109 del 2012 che ha introdotto l'art. 25 – duodecies.
La L. n. 190 del 06 novembre 2012 che ha modificato il comma 3 dell'art. 25.
La L. n. 125 del 30 ottobre 2013 che ha modificato l'art. 53.
La L. n. 186 del 15 dicembre 2014 che ha modificato l'art. 25 octies.
La L. n. 68 del 22 maggio 2015 che ha modificato l'art. 25 undecies.
La L. n. 69 del 27 maggio 2015 che ha modificato l'art. 25 ter.
Il D. Lgs. n. 125 del 21 giugno 2016 che ha modificato l'art. 25 bis.
Di seguito si riportano gli interventi normativi che hanno introdotto ulteriori reati presupposto della responsabilità della società ex D. Lgs. 231/2001:
L. n. 199/2016 che ha modificato l'art. 25 quinquies introducendo i reati di riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.), tratta di persone (art. 601 c.p.), acquisto o alienazione di schiavi (art. 602 c.p.), intermediazione illecita e sfruttamento del lavoro (art. 603 bis c.p.);
D. Lgs. n. 38 del 15 marzo 2017, che ha modificato l'art. 25 ter aggiungendo alla lettera s- bis il reato di istigazione alla corruzione fra privati;
L. n. 161 del 17 ottobre 2017, che ha modificato l'art. 25 duodecies ed introdotto i reati ''di trasporto ed ingresso di stranieri nel territorio dello Stato" e " il trarre profitto dalla condizione di illegalità e/o il favorire la permanenza illecita dello straniero";
L. n. 167 dell'11 novembe 2017, che ha introdotto i reati di ''razzismo e xenofobia" previsti dall'art. 3 L. n. 654/1975;L. n. 3 del 9 gennaio 2019, che ha modificato l'art. 25 ed ha introdotto il reati di traffico di influenze illecite (art. 346 bis c.p.);
L. n. 39 del 03 maggio 2019 che ha inserito l'art. 25 quaterdecies ed introdotto i reati di ''Frode in competizione sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitato a mezzo di apparecchi vietati;
D.L. n. 105 del 21 settembre 2019, convertito, con modificazioni, dalla L. 18 novembre 2019, n. 133 che ha modificato l'art. 24 bis ed introdotto il cosiddetto reato ''Perimetro di sicurezza cibernetico";
D.L. n. 124 del 26 ottobre 2019, convertito, con modificazioni, dalla L. n. 157 del 19 dicembre 2019, che ha inserito l'art. 25 quinquies ed introdotto i cosiddetti ''reati tributari".
La normativa del D. Lgs. 231/2001 ha avuto modifiche ed evoluzioni anche in merito ai principi generali e ai modelli di organizzazione e gestione. Di seguito i riferimenti:

L. 30 novembre 2017, n. 179 che ha modificato l'art. 6 del D. Lgs inserendovi la lettera d del comma 2bis ed i commi 2ter e quater prevedendo che:
lett. d, il modello di organizzazione e gestione prevede che nel sistema disciplinare adottato ai sensi del comma 2, lettera e), siano comminate 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;
comma 2-ter. L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2-bis 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.
comma 2-quater. 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.
Infine, ulteriori modifiche della normativa hanno avuto ad oggetto la durata delle misure cautelari, sanzioni, misure interdittive, confisca e pubblicazione della sentenza a carico dell'ente. (Postilla aggiornamento 2020)

ESIMENTI DALLA RESPONSABILITÀ

Il Decreto prevede una specifica esimente dalla responsabilità amministrativa qualora l'Ente dimostri che:
a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto illecito, modelli di organizzazione e gestione idonei a prevenire la realizzazione degli illeciti penali considerati;
b) ha affidato, ad un organo interno (di seguito "Organismo di Vigilanza") dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e sull'efficace osservanza del modello, nonché di curarne l'aggiornamento;
c) le persone che hanno commesso il reato hanno agito fraudolentemente eludendo il modello;
d) non vi è stato omesso o insufficiente controllo da parte dell'Organismo di Vigilanza.
Ai sensi dell'articolo 6, comma 2, il Decreto prevede inoltre che i Modelli di organizzazione e gestione debbano rispondere alle seguenti esigenze:
a) individuare le attività nel cui ambito possono essere commessi i reati;
b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
c) individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;

d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello;
e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

SANZIONI APPLICABILI

Le sanzioni amministrative per gli illeciti amministrativi dipendenti da reato sono:
a) sanzioni pecuniarie;
b) sanzioni interdittive;
c) confisca;
d) pubblicazione della sentenza.
In particolare le principali sanzioni interdittive concernono:
- l'interdizione dall'esercizio delle attività;
- la sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- l'esclusione da agevolazioni, finanziamenti, contributi e sussidi, nonché la revoca di quelli eventualmente già concessi;
- il divieto di pubblicizzare beni o servizi.

IL MODELLO ADOTTATO DA T Bridge

T Bridge ha adottato il presente Modello di Organizzazione e di Gestione ed ha adottato il Codice Etico, ritenendo che l'insieme di tali documenti, al di là delle prescrizioni di legge, costituisca un ulteriore valido strumento di sensibilizzazione dei propri dipendenti e degli altri soggetti alla stessa legati (collaboratori, consulenti, ecc.). Tutto ciò affinché i suddetti soggetti seguano, nell'espletamento delle proprie attività, comportamenti corretti e trasparenti in linea con i valori etico-sociali cui si ispira T Bridge nel perseguimento del proprio oggetto sociale, e tali comunque da prevenire il rischio di commissione dei reati contemplati dal Decreto.
In attuazione di quanto previsto dal Decreto, l'organo direttivo di T Bridge, nell'approvare il Modello, ha costituito l'Organismo di Vigilanza, attribuendogli i compiti stabiliti dal Decreto. L'Organismo di Vigilanza può farsi assistere da altri soggetti, tra cui i revisori interni, la funzione risorse umane, consulenti legali. Per maggiori dettagli sull'Organismo di Vigilanza si rimanda sotto all'apposito capitolo del presente Modello.
Il Modello si fonda su un complesso, strutturato ed organico, di procedure e controlli finalizzati al presidio delle attività aziendali maggiormente esposte, anche solo potenzialmente, alla commissione dei reati contemplati dal Decreto, per prevenirne od impedirne la commissione. Tale sistema di procedure organizzative operative e di attività di controllo nella sostanza:

a) individua le aree ed i processi fonti di possibili rischi nella attività aziendale, con particolare riguardo a quelle che comportano un rischio reato ai sensi del Decreto, ne valutano l'impatto economico, lo verificano e lo documentano (Risk Management);
b) definisce un sistema organizzativo interno diretto a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai rischi/reati da prevenire tramite:
I) un sistema normativo – composto dal Codice Etico della Società – che fissa le linee di orientamento generali, formalizzate nel tempo, tese a disciplinare in dettaglio le modalità per assumere ed attuare decisioni nei settori "sensibili";
II) un sistema di deleghe e di poteri aziendali che assicuri una chiara e trasparente rappresentazione del processo aziendale di formazione e di attuazione delle decisioni;
III) la definizione di strutture organizzative coerenti ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando una giusta segregazione delle funzioni, assicurando che gli assetti voluti della struttura organizzativa siano realmente attuati;
c) individua i processi di gestione e controllo delle risorse finanziarie nelle attività potenzialmente a rischio reato;
d) attribuisce all'Organismo di Vigilanza specifici compiti di controllo sull'efficacia e sul corretto funzionamento del Modello, sulla coerenza dello stesso con gli obiettivi e sul suo aggiornamento periodico.
Le finalità del Modello, in conformità al Decreto, sono pertanto quelle di:
I) prevenire e ragionevolmente limitare i possibili rischi connessi all'attività aziendale con particolare riguardo alla riduzione di eventuali condotte illecite;
II) determinare, in tutti coloro che operano in nome e per conto di T Bridge, nelle aree di attività a rischio, la consapevolezza di poter incorrere, nel caso di violazioni alle disposizioni riportate nel Modello anche di sanzioni nei confronti di T Bridge;
III) ribadire che T Bridge non tollera comportamenti illeciti, di ogni tipo e indipendentemente da qualsiasi finalità, in quanto gli stessi, oltre a trasgredire le leggi vigenti, sono comunque contrari ai principi etico-sociali cui T Bridge intende attenersi.
Spostando l'attenzione allo specifico contesto operativo di T Bridge, il Modello rappresenta il risultato dell'applicazione metodologica documentata dei criteri di identificazione dei rischi, da un lato, e di individuazione dei protocolli per la programmazione e per la formazione ed attuazione delle decisioni della Società, dall'altro.
Nell'ottica di un processo di adeguamento continuo ai mutamenti societari, alle esigenze in divenire del mercato ed alla evoluzione normativa di riferimento, il Modello è volto ad imporre un sistema compatibile con la struttura societaria, così da integrarsi efficientemente con l'operatività aziendale, ma nello stesso tempo fermamente rivolto al perseguimento dei rigorosi principi finalistici che lo animano.

Il Modello si prefigge, infatti, di indurre tutti quei soggetti che siano in posizione apicale, gli Amministratori, i dipendenti, nonché coloro che operano per T Bridge, quale che sia il rapporto, anche temporaneo che li lega alla stessa, ad acquisire la sensibilità necessaria per percepire la sussistenza dei rischi di commissione di reati nell'esercizio di determinate attività ed insieme comprendere la portata, non solo personale ma anche societaria, delle possibili conseguenze connesse, in termini di sanzioni penali ed amministrative.

A tal fine, T Bridge si propone, con l'adozione del Modello, di conseguire il pieno e consapevole rispetto dei principi su cui lo stesso si fonda, così da impedirne l'elusione fraudolenta, e, nel contempo, contrastare fortemente tutte quelle condotte che siano contrarie alle disposizioni di legge ed al Codice Etico di T Bridge.

Il Modello si compone di una "Parte Generale" e di singole "Parti Speciali" predisposte per le differenti tipologie di reati contemplate dal Decreto.

In particolare la prima "Parte Speciale" – denominata Parte Speciale "A" - trova applicazione per i reati realizzati nei confronti della Pubblica Amministrazione.

La seconda "Parte Speciale" – denominata Parte Speciale "B" - trova applicazione per altre tipologie di reati, tra cui, in particolare, i reati societari, comunque considerate "sensibili" per l'attività di T Bridge.

La terza "Parte Speciale" – denominata Parte Speciale "C" – concerne i reati di omicidio colposo e di lesioni personali colpose derivanti dall'inosservanza della normativa in materia antinfortunistica e di igiene e di sicurezza sui luoghi di lavoro, nonché il recepimento degli standard dettati dall'art. 30 del D.L.vo 9.4.2008, n. 81.

La Parte Speciale "D" riguarda i reati legati ai cd. "delitti informatici e legati al trattamento illecito di dati".

La Parte Speciale "E" fa riferimento ai delitti contro l'industria ed il commercio previsti dal Decreto.

La Parte Speciale "F" fa riferimento ai delitti contro la personalità individuale previsti dal Decreto.

La Parte Speciale "G" fa riferimento ai reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio previsti dal Decreto.

La Parte Speciale "H" fa riferimento ai reati in materia di violazione del diritto di autore previsti dal Decreto.

La Parte Speciale "I" fa riferimento al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria previsto dal Decreto.

La Parte Speciale "L" fa riferimento ai reati ambientali previsti dal Decreto.

La Parte Speciale "M" fa riferimento ai reati attinenti all'impiego di cittadini di paesi terzi il cui soggiorno e' irregolare previsti dal Decreto.

La parte speciale "N" è dedicata ai reati tributari, la più importante innovazione apportata dalle ultime novelle legislative in tema di reati presupposto ai fini della configurazione della responsabilità amministrativa per le persone giuridiche.

In ultimo vengono elencati i reati non ritenuti rilevanti e sensibili in base alle attività svolte dalla società.

Sulla base dell'analisi preliminare svolta, sono stati considerati "sensibili" per la Società, unicamente i reati individuati nella parte speciale. Per la natura dell'attività e dell'organizzazione di T Bridge, si è ritenuto, per il momento, di non considerare come fattispecie rilevanti all'interno del Modello i reati disciplinati dagli artt. 25-bis (falsità in monete, in carta di pubblico credito e in valori di bollo), 25-quinquies (reati verso la persona, quali "riduzione, mantenimento in schiavitù o tratta delle persone", eccezion fatta per quelli legati alla detenzione di materiale pornografico minorile) e 25-sexies (reati a tutela del mercato regolamentato), non considerando ipotizzabili le relative fattispecie di reati nell'ambito dell'attività svolta dalla Società.

Le attività di analisi relative a queste ultime tipologie di reati saranno eventualmente svolte successivamente qualora, a seguito di specifiche valutazioni esse dovessero essere ritenute pertinenti all'azienda.

Il Modello è stato così articolato al fine di garantire una più efficace e snella attività di aggiornamento dello stesso. Infatti, se la "Parte Generale" ha un contenuto sostanzialmente invariabile, le diverse "Parti Speciali", in considerazione del loro particolare contenuto, sono suscettibili invece di costanti aggiornamenti. Inoltre, l'evoluzione legislativa – quale ad esempio una possibile estensione delle tipologie di reati che, per effetto di altre normative, risultino inserite o comunque collegate all'ambito di applicazione del Decreto – potrà rendere necessaria l'integrazione del Modello con ulteriori "Parti Speciali".

T Bridge, già prima dell'adozione del presente Modello, anche nel contesto delle procedure relative all'assicurazione qualità, ha inteso innanzitutto dotarsi di un sistema organizzativo adeguatamente formalizzato e rigoroso nell'attribuzione delle responsabilità, linee di dipendenza gerarchica e puntuale descrizione dei ruoli, con assegnazione di poteri autorizzatori e di firma coerenti con responsabilità definite, nonché con predisposizione di meccanismi di controllo fondati sulla contrapposizione funzionale e sulla separazione dei compiti.

L'applicazione del Modello viene garantita anche mediante la definizione di regole generali e di idonee procedure per disciplinare i processi delle diverse aree aziendali, soprattutto quelle a maggior rischio di commissione dei reati, nonché da un sistema disciplinare.

MODIFICHE ED INTEGRAZIONI DEL MODELLO

Essendo il Modello un "atto di emanazione dell'organo dirigente" (in conformità all'articolo 6, comma 1, lettera a) del Decreto), anche le successive modifiche ed integrazioni di carattere sostanziale, che dovessero rendersi necessarie per sopravvenute esigenze aziendali ovvero per adeguamenti normativi ovvero in accoglimento dei suggerimenti dell'Organismo di Vigilanza, sono rimesse alla competenza dell'organo direttivo di T Bridge.

E' attribuito all'Organismo di Vigilanza il potere di proporre modifiche al Modello o integrazioni di carattere formale nonché quelle modifiche ed integrazioni del Modello consistenti nella:
I) introduzione di nuove procedure e controlli nel caso in cui non sia sufficiente una revisione di quelle esistenti;
II) revisione dei documenti e delle procedure aziendali e societari che formalizzano l'attribuzione delle responsabilità e dei compiti alle posizioni responsabili di strutture organizzative "sensibili" o comunque che svolgono un ruolo di snodo nelle attività a rischio;
III) introduzione di ulteriori controlli delle attività sensibili, con formalizzazione delle iniziative di miglioramento intraprese in apposite procedure;
IV) evidenziazione delle esigenze di integrare regole di carattere generale.

OBBLIGO DI CONOSCENZA DEL MODELLO

È obbligo dei dirigenti, dei dipendenti e dei collaboratori di T Bridge conoscere il Codice Etico e, nelle Sue parti essenziali, il presente Modello.

L'ORGANISMO DI VIGILANZA

IDENTIFICAZIONE DELL'ORGANISMO DI VIGILANZA

In ottemperanza a quanto previsto all'art. 6, lettera b, del Decreto, che prevede che il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne il relativo aggiornamento, sia affidato ad un organismo della Società, dotato di autonomi poteri di iniziativa e controllo, T Bridge, subito dopo l'adozione del presente Modello, ha proceduto alla nomina di un Organismo di Vigilanza, che risponderà direttamente all'organo direttivo, composto da membri che, per numero, specifiche competenze e qualità personali e morali, diano garanzia del corretto perseguimento delle finalità imposte dal Decreto.
In considerazione della peculiarità delle proprie attribuzioni e dei propri requisiti professionali, l'Organismo di Vigilanza, nello svolgimento dei compiti che gli competono, si avvarrà del supporto di altre funzioni aziendali di T Bridge che di volta in volta si rendessero utili per il perseguimento del fine detto.
L'Organismo di Vigilanza della Società si avvale del supporto delle strutture aziendali specializzate che cui viene affidato il compito di esaminare le richieste di controllo e vigilanza inoltrate dall'Organismo di Vigilanza, nonché dalle altre unità aziendali di T Bridge che possono essere definite a rischio ai sensi del Decreto.
L'Organismo di Vigilanza nominato da T Bridge, in linea con le disposizioni del Decreto, e precisamente, da quanto si evince dalla lettura del combinato disposto degli articoli 6 e 7, e dalle indicazioni contenute nella Relazione di accompagnamento al Decreto, possiede le seguenti caratteristiche precipue:

a) autonomia e indipendenza. I requisiti di autonomia e indipendenza sono fondamentali e presuppongono che l'Organismo di Vigilanza non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo;
b) professionalità. L'Organismo di Vigilanza possiede, al suo interno, competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite all'indipendenza, garantiscono l'obiettività di giudizio;
continuità d'azione. L'Organismo di Vigilanza svolge in modo continuativo le attività necessarie per la vigilanza del Modello con adeguato impegno e con i necessari poteri di indagine; è una struttura riferibile alla Società, in modo da garantire la dovuta continuità nell'attività di vigilanza; cura l'attuazione del Modello e assicurandone costante aggiornamento; non svolge mansioni operative che possano condizionare e contaminare quella visione d'insieme sull'attività aziendale che ad esso si richiede.
FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA.
Da un punto di vista generale, all'Organismo di Vigilanza, spettano essenzialmente due tipi di attività, che tendono ad eliminare e/o ridurre i rischi di commissione dei reati, e più precisamente:
a) vigilare che i destinatari del Modello, appositamente individuati in base alle diverse fattispecie di reato, osservino le prescrizioni in esso contenute (funzione ispettiva e repressiva dei reati);
b) verificare affinche' i risultati raggiunti dall'applicazione del Modello in ordine alla prevenzione di reati e valutare la necessità o semplicemente l'opportunità di adeguare il Modello a norme sopravvenute ovvero alle nuove esigenze aziendali (funzione preventiva dei reati).
In estrema sintesi, le attività di cui sopra, sono finalizzate all'effettuazione, da parte dell'Organismo di Vigilanza, di una costante vigilanza in merito al recepimento, all'attuazione e all'adeguatezza del Modello.
Qualora emerga che lo stato di attuazione degli standard operativi richiesti sia carente spetterà all'Organismo di Vigilanza adottare tutte le iniziative necessarie per correggere tale condizione:
a) sollecitando i responsabili delle singole unità organizzative al rispetto dei modelli di comportamento;
b) indicando direttamente quali correzioni e modifiche modificazioni debbano essere apportate ai protocolli;
c) segnalando i casi di mancata attuazione del Modello ai responsabili ed agli addetti ai controlli all'interno delle singole funzioni e riportando, per i casi più gravi, direttamente all'organo direttivo.
Qualora, invece, dal monitoraggio dello stato di attuazione del Modello emerga la necessità di adeguamento dello stesso, che peraltro risulta integralmente e correttamente attuato, ma si riveli non idoneo allo scopo di evitare il rischio del verificarsi di taluno dei reati previsti dal Decreto, l'Organismo di Vigilanza dovrà attivarsi affinché vengano apportati, in tempi brevi, i necessari aggiornamenti.
Su di un piano più operativo, le suindicate funzioni si tradurranno nella seguenti azioni:
a) effettuare interventi periodici, sulla base di un programma annuale approvato dall'organo direttivo, volte all'accertamento di quanto previsto dal Modello ed in particolare vigilare:

I) affinche' le procedure ed i controlli da esso contemplati siano posti in essere e documentati in maniera conforme;
II) affinche' i principi etici siano rispettati;
III) sull'adeguatezza e sull'efficacia del Modello nella prevenzione dei reati di cui al Decreto.
b) segnalare eventuali carenze/inadeguatezze del Modello nella prevenzione dei reati di cui al Decreto e verificare che il Management provveda ad implementare le misure correttive;
c) suggerire procedure di verifica adeguate, tenendo comunque sempre presente, come rimanga in capo al Management della Società, agli organi sociali specificatamente deputati, la rispettiva responsabilità di controllo delle attività sociali;
d) avviare indagini interne straordinarie laddove si sia evidenziata o sospettata la violazione del Modello ovvero la commissione dei reati;
e) verificare periodicamente gli atti societari più significativi ed i contratti di maggior rilievo conclusi dalla società;
f) promuovere iniziative per diffondere la conoscenza e l'effettiva comprensione del Modello tra i dipendenti ed i collaboratori predisponendo la documentazione interna (istruzioni, chiarimenti, aggiornamenti) ovvero specifici seminari di formazione;
g) coordinarsi con i responsabili delle varie funzioni aziendali per il controllo delle attività nelle aree a rischio e confrontarsi con essi su tutte le problematiche relative all'attuazione del Modello (es. definizione clausole standard per i contratti, organizzazione di corsi per il personale, ecc.). In particolare, l'Organismo di Vigilanza dovrà coordinarsi con le funzioni competenti presenti in Società per i diversi profili specifici
h) coordinarsi con le altre funzioni aziendali:
I) per uno scambio di informazioni per tenere aggiornate le aree a rischio reato. In particolare, le funzioni aziendali dovranno comunicare per iscritto i nuovi rapporti con la Pubblica Amministrazione non già a conoscenza dell'Organismo di Vigilanza;
II) per tenere sotto controllo la loro evoluzione al fine di realizzare il costante monitoraggio;
III) per i diversi aspetti attinenti l'attuazione del Modello;
IV)per garantire che le azioni correttive necessarie a rendere il Modello adeguato ed efficace vengano intraprese tempestivamente;
i) richiedere di mantenere il Modello aggiornato, adeguandolo alle normative sopravvenute ovvero a mutamenti organizzativi della Società e/o a differenti esigenze aziendali;
j) richiedere l'aggiornamento periodico della mappa delle attività a rischio, e verificarne l'effettivo aggiornamento attraverso il compimento di verifiche periodiche puntuali e mirate sulle attività a rischio. A tal fine all'Organismo di Vigilanza devono essere segnalate da parte del management e da parte degli addetti alle attività di controllo, nell'ambito delle singole funzioni, le eventuali situazioni che possono esporre l'Azienda al rischio di reato;

k) raccogliere, elaborare e conservare tutte le informazioni rilevanti ricevute sul rispetto del Modello, nonché aggiornamento della lista delle informazioni che allo stesso devono essere trasmesse;
l) verificare che gli elementi previsti dalle singole Parti Speciali del presente Modello siano comunque adeguate e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto.
A tal fine, l'Organismo di Vigilanza deve avere libero accesso, senza la necessità di alcun consenso preventivo, salvi i casi in cui tale consenso preventivo sia reso necessario da leggi e regolamenti, alle persone e a tutta la documentazione aziendale, nonché la possibilità di acquisire dati ed informazioni rilevanti dai soggetti responsabili.
L'Organismo di Vigilanza deve essere inoltre dotato di un budget adeguato all'espletamento delle attività necessarie al corretto svolgimento dei compiti (es. consulenze specialistiche, trasferte ecc.) e deve avere la possibilità di avvalersi di consulenti esterni, coordinandosi ed informando preventivamente le funzioni aziendali interessate.
In caso di Organismo di Vigilanza in forma collegiale, questo, in relazione agli aspetti concernenti la calendarizzazione delle attività, le modalità di verbalizzazione delle riunioni, la disciplina dei flussi informativi, la nomina dell'eventuale Presidente e Segretario, le modalità di convocazione, l'Organismo di Vigilanza stesso, dovrà emanare un regolamento a disciplina di tali aspetti, da ratificarsi da parte dell'organo direttivo.

REPORTING DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza, salve le ulteriori variazioni strutturali connesse all'evoluzione del Modello, osserverà due linee di reporting con diverso riferimento temporale:
a) reporting periodico con cadenza almeno annuale al Collegio Sindacale, o altro organo di controllo equipollente, ed all'organo di gestione;
b) reporting continuativo al Collegio Sindacale, o ad altro organo di controllo equipollente, ed all'organo di gestione.
Premesso che la responsabilità del Modello permane in capo all'organo direttivo della Società, l'Organismo di Vigilanza riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità.
Più specificatamente, l'Organismo di Vigilanza nei confronti dell'organo direttivo, ha la responsabilità di:
a) comunicare, all'inizio di ciascun esercizio, il piano delle attività che intende svolgere per adempiere ai compiti assegnatigli;
b) comunicare periodicamente lo stato di avanzamento del programma definito ed eventuali cambiamenti apportati al piano, motivandoli;
c) comunicare immediatamente eventuali problematiche significative scaturite dalle attività;
d) relazionare, almeno annualmente, al Collegio Sindacale o ad altro organo di controllo equipollente, in merito all'attuazione del Modello da parte di T Bridge.

Con cadenza annuale, in concomitanza con l'assemblea di approvazione del bilancio, l'Organismo di Vigilanza predisporrà una relazione avente ad oggetto gli eventi maggiormente significativi che abbiano caratterizzato la vita della Società dal punto di vista di quanto forma oggetto del Decreto.
La convocazione dell'Organismo di Vigilanza potrà essere chiesta, in qualsiasi momento, dall'organo direttivo, per riferire sul funzionamento del Modello o su altre situazioni specifiche che si dovessero verificare volta per volta nello svolgimento dell'attività di T Bridge.
L'Organismo di Vigilanza potrà, inoltre, valutando le singole circostanze:
a) comunicare i risultati dei propri accertamenti ai responsabili delle funzioni e/o dei processi, qualora dalle attività scaturissero aspetti suscettibili di miglioramento. In tal caso, sarà necessario che l'Organismo di Vigilanza ottenga dai responsabili dei processi medesimi un piano delle azioni, con relativa tempistica, in ordine alle attività suscettibili di miglioramento, nonché le specifiche delle modifiche che dovrebbero essere attuate;
b) segnalare eventuali comportamenti/azioni non in linea con il Codice Etico e con le procedure aziendali al fine di:
I) acquisire, sulla base di specifiche segnalazioni ricevute, o di dati oggettivi riscontrati, tutti gli elementi da eventualmente comunicare alle strutture preposte per la valutazione e l'applicazione delle sanzioni disciplinari;
II) evitare il ripetersi dell'accadimento, dando indicazioni per la rimozione delle carenze.
Le attività indicate al punto b) dovranno, nel più breve tempo possibile, essere comunicate dall'Organismo di Vigilanza all'organo di gestione ed al Collegio Sindacale o ad altro organo di controllo equipollente, richiedendo anche il supporto delle strutture aziendali in grado di collaborare nell'attività di accertamento e nell'individuazione delle azioni idonee ad impedire il ripetersi di tali circostanze.
L'Organismo di Vigilanza ha l'obbligo di informare immediatamente sia il Collegio Sindacale o altro organo di controllo equipollente, sia il Consiglio di Amministrazione, qualora la violazione riguardi i vertici dell'Azienda.

INFORMAZIONI ALL'ORGANISMO DI VIGILANZA

Al fine di agevolare l'attività dell'Organismo di Vigilanza – nonché l'accertamento delle cause/disfunzioni che avessero reso eventualmente possibile il verificarsi del reato – qualsiasi informazione, comunicazione e documentazione, anche se proveniente da terzi, riguardante l'attuazione del Modello va inoltrata all'Organismo di Vigilanza con le modalità stabilite nelle procedure di controllo.
A tal fine, T Bridge si doterà di "canali informativi dedicati" per facilitare l'afflusso di informazioni, segnalazioni e comunicazioni verso l'Organismo di Vigilanza.
I dipendenti e gli Organi societari dovranno segnalare all'Organismo di Vigilanza le notizie relative alla commissione, o alla ragionevole convinzione di commissione, dei Reati ovvero notizie in merito a

comportamenti non in linea con il Codice Etico ovvero con il Modello. La mancata segnalazione costituirà infrazione discipilnare.
I dipendenti con la qualifica di Dirigente avranno l'obbligo di segnalare all'Organismo di Vigilanza le violazioni del Modello commesse dai Dipendenti che a loro rispondono gerarchicamente, nonché di quelle eventualmente commesse da altri Dirigenti e/o da soggetti apicali.
Consulenti e collaboratori in genere saranno tenuti ad effettuare le segnalazioni relative alla commissione, o alla ragionevole convinzione di commissione, dei Reati nei limiti e con le modalità che, ove possibile, dovranno essere previste contrattualmente.
Le segnalazioni devono essere effettuate in forma scritta e non anonima e possono avere ad oggetto ogni violazione o sospetto di violazione del Modello e del Codice Etico.
Le informative acquisite dall'Organismo di Vigilanza saranno trattate, in aderenza al Codice Etico, in modo da garantire:
(a) il rispetto della persona, della dignità umana, del diritto di difesa e della riservatezza e da evitare per i segnalanti qualsiasi forma di ritorsione, penalizzazione o discriminazione, nonche'
(b) la tutela dei diritti di enti/società e persone in relazione alle quali siano state effettuate segnalazioni in mala fede e che siano risultate infondate.

L'Organismo di Vigilanza valuterà le segnalazioni ricevute con discrezionalità e responsabilità. A tal fine potrà ascoltare l'autore della segnalazione e/o il responsabile della presunta violazione, motivando per iscritto la ragione dell'eventuale autonoma decisione a non procedere.
Le procedure, aperte d'ufficio o a seguito delle predette segnalazioni, dovranno essere repertoriate secondo ordine cronologico dall'Organismo di Vigilanza in apposito registro dallo stesso conservato e la relativa documentazione dovrà essere raccolta in separati fascicoli aventi numerazione progressiva corrispondente a quella di repertorio.
Sono considerate informazioni da trasmettere obbligatoriamente all'Organismo di Vigilanza quelle riguardanti:
a) le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
b) le commissioni di inchiesta o relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al Decreto;
c) provvedimenti e/o notizie, relative a T Bridge, provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto;
d) le richieste di assistenza legale inoltrate dagli Amministratori, dai Dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per i reati previsti dal Decreto;
e) le notizie relative alla effettiva attuazione, a tutti i livelli aziendali, del Modello, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;

f) le relazioni preparate da responsabili delle varie funzioni aziendali da cui emergano fatti, eventi od omissioni anche solo potenzialmente ricollegabili a fattispecie di reato previste dal Decreto;
g) informazioni sulla evoluzione delle attività attinenti alle aree a rischio individuate dal Modello e/o sulle modifiche della organizzazione aziendale;
h) le operazioni atipiche, le relazioni della società di revisione, le copie dei verbali del Collegio Sindacale, o di altro organo di controllo equipollente, e dell'organo direttivo di T Bridge;
i) le informazioni, di qualsiasi natura e da chiunque provenienti, concernenti indagini o procedimenti, civili, amministrativi, tributari e/o penali aventi attinenza con i reati previsti dal Decreto e con le specifiche attribuzioni dell'Organismo di Vigilanza.
L'Organismo di Vigilanza potrà proporre all'organo direttivo eventuali modifiche alla casistica suindicata.
All'Organismo di Vigilanza deve essere obbligatoriamente comunicato il sistema delle deleghe di poteri e di firma in vigore in T Bridge e qualsiasi modifica ad esso riferita.

FORMAZIONE E INFORMATIVA

Ai fini dell'attuazione del Modello, la funzione Risorse Umane di T Bridge gestirà, in stretta cooperazione con l'Organismo di Vigilanza, l'attività di formazione del personale.
La formazione del personale della Società e dei collaboratori dovrà avvenire attraverso la diffusione del presente Modello e del Codice Etico, con le modalità di cui in appresso:

PERSONALE DIRIGENTE E DIPENDENTE

La formazione del personale dirigente e dipendente prevede la consegna o l'invio, anche tramite e-mail, del Codice Etico e di un Documento di Sintesi, breve, essenziale e chiaro, della normativa introdotta con il Decreto e del Modello adottato dalla Società.
Saranno poi organizzate specifiche attività di informazione/formazione sull'argomento, con le modalità che verranno stabilite dall'unità aziendale preposta, in collaborazione con l'Organismo di Vigilanza.
Saranno, inoltre, organizzate periodicamente attività di aggiornamento finalizzate all'informazione a tutto il personale circa eventuali modifiche e/o integrazioni del presente Modello.
Per tutti i nuovi assunti, oltre alla consegna del Codice Etico e del Documento di Sintesi, allegati alla lettera di assunzione, verranno organizzati specifici eventi informativi/formativi sull'argomento.
Nel corso degli incontri di informazione/formazione verrà specificato ai dipendenti che essi sono tenuti a conoscere il Modello ed a darvi attuazione, nonché a suggerire all'Organismo di Vigilanza eventuali carenze.
Al termine degli eventi di informazione/formazione ai dipendenti verrà fatta sottoscrivere dichiarazione attestante la partecipazione agli stessi.
Viene garantito il diritto di accesso dei dipendenti al testo integrale del Modello, sia in forma cartacea che elettronica.

A tutti i componenti dell'organo di gestione della società verrà consegnata copia del Modello e del Codice Etico e sarà fatta loro sottoscrivere dichiarazione di impegno all'osservanza degli stessi.

INFORMATIVA A COLLABORATORI ESTERNI E TERZE PARTI

Dovranno essere forniti a soggetti esterni a T Bridge (Rappresentanti, Agenti, Consulenti, ecc.) apposite informative sulle politiche e le procedure adottate da T Bridge sulla base del Modello e del Codice Etico.

Per quanto possibile tali informative e le misure adottate per prevenire i reati di cui al Decreto, dovranno formare oggetto di sottoscrizione di apposite clausole contrattuali con gli stessi.

Ai collaboratori verrà data specifica informativa nella lettera di instaurazione del rapporto di collaborazione, e verrà trasmesso, con vincolo di accettazione in forma espressa, il Codice Etico della Società. Inoltre, il Codice Etico verrà menzionato nella documentazione promozionale della società.

La Società, previa proposta dell'Organismo di Vigilanza, potrà, inoltre:

a) fornire ai collaboratori adeguate informative sulle politiche e le procedure indicate nel presente Modello;

b) dotare i collaboratori di testi contenenti le clausole contrattuali utilizzate al riguardo.

SISTEMA DISCIPLINARE

La predisposizione di un efficace sistema disciplinare per la violazione delle prescrizioni contenute nel Modello è condizione essenziale per garantire l'effettività del Modello stesso.

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

L'applicazione delle sanzioni disciplinari determinate ai sensi del Decreto prescinde dall'esito di eventuali procedimenti penali, in quanto le regole imposte dal modello sono assunte da T Bridge in piena autonomia, con lo scopo di regolamentare in senso etico le proprie condotte.

In tale direzione, T Bridge si avvarrà di un sistema disciplinare basato sulle seguenti linee d'indirizzo:

a) il sistema disciplinare sarà diversamente strutturato a seconda dei soggetti destinatari e tenendo conto delle limitazioni dettate dalle legislazioni locali;

b) il sistema disciplinare individuerà esattamente le sanzioni disciplinari da adottarsi nei confronti dei soggetti destinatari, per il caso in cui questi ultimi si rendessero responsabili di violazioni, infrazioni, elusioni, imperfette o parziali applicazioni delle prescrizioni contenute nel Modello, il tutto nel rispetto delle relative disposizioni dei contratti collettivi e delle prescrizioni legislative applicabili;

c) il sistema disciplinare dovrà prevedere una apposita procedura di irrogazione delle sanzioni, nel rispetto delle procedure previste dalla legislazione locale;

d) il sistema disciplinare introdurrà idonee modalità di pubblicazione e di diffusione del relativo codice.

MODELLO E CODICE ETICO

Il Codice Etico ed il Modello sono due strumenti complementari ed integrati.

Il Codice Etico è stato adottato in via autonoma per comunicare a tutti i soggetti cointeressati i principi di deontologia aziendale cui T Bridge intende uniformarsi, anche indipendentemente da quanto stabilito dal Decreto.

Il Modello risponde, invece, più specificatamente, alle prescrizioni contenute nel Decreto, ha portata ristretta nell'ambito aziendale e tende a prevenire quelle particolari tipologie di rischi/reati previsti dal Decreto stesso.

PARTE SPECIALE "A"

REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

LE FATTISPECIE DI REATO

Al fine di divulgare la conoscenza degli elementi essenziali dei reati cd. "sensibili" per l'attività di T Bridge, riportiamo qui di seguito una sintetica descrizione delle condotte cui è collegata, secondo le previsioni del Decreto, anche una responsabilità amministrativa a carico della Società.
Reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 D.Lgs.231/2001) (Postilla aggiornamento 2020)
Malversazione a danno dello Stato o di altro ente pubblico (art. 316-bis c.p.);
Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico o delle Comunità europee (art.316-ter c.p.);
truffa in danno dello Stato o di altro ente pubblico o delle Comunità Europea (art.640 comma 2, n.1, c.p.);
truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.);
corruzione per un atto d'ufficio (art. 318 c.p.);
pene per il corruttore (art. 321 c.p.);
corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.);
circostanze aggravanti (art. 319-bis c.p.);
corruzione in atti giudiziari (art. 319-ter c.p.);
istigazione alla corruzione (art. 322 c.p.);
concussione (art. 317 c.p.);
induzione indebita a dare o promettere utilità (art. 319 quater c.p.);
peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte Penale Internazionale o degli Organi delle Comunità Europee e di funzionari delle Comunità Europee e di stati esteri (art. 322 bis c.p.);
corruzione di persona incaricata di pubblico servizio (art. 320 c.p.)
Traffico di influenze illecite (art. 346 c.p.) (Postilla aggiornamento 2020)

Reati legati alla corruzione ed alla concussione (artt. 24 - 25 Decreto):

MALVERSAZIONE A DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (art. 316-bis c.p.)

Viene punito chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità.

INDEBITA PERCEZIONE DI CONTRIBUTI, FINANZIAMENTI O ALTRE EROGAZIONI DA PARTE DELLO STATO O DI ALTRO ENTE PUBBLICO (art. 316-ter c.p.)

Viene punito chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sè o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee

CONCUSSIONE (art. 317 c.p.)

Viene punito il pubblico ufficiale o l'incaricato di un pubblico servizio, che, abusando della sua qualità o dei suoi poteri, costringe o induce taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro od altra utilità. In base ai principi generali del diritto penale, può essere punito anche il soggetto, ancorché non pubblico ufficiale, che si renda compartecipe del reato.

CORRUZIONE PER UN ATTO D'UFFICIO (art. 318 c.p.)

Viene punito il pubblico ufficiale, che, per compiere un atto del suo ufficio, riceve, per sè o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa. In base ai principi generali del diritto penale, può essere punito anche il soggetto, ancorchè non pubblico ufficiale, che si renda compartecipe del reato.

CORRUZIONE PER UN ATTO CONTRARIO AI DOVERI D'UFFICIO (art. 319 c.p.)

Viene punito il pubblico ufficiale, che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sè o per un terzo, denaro od altra utilità, o ne accetta la promessa. In base ai principi generali del diritto penale, può essere punito anche il soggetto, ancorchè non pubblico ufficiale, che si renda compartecipe del reato.

CORRUZIONE IN ATTI GIUDIZIARI (art. 319-ter c.p.)

Viene punito il pubblico ufficiale nell'ipotesi in cui i fatti indicati negli articoli 318 e 319 del codice penale sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo. In base ai principi generali del diritto penale, può essere punito anche il soggetto, ancorché non pubblico ufficiale, che si renda compartecipe del reato.

INDUZIONE INDEBITA A DARE O PROMETTERE UTILITA' (art. 319 quater c.p.)

Il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito.

Allo stesso modo è punito chi dà o promette denaro o altra utilità.

CORRUZIONE DI PERSONE INCARICATE DI PUBBLICO SERVIZIO (art. 320 c.p.)

Le condotte di corruzione per esercizio della funzione o per un atto contrario ai doveri d'ufficio si applicano anche all'incaricato di pubblico servizio.

ISTIGAZIONE ALLA CORRUZIONE (art. 322 c.p.)

Viene punito chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato, per indurlo a compiere, omettere o ritardare un atto del suo ufficio, qualora l'offerta o la promessa non sia accettata.

PECULATO, CONCUSSIONE, INDUZIONE INDEBITA A DARE O PROMETTERE UTILITA', CORRUZIONE ED ISTIGAZIONE ALLA CORRUZIONE DI MEMBRI DELLA CORTE PENALE INTERNAZIONALE O DEGLI ORGANI DELLE COMUNITA' EUROPEE E DI FUNZIONARI DELLE COMUNITA' EUROPEE E DEGLI STATI ESTERI (ART. 322 BIS C.P.)

Reati legati alla truffa ed alla frode (artt. 24 - 25 Decreto)

TRUFFA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (art. 640, 2° comma, n. 1 c.p.)

Viene punito Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sè o ad altri un ingiusto profitto con altrui danno, nell'ipotesi in cui il fatto sia commesso in danno dello Stato o di altro ente pubblico

TRUFFA AGGRAVATA PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE (art. 640-bis c.p.)

Viene punito colui che commette una truffa con riguardo a contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

FRODE INFORMATICA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (art. 640-ter c.p.)

Viene punito chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, o abusando della qualità di operatore del sistema, procura a sè o ad altri un ingiusto profitto con altrui danno.

Traffico di influenze illecite (art. 346 bis c.p.): la fattispecie si concretizza nel comportamento di chi, fuori dai casi di corruzione, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale. (Postilla aggiornamento 2020)

LE ATTIVITA' SENSIBILI

Attraverso l'analisi della società, è stato possibile individuare le attività sensibili, nelle quali può esistere, seppur in forma ridotta, il rischio di commissione dei reati previsti dagli artt. 24 e 25 del d.lgs. 231/01. Le attività sono le seguenti:

1. negoziazione/stipulazione/esecuzione di contratti e convenzioni con enti pubblici;
2. partecipazione a gare indette da enti pubblici;
3. adempimenti legati alla normativa sulla sicurezza sul posto di lavoro e relativi rapporti con le autorità preposte al controllo, anche in caso di ispezioni;
4. selezione, assunzione, valutazione, formazione e sviluppo del personale, ed amministrazione degli aspetti retributivi e previdenziali connessi al personale dipendente e ai collaboratori esterni e dei rapporti con enti previdenziali ed assistenziali (INPS, INAIL, uffici di collocamento, ecc.);
5. gestione dei rapporti con Autorità Garante per la Privacy, Banca d'Italia, Registration Authority ed altri enti, sia nell'attività ordinaria che in caso di ispezioni, degli adempimenti antiriciclaggio, e delle autorizzazioni e licenze per l'esercizio di attività aziendali;
6. gestione dei rapporti con l'amministrazione finanziaria per gli adempimenti tributari e fiscali;
7. gestione delle richieste di contributi/sovvenzioni provenienti da soggetti pubblici;

gestione di applicativi software forniti da soggetti pubblici e trasmissione telematica di dati a autorità di vigilanza, amministrazione finanziaria e altri soggetti pubblici.

AREE AZIENDALI A RISCHIO

Sono considerate a rischio tutte le aree aziendali che hanno contatti e rapporti con la Pubblica Amministrazione (Direzione, Risorse Umane, Amministrazione e Finanza, Acquisti e logistica, Legale Societario e Affari Generali, Strategia, Sviluppo Business)

IL SISTEMA DEI CONTROLLI

Gli standard di controllo fissi

Gli standard di controllo "fissi" (validi per tutte le attività "sensibili") sono i seguenti:

A) Segregazione delle attività: si richiede la costante applicazione del principio di separazione delle attività tra chi esegue, chi controlla e chi autorizza.

B) Norme/Circolari: è prescritto che le disposizioni aziendali siano sempre idonee a fornire chiari principi generali di riferimento per la regolamentazione dell'attività.

C) Poteri di firma e poteri autorizzativi: si prevede l'obbligo di fissare costantemente regole formalizzate per l'esercizio di poteri autorizzativi e poteri di firma.

Tracciabilità: si richiede l'esistenza di strumenti che, in relazione ad ogni comunicazione scritta relativa a ciascuna attività, assicurino la tracciabilità degli elementi informativi e delle relative fonti.

Controlli specifici

Di seguito si individuano, i controlli specifici previsti per le attività sensibili come sopra individuate. Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.

Divieto di stipulazione di contratti in autonomia:

il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non può da solo e liberamente stipulare i contratti che ha negoziato.

Tutti gli atti e le comunicazioni formali devono essere gestiti e firmati solo da coloro che sono dotati di idonei poteri in base alle norme interne.

Divieto di accesso a risorse finanziarie in autonomia:

il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non può da solo e liberamente accedere alle risorse finanziarie e/o autorizzare disposizioni di pagamento.

Devono essere stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la definizione di soglie quantitative di spesa, coerenti con le competenze gestionali e le responsabilità organizzative.

Le operazioni che comportano utilizzazione o impiego di risorse economiche o finanziarie devono avere una causale espressa ed essere documentate e registrate in conformità ai principi di correttezza professionale e contabile.

L'impiego di risorse finanziarie deve essere motivato dal soggetto richiedente, anche attraverso la mera indicazione della tipologia di spesa alla quale appartiene l'operazione.

Nessun pagamento o incasso può essere regolato in contanti, salvo che vi sia espressa autorizzazione da parte della Direzione della Società e comunque per importi che non superino somme gestite attraverso la piccola cassa.

La Società deve avvalersi solo di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea.

Sono preventivamente stabiliti, in funzione della natura della prestazione svolta, limiti quantitativi all'erogazione di anticipi di cassa e al rimborso di spese sostenute da parte del personale della Società. Il rimborso delle spese sostenute deve essere richiesto attraverso la compilazione di modulistica specifica e solo previa produzione di idonea documentazione giustificativa delle spese sostenute.

Divieto di conferimento di contratti di consulenza o similari in autonomia:

il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non può da solo e liberamente conferire incarichi di consulenza / prestazioni professionali.

Divieto di conferimento e/o stipula di contratti di intermediazione in autonomia:

il soggetto che gestisce rapporti con controparti nell'ambito delle fattispecie di attività sensibili non può da solo e liberamente conferire e/o stipulare incarichi/contratti di intermediazione.

I consulenti esterni sono scelti in base ai requisiti di professionalità, indipendenza e competenza.
L'incarico è conferito per iscritto con indicazione del compenso pattuito e del contenuto della prestazione.
I contratti che regolano i rapporti con i consulenti devono prevedere apposite clausole che richiamino gli adempimenti e le responsabilità derivanti dal Decreto e dal rispetto dei principi fondamentali del Modello, che deve essere loro comunicato assieme al Codice di Comportamento.
Non devono essere corrisposti compensi o parcelle in misura non congrua rispetto alle prestazioni rese alla Società o non conformi all'incarico conferito, alle condizioni o prassi esistenti sul mercato o alle tariffe professionali vigenti per la categoria interessata.
Divieto di concessione di utilità in autonomia:
il soggetto che intrattiene rapporti e/o effettua negoziazioni con la Pubblica Amministrazione non può da solo e liberamente concedere qualsivoglia utilità.
Divieto di assunzione di personale in autonomia:
il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non può da solo e liberamente procedere ad assunzioni di personale (rapporti di lavoro);
Criteri di selezione del personale:
devono essere formalizzati criteri oggettivi di selezione dei candidati.
Le funzioni che richiedono la selezione e assunzione del personale, devono formalizzare la richiesta attraverso la compilazione di modulistica specifica e nell'ambito di un budget annuale. La richiesta deve essere autorizzata dal responsabile competente. I candidati devono essere sottoposti ad un colloquio valutativo.
Devono essere preventivamente accertati e valutati i rapporti, diretti o indiretti, tra il candidato e la Pubblica Amministrazione.
Il sistema di valutazione del personale ed i sistemi incentivanti devono essere improntati a criteri di oggettività, di misurabilità e di congruità in relazione ai vari livelli aziendali;
Deve essere individuato, secondo i livelli gerarchici presenti in azienda, il responsabile che autorizza ex ante o ex post (a seconda delle tipologie di trasferte, missioni o viaggi al di fuori dei consueti luoghi di lavoro), le note spese ai soggetti richiedenti.
Sicurezza informatica:
devono esistere adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nelle leggi vigenti e negli standard internazionali di Information Security Management System.
Acquisizione/gestione di contributi/sovvenzioni/ finanziamenti:
deve esistere segregazione di ruoli e responsabilità nelle fasi di istanza, gestione e rendicontazione in riferimento alla gestione dei finanziamenti, contribuzioni o altre agevolazioni.

Al responsabile interno per l'attuazione dell'operazione deve essere dato il compito di verificare che le dichiarazioni e la documentazione presentata al fine di ottenere il finanziamento o il contributo siano complete e rappresentino la reale situazione economica, patrimoniale e finanziaria della Società.
Le risorse finanziarie ottenute come contributo, sovvenzione o finanziamento pubblico devono essere destinate esclusivamente alle iniziative e al conseguimento delle finalità per le quali sono state richieste e ottenute.
L'impiego di tali risorse è sempre motivato dal soggetto richiedente, che ne attesta la coerenza con le finalità per le quali il finanziamento è stato richiesto e ottenuto.
Obbligo di collaborazione:
devono esistere direttive che sanciscano l'obbligo alla massima collaborazione e trasparenza nei rapporti con le Autorità di vigilanza.
Obbligo di segnalazione, archiviazione e conservazione nelle ispezioni:
in caso di ispezioni, deve esistere uno strumento normativo per l'identificazione di un soggetto responsabile per la gestione dei rapporti con l'Autorità di vigilanza, appositamente delegato dai vertici aziendali. Tale strumento normativo deve disciplinare anche le modalità di archiviazione e conservazione delle informazioni fornite, nonché l'obbligo di segnalazione iniziale e di relazione sulla chiusura delle attività sia verso i vertici aziendali che verso l'ODV

PARTE SPECIALE "B"

REATI SOCIETARI

LE FATTISPECIE DI REATO

Riportiamo qui di seguito una sintetica descrizione delle condotte cui è collegata, secondo le previsioni del Decreto, anche una responsabilità amministrativa a carico della Società.
Reati legati ai rapporti societari (art. 25 ter Decreto)
FALSE COMUNICAZIONI SOCIALI (art. 2621 c.c.); Vengono puniti gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, sindaci e i liquidatori, i quali al fine di conseguire per sè o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, espongono fatti materiali non rispondenti al vero ancorchè oggetto di valutazioni ovvero omettono informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale, o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione. La punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento. In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 per cento da quella corretta.
FALSE COMUNICAZIONI SOCIALI IN DANNO DEI SOCI O DEI CREDITORI (art. 2622 c.c.); modificato in False comunicazioni sociali delle società quotate ex art. 2622 cc (Postilla aggiornamento 2020)
Vengono puniti gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro paese dell'Unione europea, i quali al fine di conseguire per sè o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali (previste dalla legge,) dirette ai soci o al pubblico, consapevolmente espongono fatti materiali non rispondenti al vero (ancorché oggetto di valutazioni,) ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo concretamente idoneo ad

indurre altri in errore (i destinatari sulla predetta situazione) sono puniti con la pena della reclusione da tre a otto anni.
Le disposizioni di cui ai commi precedenti si applicano anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

FALSO IN PROSPETTO (art. 2623 c.c.)
Viene punito chiunque, allo scopo di conseguire per sè o per altri un ingiusto profitto, nei prospetti richiesti ai fini della sollecitazione all'investimento o dell'ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari del prospetto, espone false informazioni od occulta dati o notizie in modo idoneo ad indurre in errore i suddetti destinatari.
FALSITÀ NELLE RELAZIONI O NELLE COMUNICAZIONI DELLE SOCIETÀ DI REVISIONE (art. 2624 c.c.)
Sono puniti i responsabili della revisione i quali, al fine di conseguire per sè o per altri un ingiusto profitto, nelle relazioni o in altre comunicazioni, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni, attestano il falso od occultano informazioni concernenti la situazione economica, patrimoniale o finanziaria della società, ente o soggetto sottoposto a revisione, in modo idoneo ad indurre in errore i destinatari delle comunicazioni sulla predetta situazione.
IMPEDITO CONTROLLO (art. 2625 c.c.)
Sono puniti gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci, ad altri organi sociali.
INDEBITA RESTITUZIONE DEI CONFERIMENTI (art. 2626 c.c.)
Sono puniti gli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli.
ILLEGALE RIPARTIZIONE DEGLI UTILI E DELLE RISERVE (art. 2627 c.c.)
Sono puniti gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite.
ILLECITE OPERAZIONI SULLE AZIONI O QUOTE SOCIALI O DELLA SOCIETÀ CONTROLLANTE (art. 2628 c.c.)
Sono puniti gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge. Inoltre, sono puniti gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

OPERAZIONI IN PREGIUDIZIO DEI CREDITORI (art. 2629 c.c.)

Sono puniti gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.

FORMAZIONE FITTIZIA DEL CAPITALE (art. 2632 c.c.)

Sono puniti gli amministratori e i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

INDEBITA RIPARTIZIONE DEI BENI SOCIALI DA PARTE DEI LIQUIDATORI (art. 2633 c.c.)

Sono puniti i liquidatori che, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionano danno ai creditori.

CORRUZIONE TRA PRIVATI (art. 2635 c.c.)

Sono puniti gli amministratori, i direttori generali, i dirigenti preposti alla redazione di documenti contabili/societari, i sindaci, i liquidatori e i responsabili della revisione, i quali, a seguito della dazione o della promessa di utilità, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio, cagionando nocumento alla società. È altresì punibile chi dà o promette l'utilità.

ILLECITA INFLUENZA SULL'ASSEMBLEA (art. 2636 c.c.)

È punito chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sè o ad altri un ingiusto profitto.

AGGIOTAGGIO (art. 2637 c.c.)

È punito chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.

OSTACOLO ALL'ESERCIZIO DELLE FUNZIONI DELLE AUTORITÀ PUBBLICHE DI VIGILANZA (art. 2638 c.c.)

Sono puniti gli amministratori, i direttori generali, i dirigenti preposti alla redazione di documenti contabili/societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano

con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima. Sono altresì puniti gli amministratori, i direttori generali, i sindaci e i liquidatori di società, o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni. Corruzione tra privati (art. 2635 cc): Salvo che il fatto non costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da 1 a 3 anni. Si applica la stessa pena se il fatto è commesso da chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al periodo precedente. Si applica la pena della reclusione fino ad un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma. Chi, anche per interposta persona, promette o dà danaro o altra utilità non dovuti alle persone indicate nel primo e nel secondo comma, è punito con le pene ivi previste.
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.): chiunque offre o promette denaro o altra utilità non dovuta agli amministratori, ai direttori generali, ai dirigenti preposto alla redazione di documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinchè compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo. (Postilla aggiornamento 2020).

LE ATTIVITA' SENSIBILI

Dall'analisi effettuata, è stato possibile individuare le attività sensibili, nelle quali può esistere, seppur in forma ridotta, il rischio di commissione dei reati previsti dall'art. 25 ter del d.lgs. 231/01. Le attività sono le seguenti:
1. tenuta della contabilità, predisposizione di bilanci, relazioni periodiche, comunicazioni di dati societari ad enti pubblici e privati oltre che ad autorità di vigilanza, adempimenti di oneri informativi obbligatori per legge e/o per disposizioni di autorità di vigilanza;
2. gestione dei rapporti con organi sociali di controllo, società di revisione e altri organi societari; redazione, tenuta e conservazione dei documenti su cui gli stessi potrebbero esercitare il controllo;
3. adempimenti legislativi legati alla gestione di operazioni sul capitale al fine di salvaguardare il patrimonio della società (operazioni su azioni o quote; acconti su dividendi; conferimenti, fusioni e scissioni; distribuzione utili);
attività di preparazione delle riunioni assembleari.

AREE AZIENDALI A RISCHI.

Sono considerate a rischio le aree aziendali che si occupano delle attività sopra elencate: direzione, amministrazione, finanza e controllo, legale societario e affari generali.

IL SISTEMA DEI CONTROLLI

Sono stati individuati i seguenti standard di controllo specifici:

1) Relativamente all'attività sensibile di cui al punto 1, gli standard di controllo specifici sono i seguenti:

- Norme contabili: lo standard prescrive che siano portate a conoscenza del personale coinvolto in attività di predisposizione del bilancio, norme di che definiscono con chiarezza i principi contabili da adottare per la definizione delle poste del bilancio e le modalità operative per la loro contabilizzazione. Tali norme devono essere tempestivamente aggiornate dall'ufficio competente alla luce delle novità della normativa e diffuse ai destinatari sopra indicati.
- Istruzioni di chiusura contabile: lo standard dispone la formazione e diffusione di istruzioni che indichino dati e notizie che è necessario fornire agli uffici coinvolti nel processo di redazione del bilancio in relazione alle chiusure annuali ed infrannuali, nonché le relative modalità e la tempistica.
- Flusso informativo e procedure: lo standard prescrive l'esistenza di una procedura formalizzata che preveda ruoli e responsabilità relativamente al flusso informativo da fornire ai vari uffici coinvolti nel processo di bilancio.
- Tracciabilità: lo standard stabilisce che il sistema informatico utilizzato per la trasmissione di dati e informazioni debba garantire la tracciabilità dei singoli passaggi e l'identificazione delle postazioni che inseriscono i dati nel sistema. Il responsabile di ciascun Servizio coinvolto nel processo deve garantire la tracciabilità delle informazioni contabili non generate in automatico dal sistema.
- Lettere di attestazione: lo standard impone che il soggetto responsabile dell'attività di predisposizione del bilancio acquisisca dai responsabili delle funzioni coinvolte nel processo di bilancio una dichiarazione attestante la veridicità e completezza delle informazioni fornite ai fini della redazione del bilancio civilistico e consolidato.
- Riunioni tra Società di revisione, organo interno di controllo ed Audit Committee: lo standard prescrive che debbano essere effettuate una o più riunioni tra la Società di revisione e l'organo interno di controllo e/o tra la Società di revisione e l'Audit Committee, prima delle riunioni del consiglio di amministrazione e della relativa assemblea indette per l'approvazione del bilancio, che abbiano per oggetto la valutazione di eventuali criticità emerse nello svolgimento delle attività di revisione.
- Attività di formazione: lo standard dispone che debbano essere svolte attività di formazione di base, rivolte agli uffici coinvolti nella redazione del bilancio e degli altri documenti connessi, in merito alle principali nozioni ed alle problematiche giuridico-contabili inerenti il bilancio.

- Conservazione del fascicolo di bilancio: lo standard impone l'esistenza di regole formalizzate che identifichino ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio, dall'approvazione del consiglio di amministrazione al deposito e pubblicazione (anche informatica) dello stesso fino alla relativa archiviazione.

2) Relativamente all'attività sensibile di cui al punto 2, gli standard di controllo specifici sono i seguenti:
- Direttive: lo standard prescrive che debbano esistere direttive che sanciscano l'obbligo alla massima collaborazione e trasparenza nei rapporti con Collegio Sindacale o altro organo di controllo equipollente, Società di Revisione e altri organi societari.
- Selezione della società di revisione e sua indipendenza nel mandato: lo standard richiede che debba esistere una disposizione aziendale che regolamenti le fasi di selezione della società di revisione contabile e che debbano altresì esistere regole per salvaguardare l'indipendenza della società di revisione nel periodo del mandato.
- Verifica del grado di indipendenza: lo standard impone la verifica da parte dell'organo interno di controllo del grado di indipendenza della Società di Revisione alla luce delle regole e criteri fissati per la selezione e valutazione della Società di Revisione.
- Riunioni tra società di revisione, collegio sindacale e Audit Committee: lo standard richiede che vadano effettuate una o più riunioni, tra la Società di Revisione ed il Collegio Sindacale e/o tra la Società di Revisione e l'Audit Committee, aventi ad oggetto la valutazione di eventuali criticità emerse nello svolgimento delle attività di revisione.
- Obbligo di informativa verso la revisione interna: lo standard prescrive l'obbligo di comunicazione sistematica all'Internal Audit di ogni richiesta di informazioni o documentazione ricevute dall'organo amministrativo o dai suoi delegati e provenienti dai soci, da altri organi sociali o dalla società di revisione.
- Documentazione: lo standard sancisce l'obbligo di trasmissione alla società di revisione con congruo anticipo di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del CdA sui quali essa debba esprimere un parere ai sensi di legge o in base ai regolamenti interni.
- Report: lo standard prescrive l'obbligo di report periodici all'organo interno di controllo sulle informazioni richieste dalla e rese alla Società di Revisione, nonché l'obbligo di report periodico al vertice sullo stato dei rapporti con le Società di Revisione da parte dei servizi istituzionalmente deputati ai rapporti con tali soggetti.

3) Relativamente all'attività sensibile inerente il punto 3, gli standard di controllo specifici sono i seguenti:

- Documentazione: lo standard richiede la predisposizione di idonea documentazione relativa alle operazioni in esame.
- Conservazione del fascicolo di bilancio: lo standard prescrive debbano esistere regole formalizzate che identifichino ruoli e responsabilità relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio, dalla sua approvazione da parte del Consiglio di Amministrazione al deposito e pubblicazione (anche informatica) dello stesso fino alla relativa archiviazione.
- Procedure: il presente presidio impone che l'esistenza di procedure autorizzative per acquisti e vendite di partecipazioni proprie e/o in altre società (esistenza di una procedura per la valutazione, autorizzazione e gestione delle operazioni sul capitale), nonché l'esistenza di una procedura che regolamenti la predisposizione di una relazione per l'organo amministrativo che giustifichi la distribuzione di utili e riserve nel rispetto di quanto previsto dalla legge.
- Obblighi: lo standard richiede che debba esistere un obbligo di informativa e di segnalazione agli organi deputati nel caso di iniziative di operazioni sul capitale o di compravendita di azioni o altri strumenti finanziari emessi dalla Società e/o dalle società controllanti.

4) Relativamente all'attività sensibile inerente il punto 4, gli standard di controllo specifici sono i seguenti:
- Obblighi informativi: lo standard prescrive l'esistenza di una disposizione aziendale formalizzata che identifichi ruoli e responsabilità, relativamente agli obblighi informativi della Società (Registro Imprese, ecc.) con riferimento alla stipulazione di patti parasociali.
- Regolamento assembleare: lo standard richiede che debba essere adottato un regolamento assembleare, che sia adeguatamente diffuso agli azionisti.
- Regole per l'esercizio: lo standard prescrive la necessaria definizione di regole formalizzate per il controllo dell'esercizio del diritto di voto e per il controllo della raccolta ed esercizio delle deleghe di voto.
- Gestione del verbale d'assemblea: lo standard richiede che debba esistere una disposizione aziendale chiara e formalizzata che identifichi ruoli e responsabilità, relativamente alla trascrizione, pubblicazione del verbale d'assemblea e conservazione del relativo libro verbali assemblee.

T BRIDGE
BV'TECH

PARTE SPECIALE "C"

REATI IN MATERIA ANTIINFORTUNISTICA
E DI SICUREZZA SUL LAVORO

LE FATTISPECIE DI REATO

Riportiamo qui di seguito una sintetica descrizione delle condotte cui è collegata, secondo le previsioni del Decreto, anche una responsabilità amministrativa a carico della Società.
Omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25 septies Decreto)
L'ipotesi sanzionatoria concerne la consumazione dei delitti di cui agli articoli 589 c.p. (omicidio colposo) e 590, terzo comma, c.p. (lesioni personali colpose gravi o gravissime) derivanti dalla violazione delle norme sulla prevenzione degli infortuni e sulla sicurezza sui luoghi di lavoro. Le lesioni personali sono gravi: se comportano una malattia che metta in pericolo la vita della persona o un'inabilità temporanea di più di quaranta giorni; se producono un indebolimento permanente di un senso o di un organo; se riguardano una donna in stato di gravidanza con conseguente acceleramento del parto. Le lesioni personali sono gravissime: se comportano una malattia insanabile; se comportano la perdita di un senso o di un arto o, la mutilazione di un arto, o la perdita dell'uso di un organo o della capacità di procreare, o una permanente e grave difficoltà di parlare; se ne derivi la deformazione o lo sfregio permanente del viso.

LE ATTIVITA' SENSIBILI
Le attività sensibili legate alle ipotesi sanzionatorie previste dall'articolo 25 septies del Decreto sono legate al mancato rispetto da parte della società del generale obbligo di protezione nei confronti dei propri dipendenti e, nello specifico, alla mancata adozione da parte della società delle misure previste dalla normativa speciale (tra cui quelle di cui al decreto legislativo 9.4.2008, n. 81 ed alla relativa normativa connessa e correlata).
Con particolare riferimento alla specifica attività svolta dalla società, le aree e le attività sensibili sono dettagliatamente individuate nel documento di valutazione dei rischi predisposto dalla società ai sensi dell'articolo 28 del decreto legislativo n. 81/2008 cui il presente Modello espressamente rinvia.

IL SISTEMA DEI CONTROLLI

Le prescrizioni volte a prevenire la violazione della normativa antinfortunistica e di tutela della salute e della sicurezza dei lavoratori sono specificamente individuate nel documento di valutazione dei rischi che la società ha adottato in base a quanto stabilito dall'art. 28 del decreto legislativo n. 81/2008.
Tra gli standard richiesti in rapporto all'attività svolta dalla società vanno segnalati quelli:
- di carattere informativo e formativo periodico nei confronti dei dipendenti, di calendarizzazione di riunioni periodiche sulla sicurezza e di consultazione con i rappresentanti dei lavoratori per la sicurezza;
- di programmazione dell'attività di controllo e di verifica sotto ogni profilo dei locali di lavoro, degli strumenti ed attrezzature e degli impianti;
- relativi all'effettuazione di simulazioni e prove pratiche di allarme incendio, evacuazione, gestione delle emergenze, del primo soccorso, degli appalti;
- concernenti la tutela delle lavoratrici in stato di gravidanza;
- volti al rispetto del divieto di fumare nei locali in cui si svolge l'attività lavorativa;
- volti al rispetto delle linee guida sull'uso dei videoterminali;
- concernenti la sorveglianza sanitaria;
- di carattere disciplinare relativamente alla vigilanza sul rispetto delle procedure e delle istruzioni di lavoro ed alle ipotesi di inosservanza delle disposizioni impartite per la tutela della sicurezza e della salute sul lavoro;
- relative all'acquisizione delle certificazioni obbligatorie per legge;
- concernenti le verifiche periodiche sull'applicazione ed efficacia delle procedure adottate;
- alla registrazione delle attività.

Con particolare riferimento a quanto previsto dall'art. 30 del decreto legislativo n. 81/2008, la Società ha assunto come modello di riferimento quello dettato dalle Linee Guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28.9.2001, secondo quanto riportato nel documento denominato "Linee Guida per un sistema di gestione della salute e sicurezza sul lavoro (SGSL)", allegato al presente Modello a formarne ad ogni effetto parte integrante e sostanziale.

T BRIDGE
BV'TECH

PARTE SPECIALE "D"

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI
LE FATTISPECIE DI REATO

Le fattispecie di reato previste dall'art. 24-bis del Decreto sono quelle previste:
- dall'art. 491 bis c.p., che punisce, in via residuale quale norma di chiusura, chiunque commette una falsità riguardante un documento informatico pubblico avente efficacia probatoria;
- dall'art. 615-ter c.p., che punisce l'accesso abusivo ad un sistema informatico o telematico, ossia "chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo";
- dall'art. 615-quater c.p., che punisce chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave, o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo;
- dall'art. 615 quinquies c.p., che punisce chiunque, in qualsiasi modo, diffonde apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- dall'art. 617-quater c.p., che punisce l'intercettazione, l'impedimento o l'interruzione illecita di comunicazioni informatiche o telematiche, ossia "chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe";
- dall'art. 617-quiquies c.p., l'installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche, ossia "chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi";
- dall'art. 635-bis c.p., che punisce il danneggiamento di informazioni, dati e programmi informatici, ossia "chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui";
- dall'art. 635-ter c.p., che punisce il danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità, ossia "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";

- dall'art. 635-quater c.p., che punisce il danneggiamento di sistemi informatici o telematici, ossia "chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento";

dall'art. 635-quinques c.p., che punisce il danneggiamento di sistemi informatici o telematici di pubblica utilità, ossia l'ipotesi in cui "il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento".

Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.);

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

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

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

''Perimetro di sicurezza informatico" art. 1 D. L. 105/2019: Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a cinque anni" e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote". (Postilla aggiornamento 2020)

LE ATTIVITA' SENSIBILI

Le attività sensibili legate alle ipotesi sanzionatorie previste dalla normativa in esame sono quelle concernenti la negoziazione, la stipulazione, l'esecuzione e la gestione di contratti, commesse e convenzioni sia con soggetti privati sia con enti pubblici, nonché, più in generale, l'utilizzo di sistemi informatici in dotazione alla Società e/o da questa o da suoi dipendenti/collaboratori utilizzati e/o in qualsiasi modo raggiungibili. In particolare, le seguenti attività:

Gestione dei profili utenti e del processo di autenticazione per l'accesso alle informazioni, ai sistemi informativi, alle applicazioni, alla rete.

Gestione e protezione logica e fisica delle postazioni di lavoro.

Gestione del processo di assegnazione e dismissione degli asset IT (software e hardware).

Sicurezza fisica dei centri di elaborazioni dati e locali tecnici IT.

Gestione e protezione dei dati e delle reti.

Gestione delle comunicazioni e dell'operatività (scambio di informazioni, log management, patch management, politiche di backup, etc..).

Gestione degli incidenti e dei problemi di sicurezza informatica.

Gestione dei controlli crittografici.

Produzione e/o vendita di programmi informatici, di servizi di installazione e manutenzione di hardware,software,reti.

AREE AZIENDALI A RISCHIO

Sono considerate a rischio
le aree aziendali che si occupano delle attività sopra elencate (Area Sistemi informativi).

IL SISTEMA DEI CONTROLLI

Vale anche per le fattispecie in esame il richiamo ai seguenti standard di controllo:

A) Segregazione delle attività: si richiede la costante applicazione del principio di separazione delle attività tra chi esegue, chi controlla e chi autorizza; inoltre, allo stesso livello di attività, appare necessario un controllo incrociato nell'esecuzione delle attività materiali di utilizzo ed accesso dei sistemi informatici.

B) Norme/Circolari: è prescritto che le disposizioni aziendali siano sempre idonee a fornire chiari principi generali di riferimento per la regolamentazione dell'attività, anche per quel che concerne il rispetto della normativa in materia di protezione dei dati personali (Codice della Privacy e disposizioni dell'Autorità Garante per la Privacy).

C) Tracciabilità: si richiede l'esistenza di strumenti che assicurino la tracciabilità di ciascuna attività di utilizzo, accesso e gestioni di sistemi informatici.

D) Manuale della Qualità: si richiede l'osservanza delle specifiche e delle procedure previste dal Manuale della Qualità adottato dalla Società.

CONTROLLI SPECIFICI

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate. Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.

Controllo degli accessi.

Tale controllo prevede che:

siano definiti formalmente dei requisiti di autenticazione ai sistemi per l'accesso ai dati e per l'assegnazione dell'accesso remoto agli stessi da parte di soggetti terzi quali consulenti e fornitori;

i codici identificativi (user-id) per l'accesso alle applicazioni ed alla rete siano individuali ed univoci;

siano definiti i criteri e le modalità per la creazione delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale ed ai sistemi critici o sensibili (ad esempio, lunghezza minima della password, regole di complessità, scadenza);

gli accessi effettuati dagli utenti, in qualsiasi modalità, ai dati, ai sistemi ed alla rete siano oggetto di verifiche periodiche;

le applicazioni tengano traccia delle modifiche ai dati compiute dagli utenti;

siano definiti i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;

sia predisposta una matrice autorizzativa – applicazioni/profili/richiedente – allineata con i ruoli organizzativi in essere;

Gestione dei problemi di sicurezza informatica

Tale controllo prevede adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica, in particolare che:

siano implementati controlli di sicurezza al fine di garantire la riservatezza dei dati interni alla rete e in transito su reti pubbliche;

siano adottati meccanismi di segregazione delle reti e di monitoraggio del traffico di rete;

siano implementati meccanismi di tracciatura degli eventi di sicurezza sulle reti (ad esempio, accessi anomali per frequenza, modalità, tempi);

sia regolamentata l'implementazione e la manutenzione delle reti telematiche mediante la definizione di responsabilità e modalità operative, di verifiche periodiche sul funzionamento delle reti e sulle anomalie riscontrate; inoltre deve essere regolamentata l'esecuzione di attività periodiche di vulnerability assessment ed ethical hacking;

siano definiti i criteri e le modalità per le attività di back up che prevedano, la frequenza dell'attività, le modalità, il numero di copie, il periodo di conservazione dei dati;

la documentazione riguardante ogni singola attività sia archiviata allo scopo di garantire la completa tracciabilità della stessa.

Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi

Tale controllo prevede l'adozione di uno strumento normativo che definisca:

l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;

la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;

la confidenzialità, autenticità e integrità delle informazioni;

la sicurezza nel processo di sviluppo dei sistemi informativi.

Organizzazione della sicurezza per gli utenti esterni

Tale controllo prevede l'adozione di uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso,

gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.

Sicurezza fisica

Tale controllo prevede l'adozione di misure finalizzare a prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature, in particolare:

siano definite le credenziali fisiche di accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT quali, a titolo esemplificativo: badge, codici di accesso, pin specifici e la tracciabilità degli stessi;

siano definite le misure di sicurezza adottate, le modalità di vigilanza e la relativa frequenza, la responsabilità, il processo di reporting delle violazioni/effrazioni dei locali tecnici o delle misure di sicurezza, le contromisure da attivare;

la documentazione riguardante ogni singola attività sia archiviata allo scopo di garantire la completa tracciabilità della stessa.

T BRIDGE
BV'TECH

PARTE SPECIALE "E"

DELITTI CONTRO L'INDUSTRIA ED IL COMMERCIO (ART. 25 BIS.1)

LE FATTISPECIE DI REATO

Le fattispecie di reato previste dall'art. 25 bis.1 del Decreto sono quelle previste:

Turbata libertà dell'industria o del commercio. (art. 513 c.p.)

Illecita concorrenza con minaccia o violenza. (art. 513-bis c.p.)

Frodi contro le industrie nazionali. (art. 514 c.p.)

Frode nell'esercizio del commercio. (art. 515 c.p.)

Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale. (art.517-ter c.p.)

Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari. (art. 517-quater c.p.)

ATTIVITÀ SENSIBILI NELL'AMBITO DEI DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

Non sussistono ragioni di escludere, in via di principio, la commissione dei reati in oggetto, tranne che per il reato di vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)

Le attività sensibili nell'ambito di delitti contro l'industria ed il commercio, in considerazione dell'attuale operatività di T Bridge, sono le seguenti:

Gestione delle procedure di acquisto.

Gestione dei contratti/convenzioni con i fornitori di beni o servizi.

AREE AZIENDALI A RISCHIO

Sono considerate a rischio tutte le aree aziendali che svolgono le attività sensibili sopra individuate (Direzione, Amministrazione e Finanza, Acquisti e logistica, Legale Societario e Affari Generali).

IL SISTEMA DEI CONTROLLI

CONTROLLI GENERALI

Oltre al rigoroso rispetto del documento denominato "Codice "Etico", i controlli generali relativi alle attività in oggetto sono descritti di seguito:

Segregazione delle attività/funzioni/processo

Si richiede la costante applicazione del principio di separazione delle attività tra chi esegue, chi controlla e chi autorizza.

-Normativa aziendale e circolari interne destinate a regolamentare la specifica attività

Devono esistere disposizioni aziendali che forniscano chiari principi generali di riferimento per la regolamentazione dell'attività.

Sistema deleghe, poteri di firma e poteri autorizzativi

Devono essere stabilite ed aggiornate regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma relativamente all'attività sensibile individuata.

Tracciabilità

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurino la tracciabilità degli elementi informativi e delle relative fonti.

CONTROLLI SPECIFICI

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate. Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici ad oggi pubblicati dalle principali associazioni di categoria.

Procedure di selezione dei fornitori di beni /servizi: con riferimento a tale controllo si applica quanto previsto dai protocolli di prevenzione di cui al paragrafo G della presente Parte Speciale, concernente i reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

Misure idonee a garantire la tracciabilità del processo acquisitivo, così che emergano in maniera chiara le motivazioni a sostegno di una determinata scelta organizzativa e/o operativa: anche con riferimento a tale tipo di controllo, si applica quanto previsto dai protocolli di prevenzione di cui al paragrafo G della presente Parte Speciale concernente i reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

Prescrizioni comportamentali che prevedano il divieto di porre in essere comportamenti di qualunque natura che possano fare incorrere la società nella commissione del reato in questione ed in particolare nei confronti di quei soggetti che seguono i processi di approvvigionamento e/o le procedure di gara.

PARTE SPECIALE "F"

DELITTI CONTRO LA PERSONALITA' INDIVIDUALE (ART. 25 QUINQUIES)

REATI CONTRO LA PERSONALITA' INDIVIDUALE

Le fattispecie di reato previste dall'art. 25 quinquies del Decreto sono quelle previste:

- Detenzione di materiale pornografico (art. 600-quater).
- Pornografia virtuale (art. 600-quater.1 c.p.).
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.).

ATTIVITÀ SENSIBILI NELL'AMBITO DEI DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE

Non sussistono ragioni di escludere, in via di principio, la commissione dei reati in oggetto, con riferimento agli articoli 600 – quater c.p (detenzione di materiale pornografico) e 600 quater 1. c.p. (pornografia virtuale).

Le attività sensibili nell'ambito di delitti contro la personalità individuale, in considerazione dell'attuale operatività di T Bridge S.pA., sono le seguenti:

Promozione e/o gestione di iniziative umanitarie e di solidarietà

Gestione siti internet e intranet

AREE AZIENDALI A RISCHIO

La fattispecie di cui all'art. 25 –quinquies non è ricollegabile a specifiche attività d'impresa svolte dalla Società stessa, pertanto potrebbe essere commessa ad ogni livello aziendale.

IL SISTEMA DI CONTROLLI

CONTROLLI GENERALI

I controlli generali relativi alle attività in oggetto sono descritti di seguito.

- Segregazione delle attività/funzioni/processi.

Deve esistere separazione delle attività tra chi esegue, chi controlla e chi autorizza.

- Normativa aziendale e circolari interne destinate a regolamentare la specifica attività

Devono esistere disposizioni aziendali che forniscano chiari principi generali di riferimento per la regolamentazione dell'attività.

Sistema deleghe, poteri di firma e poteri autorizzativi

Devono essere stabilite ed aggiornate regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma relativamente all'attività sensibile individuata.

Tracciabilità

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurino la tracciabilità degli elementi informativi e delle relative fonti.

CONTROLLI SPECIFICI

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate. Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.

Prescrizioni comportamentali che comprendono:

Divieto di organizzazione "Attività Sociali" in autonomia, ovvero il soggetto responsabile dell'organizzazione di "Attività Sociali" non può da solo e liberamente conferire incarichi e stipulare contratti di tale natura;

divieto di acquisire, utilizzare, diffondere e/o cedere materiale pedo pornografico;

Sicurezza dei sistemi:

esistenza di liste dei siti ai quali è autorizzato l'accesso;

effettuazione di controlli a campione relativi ai dati ed agli accessi alla rete internet;

installazione di appositi software volti ad evitare l'accesso a dati non autorizzati o il download di files aventi contenuto riconducibile a quello vietato dalla norma penale.

Controllo accessi:

Tale standard prevede il controllo degli accessi ai sistemi informativi e esistenza di automatismi di segnalazione all'amministratore del sistema di operazioni non autorizzate, pertanto, in riferimento a tale controllo si applica quanto previsto dai protocolli di prevenzione di cui al paragrafo B della presente Parte Speciale relativa ai delitti informatici ed al trattamento illecito di dati.

T BRIDGE
BV'TECH

PARTE SPECIALE "G"

RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA E AUTORICICLAGGIO (ART. 25 OCTIES DEL DECRETO)

Ricettazione, riciclaggio ed altri reati ex art. 25 octies del Decreto

Le fattispecie di reato previste dall'art. 25 octies del Decreto sono quelle previste:

Ricettazione (art. 648 c.p.).

Riciclaggio (art. 648-bis c.p.).

Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.).

Autoriciclaggio (art. 648 ter.1 c.p.).

ATTIVITÀ SENSIBILI

L'organismo di vigilanza nella sua azione di adeguamento del MOG ha individuato le attività sensibili di seguito elencate, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita previsti dall'art. 25-octies del Decreto:

Attività di acquisto e vendita di beni e servizi in Italia e all'estero.

Gestione dei flussi finanziari, dei fondi aziendali ed impiego di disponibilità liquide attraverso l'utilizzo di ogni strumento di pagamento.

Gestione sistema dei pagamenti in genere.

Gestione di operazioni straordinarie, fusioni e acquisizioni.

AREE AZIENDALI A RISCHIO

Sono considerate a rischio tutte le aree aziendali che svolgono le attività sensibili sopra individuate (Direzione, Amministrazione e Finanza, Legale Societario e Affari Generali).

IL SISTEMA DEI CONTROLLI

CONTROLLI GENERALI

I controlli generali relativi alle attività in oggetto sono descritti di seguito e prevedono:

Separazione delle responsabilità/funzioni/processo

Deve esistere separazione delle attività tra chi esegue, chi controlla e chi autorizza.

Sistema deleghe, poteri di firma e poteri autorizzativi

Devono essere stabilite ed aggiornate regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma relativamente all'attività sensibile individuata.

Tracciabilità

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurino la tracciabilità degli elementi informativi e delle relative fonti.

CONTROLLI SPECIFICI DI PREVENZIONE

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate. Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.

Per le operazioni riguardanti l'attività di acquisto e vendita di beni e servizi i protocolli prevedono:

Definizione di indicatori di anomalia.

Siano individuati degli indicatori di anomalia che consentano di rilevare eventuali transazioni a "rischio" o "sospette" con fornitori sulla base del: profilo soggettivo della controparte (es. esistenza di precedenti penali; reputazione opinabile; ammissioni o dichiarazioni da parte della controparte in ordine al proprio coinvolgimento in attività criminose); comportamento della controparte (es. comportamenti ambigui, mancanza di dati occorrenti per la realizzazione delle transazioni o reticenza a fornirli); dislocazione territoriale della controparte (es. transazioni effettuate in paesi offshore); profilo economico-patrimoniale dell'operazione (es. operazioni non usuali per tipologia, frequenza, tempistica, importo, dislocazione geografica); caratteristiche e finalità dell'operazione (es. uso di prestanome, modifiche delle condizioni contrattuali standard, finalità dell'operazione).

Procedure standardizzate per l'approvvigionamento di beni o servizi che prevedano:

Che l'acquisto di beni e servizi sia disciplinato da contratto scritto, nel quale è chiaramente prestabilito il prezzo del bene o della prestazione o i criteri per determinarlo;

che i contratti di approvvigionamento di valore significativo siano sempre preventivamente valutati e autorizzati dal Responsabile della funzione che richiede il bene o il servizio;

Per le operazioni riguardanti la gestione dei flussi finanziari, dei fondi aziendali ed impiego di disponibilità liquide attraverso l'utilizzo di ogni strumento di pagamento e gestione sistema dei pagamenti in genere, i protocolli prevedono:

Procedure standardizzate per l'utilizzo dei mezzi finanziari che in particolare dispongano:

L'utilizzo, per la gestione dei flussi in entrata e in uscita, esclusivamente di canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione europea

La tracciabilità di tutti gli incassi e i pagamenti della Società nonché in generale di tutti i flussi di denaro della stessa;

La previsione di limiti all'autonomo impiego delle risorse finanziarie, mediante la definizione di soglie quantitative di spesa, coerenti con le competenze gestionali e le responsabilità organizzative.

La registrazione e documentazione di tutte le operazioni che comportano utilizzazione o impiego di risorse economiche o finanziarie in conformità ai principi di correttezza professionale e contabile con indicazione anche di una causale espressa.
L'impiego di risorse finanziarie motivato dal soggetto richiedente, anche attraverso la mera indicazione della tipologia di spesa alla quale appartiene l'operazione.
Il divieto di regolare tutti i pagamenti e gli incassi in contanti, salvo che via espressa autorizzazione da parte della Direzione della Società e comunque per importi che non superino somme gestite attraverso la piccola cassa;
La previsione di limiti quantitativi all'erogazione di anticipi di cassa e al rimborso di spese sostenute da parte del personale della Società. Il rimborso delle spese sostenute deve essere richiesto attraverso la compilazione di modulistica specifica e solo previa produzione di idonea documentazione giustificativa delle spese sostenute.
Per le operazioni riguardanti la gestione delle operazioni straordinarie, fusioni e acquisizioni, i protocolli prevedono che:
Formalizzazione di procedure operative relative al tipo di operazione/processo.

T BRIDGE
BV'TECH

PARTE SPECIALE "H"

DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE
(ART. 25 NOVIES DEL DECRETO)
Violazioni in materia di diritto d'autore

Le fattispecie di reato previste dall'art. 25 novies del Decreto sono quelle previste:
Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, l. 633/1941 comma 1 lett a) bis).
Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, l. 633/1941 comma 3).
Abusiva duplicazione, per trarne profitto, di programmi per elaboratore (art. 171 bis, l. 633/1941).
Importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis l. 633/1941 comma 1).
Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis l. 633/1941 comma 2).
Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter l. 633/1941).
Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetto al contrassegno o falsa dichiarazione (art. 171-septies l. 633/1941).

Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171 octies, l. 633/1941).

ATTIVITÀ SENSIBILI NELL'AMBITO DEI DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE.

Non sussistono ragioni di escludere, in via di principio, la commissione dei reati in oggetto, con riferimento al reato di abusiva duplicazione o detenzione di programmi per elaboratori o di illecito utilizzo di banche dati (Art. 171-bis L. 633/1941) ed il reato di cui all'art. 171 comma 1, lett. a-bis, L. 633/1941, di messa a disposizione del pubblico in un sistema di reti telematiche, mediante connessioni di qualsiasi genere e senza averne diritto di un'opera dell'ingegno protetta. La Società ha individuato le attività sensibili, di seguito elencate, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei reati in materia di violazione del diritto d'autore previsti dall'art. 25-novies del Decreto:

- Gestione licenze d'uso prodotti software
- Gestione sito internet aziendale.

AREE AZIENDALI A RISCHIO

È considerata a rischio in ragione delle attività sensibili sopra individuate l'area aziendale Sistemi Informativi.

IL SISTEMA DEL CONTROLLI

CONTROLLI GENERALI

Oltre al rigoroso rispetto del documento denominato "Codice "Etico" i controlli generali relativi alle attività in oggetto prevedono:

Segregazione delle attività/funzioni/processi.

Deve esistere separazione delle attività tra chi esegue, chi controlla e chi autorizza.

- Normativa aziendale e circolari interne destinate a regolamentare la specifica attività

Devono esistere disposizioni aziendali che forniscano chiari principi generali di riferimento per la regolamentazione dell'attività.

Sistema deleghe, poteri di firma e poteri autorizzativi

Devono essere stabilite ed aggiornate regole formalizzate per l'esercizio di poteri autorizzativi interni e poteri di firma relativamente all'attività sensibile individuata.

Tracciabilità

Devono esistere presidi che, in relazione ad ogni fase di svolgimento di ciascuna attività sensibile, assicurino la tracciabilità degli elementi informativi e delle relative fonti.

PROTOCOLLI SPECIFICI DI PREVENZIONE

Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate. Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.

Per le operazioni riguardanti la gestione licenze d'uso prodotti software, i protocolli prevedono:

Processi di acquisizione delle licenze dei software formalizzati in una procedura operativa interna della Società

criteri e modalità per il controllo dell'uso di software formalmente autorizzato e certificato.

verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o non licenziati e/o potenzialmente nocivi;

verifiche periodiche sulla regolarità delle licenze dei prodotti e rinnovi delle stesse ove necessario

definizione di una policy aziendale la quale preveda espressamente:

il divieto di procedere ad installazione di prodotti software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano la licenza d'uso;

il divieto di procedere ad installazione di prodotti software sul personal computer in uso in violazione delle procedure aziendali in materia;

il divieto di utilizzare software/banca dati in assenza di valida licenza, anche nel caso in cui la stessa sia solamente scaduta;

l'introduzione, nel caso la presente attività sia affidata in outsourcing, nei contratti che regolano i rapporti con i fornitori del servizio, di apposite clausole che impongono la conformità dei software forniti a leggi e normative ed in particolare alle disposizioni di cui alla Legge 633/1941 e che prevedano la manleva per la Società in caso di violazioni commesse dai fornitori del servizio stessi;

Per le operazioni riguardanti la gestione del sito internet aziendale, i protocolli prevedono:

Definizione di una policy aziendale per gli utenti, che disponga:

le regole per il corretto utilizzo di internet;

Il divieto per tutti i dipendenti di diffondere immagini, documenti o altro materiale tutelati dalla normativa in materia di diritto d'autore;

meccanismi di monitoraggio del traffico e di tracciatura degli eventi di sicurezza sulle reti (ad es. accessi anomali per frequenza, modalità, temporalità);

definizione dei requisiti di autenticazione ai sistemi per l'accesso ai dati e per l'assegnazione dell'accesso remoto agli stessi da parte di soggetti terzi quali consulenti e fornitori;

istituzione e aggiornamento di una black list di siti da cui può essere effettuato il download di chiavi di licenza e codici sorgente;
meccanismi per la tracciabilità sulle applicazioni delle modifiche ai dati ed ai sistemi compiute dagli utenti;

PARTE SPECIALE "I"

INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA
(ART. 25 DECIES DEL DECRETO)

Le fattispecie di reato previste dall'art. 25 decies del Decreto sono quelle previste:
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorita' Giudiziaria (art. 377 bis c.p.)

Attività Sensibili.
L'Organismo di Vigilanza ha individuato le attività sensibili, di seguito elencate, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei reati in materia di violazione del diritto d'autore previsti dall'art. 25-decies del Decreto:
Gestione rapporti con soggetti aziendali coinvolti in procedimenti giudiziari.
Gestione rapporti con Autorità Giudiziaria (gestione del contenzioso giudiziale e stragiudiziale di cui sia parte la Società).

AREE AZIENDALI A RISCHIO

La fattispecie di cui all'art. 25 –decies risulta essere ricollegabile a tutte le aree e funzioni che sostengono la gestione delle controversie giudiziarie avanti le Autorità (Area Legale Societario e Affari generali)

IL SISTEMA DEI CONTROLLI
CONTROLLI GENERALI

I controlli generali prevedono il rigoroso rispetto del codice etico aziendale il quale dispone, fra le altre cose, che i rapporti con l'Autorità Giudiziaria relativi a questioni riguardanti la società, sono improntati al rispetto della veridicità delle informazioni rese nelle testimonianze.
PROTOCOLLI SPECIFICI DI PREVENZIONE.
Di seguito si individuano, i controlli specifici relativi alle attività sensibili come sopra individuate. Gli standard di controllo specifici sono stati definiti sulla base degli indirizzi forniti dalla normativa di legge, dalle Linee Guida di Confindustria, dai codici a oggi pubblicati dalle principali associazioni di categoria.
I protocolli specifici prevedono:

Il divieto di porre in essere comportamenti che possano rientrare nelle fattispecie di reato richiamate dall'articolo 25 - decies d.lgs. 231/2001.

L'obbligo di prestare una fattiva collaborazione e rendere dichiarazioni veritiere ed esaustivamente rappresentative dei fatti nei rapporti con l'Autorità Giudiziaria;

L'obbligo per i Destinatari (indagato/imputato, persona informata sui fatti/testimone o teste assistito/imputato in un procedimento penale connesso) chiamati a rendere dichiarazioni innanzi all'Autorità Giudiziaria in merito all'attività lavorativa prestata, di esprimere liberamente la propria rappresentazione dei fatti o ad esercitare la facoltà di non rispondere accordata dalla legge; l'obbligo altresì di mantenere il massimo riserbo relativamente alle dichiarazioni rilasciate ed al loro oggetto, ove le medesime siano coperte da segreto investigativo;

L'obbligo per tutto il personale di avvisare il Responsabile dell'Area Affari Societari di ogni atto di citazione a testimoniare e di ogni procedimento penale che li veda coinvolti, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata o comunque ad essa attinente.

Presidi di controllo e flussi informativi verso l'Organismo di Vigilanza

Controlli da parte dell'Organismo di Vigilanza diretti a verificare la conformità delle attività aziendali ai principi espressi nella presente Parte Speciale e, in particolare, alle procedure interne in essere ed a quelle che saranno adottate in futuro, in attuazione della presente Parte Speciale.

Flussi informativi verso l'Organismo di Vigilanza relativi ad ogni atto di citazione a testimoniare e di ogni procedimento penale che veda coinvolto, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata o comunque ad essa attinente il personale della società;

Flussi informativi verso l'Organismo di Vigilanza in merito alle richieste di assistenza legale inoltrate alla Società dai dipendenti in caso di avvio di un procedimento penale a carico degli stessi.

T BRIDGE
BV'TECH

PARTE SPECIALE "L"

REATI AMBIENTALI (ART. 25 UNDECIES DEL DECRETO)

Le fattispecie di reato previste dall'art. 25 undecies del Decreto sono quelle previste:

Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis, c.p.).

Scarico di acque reflue industriali contenenti sostanze pericolose (varie ipotesi previste dall'art. 137, D.Lgs. 152/2006).

Attività di gestione di rifiuti non autorizzata (varie ipotesi previste dall'art. 256, D.Lgs. 152/2006).

Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio (art. 257, D.Lgs. 152/2006).

Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari relativi alla tracciabilità dei rifiuti (art. 258, D.Lgs. 152/2006).

Traffico illecito di rifiuti (art. 259, D.Lgs. 152/2006).

"Associazione" finalizzata al traffico illecito di rifiuti. (art. 260, D.Lgs. 152/2006).

Condotte di falsificazione e detenzione di certificazioni SISTRI falsificate (art. 260- bis, D.Lgs. 152/2006).

Emissioni in atmosfera oltre i valori limite o in violazione delle prescrizioni (art. 279,D.Lgs.152/2006).

Detenzione, importazione, esportazione o riesportazione, senza autorizzazione o con autorizzazione falsa, di specie animali e vegetali in via di estinzione (L. n. 150/1992).

Produzione, consumo, importazione, esportazione, detenzione e commercializzazione di sostanze lesive dell'ozono e dell'ambiente (L. n. 549/1993).

Inquinamento provocato dalle navi (D. Lgs. n. 202/2007).

ATTIVITÀ SENSIBILI.

L'Organismo di Vigilanza ha individuato le attività sensibili, di seguito elencate, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei reati in materia di violazione del diritto d'autore previsti dall'art. 25-undecies del Decreto:

Smaltimento di toner esausti e materiale elettronico

Violazione della normativa vigente (locale e nazionale) sulla raccolta differenziata in relazione ai rifiuti prodotti in ambienti ad uso ufficio

AREE AZIENDALI A RISCHIO

La fattispecie di cui all'art. 25 –undecies risulta non essere ricollegabile a specifiche attività d'impresa svolte dalla Società stessa, pertanto potrebbe essere commesso ad ogni livello aziendale.

IL SISTEMA DEI CONTROLLI

CONTROLLI GENERALI

I rifiuti prodotti in un ambiente ad uso ufficio sono classificabili come urbani e assimilati, pertanto vi è l'obbligo, in base alla normativa vigente a livello nazionale (D.Lgs. 152/06) e locale (circolari specifiche Regionali) di effettuare la raccolta differenziata di alcune tipologie di materiali che variano da Comune a Comune pertanto:

Tutti i Soggetti, ciascuno nella misura e con le modalità richieste dalle proprie funzioni (ed in particolare quelle riconducibili al processo di approvvigionamento), sono stati informati dell'obbligo di attenersi alle disposizioni vigenti in ordine alle modalità di detta raccolta, in particolare per questi materiali principali:

- Carta/Cartone
- Vetro
- Lattine
- Plastica
- Toner
- Neon e Componenti Elettrici
- Pile Esauste
- Farmaci scaduti

CONTROLLI SPECIFICI DI PREVENZIONE

I protocolli specifici di prevenzione prevedono che:

Le funzioni aziendali che si occupano dei processi di approvvigionamento garantiscono l'attivazione e la stipula di apposite convenzioni con enti esterni autorizzati alla raccolta (es. AMSA per le cartucce esauste / contenitori toner).

T BRIDGE
BV'TECH

PARTE SPECIALE "M"

REATI ATTINENTI ALL'IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE (ART. 25 DUODECIES DEL DECRETO)

Le fattispecie di reato previste dall'art. 25 duodecies del Decreto sono quelle previste:
Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12- bis, D. Lgs. 25 luglio 1998, n. 286).

ATTIVITÀ SENSIBILI

Non sussistono ragioni di escludere, in via di principio, la commissione del reato in oggetto,l'Organismo di Vigilanza ha individuato pertanto le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbe essere commesso il delitto previsto dall'art. 25-duodecies del D.Lgs. 231/01:

Attività di selezione ed assunzione del personale (anche non dipendente)
Gestione fornitori di servizi di pulizie e del personale interinale

AREE AZIENDALI A RISCHIO

Le aree di rischio aziendale individuate sono quelle che si occupano della selezione e gestione del personale (anche non dipendente), della selezione e gestione dei fornitori operativi, dei fornitori di servizi di pulizie e del personale interinale.

IL SISTEMA DEI CONTROLLI

CONTROLLI GENERALI

Allo scopo di prevenire la commissione del reato da ultimo introdotti, si ritiene che possa essere individuata quale efficace e sufficiente misura di prevenzione generale, l'osservanza dei principi e delle disposizioni adottate dal Codice Etico.

CONTROLLI SPECIFICI DI PREVENZIONE.

I controlli specifici prevedono la redazione di procedure aziendali che dispongano:
Di verificare al momento dell'assunzione e durante lo svolgimento di tutto il rapporto lavorativo che eventuali lavoratori provenienti da paesi terzi siano in regola con il permesso di soggiorno e, in caso di scadenza dello stesso, abbiano provveduto a rinnovarlo;

Di assicurarsi, nel caso in cui si faccia ricorso al lavoro interinale mediante apposite agenzie, che tali soggetti si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno e richiedere espressamente l'impegno a rispettare il Modello;
Di assicurarsi con apposite clausole contrattuali che eventuali soggetti terzi con cui la Società collabora (fornitori, consulenti, ecc.) si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno e richiedere espressamente l'impegno a rispettare il Modello;
Di non fare ricorso, in alcun modo, al lavoro minorile o non collaborare con società che ne facciano uso.

T BRIDGE
BV'TECH

PARTE SPECIALE "N"

REATI TRIBUTARI

(ART. 25 QUINQUIESDECIES DEL DECRETO)

N) REATI TRIBUTARI (art. 25-quinquiesdecies del decreto n. 231/01)

Le fattispecie di reato previste dall'art. 25 quinquiesdecies del Decreto sono quelle previste:

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 1, D. Lgs. n. 74/2000);
- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 2-bis D. Lgs. 74/2000);
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D. Lgs. n. 74/2000)
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, comma 1 e 2-bis, D. LGS. n. 74/2000);
- Occultamento o distruzione di documenti contabili (art. 10 D. Lgs. n. 74/2000)
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D. Lgs. n. 74/2000)

(Postilla aggiornamento 2020)

N.1 Attività sensibili.

La Società ha individuato le seguenti attività sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei reati tributari:

➢Acquisto di beni e servizi;

➢Gestione flussi monetari e finanziari;

➢Cessione di campioni/licenze gratuiti di prodotti;

➢Concessione di erogazioni liberali e donazioni di beni;

➢Regali, Spese di rappresentanza;

➢Gestione dei bonus e dei benefit;

➢Emissione di documentazione afferente la contabilità;

➢Ricevimento di documentazione afferente la contabilità;

➢Predisposizione di dichiarazioni e comunicazioni concernenti la materia tributaria;

➢Presentazione di dichiarazioni e comunicazioni concernenti la materia tributaria;

➢Pagamento di imposte

N.2 Aree a Rischio.

➢Principali Soggetti, Funzioni e Unità Organizzative coinvolte: Direzione, Risorse Umane, Commerciale, Amministrazione Finanza e Controllo, Acquisti e logistica, Legale Societario e tutti coloro che, a qualunque titolo, sono coinvolti nei Processi Sensibili sopra menzionati.

N.3 Reati Ipotizzabili

Tutti i reati di cui all'art. 25-quinquiesdecies e di cui al D.lgs. n.74/2000

N.3.1 Controlli generali

Oltre al rigoroso rispetto del documento denominato "Codice "Etico, gli standard di controllo generali (ovvero validi per tutte le attività sensibili), prevedono:

Segregazione delle attività: si richiede la costante applicazione del principio di separazione delle attività tra chi esegue, chi controlla e chi autorizza.

Norme/Circolari: è prescritto che le disposizioni aziendali siano sempre idonee a fornire chiari principi generali di riferimento per la regolamentazione dell'attività.

Poteri di firma e poteri autorizzativi: si prevede l'obbligo di fissare costantemente regole formalizzate per l'esercizio di poteri autorizzativi e poteri di firma.

Tracciabilità: si richiede l'esistenza di strumenti che, in relazione ad ogni comunicazione scritta relativa a ciascuna attività, assicurino la tracciabilità degli elementi informativi e delle relative fonti.

In linea generale, il sistema di organizzazione per la gestione della materia in oggetto deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, e di segregazione delle funzioni e dei ruoli, in modo che nessun soggetto possa gestire da solo un intero processo, in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

Più in particolare con riferimento alle indicate aree sensibili è necessario seguire le seguenti regole di condotta:

Ai componenti degli organi sociali e ai dipendenti, che per conto della Società intrattengono rapporti con la Agenzia delle Entrate e le autorità fiscali, deve essere attribuito formale potere in tal senso. I soggetti muniti di poteri verso l'esterno devono agire nei limiti dei poteri ad essi conferiti. I soggetti privi di poteri verso l'esterno devono richiedere l'intervento dei soggetti muniti di idonei poteri.

Qualunque criticità o conflitto di interesse che dovessero sorgere nell'ambito del rapporto con le autorità fiscali devono essere comunicati, per iscritto, anche all'ODV.

I titolari di funzioni e mansioni relative a fisco ed imposte nelle dichiarazioni relative ad esse, e nella loro predisposizione, non devono introdurre elementi passivi fittizi avvalendosi di fatture o altri documenti per operazioni inesistenti. A tale riguardo:
(i) devono controllare che le fatture e i documenti contabili si riferiscano a prestazioni effettivamente svolte da parte dell'emittente delle fatture/documenti ed effettivamente ricevute dalla Società;
(ii) non devono registrare nelle scritture contabili obbligatorie, né detenere a fini di prova nei confronti dell'amministrazione finanziaria, fatture o altri documenti per operazioni inesistenti;
(iii) devono verificare la regolare applicazione dell'imposta sul valore aggiunto, devono astenersi (a) dal compiere operazioni simulate oggettivamente o soggettivamente nonché (aa) dall'avvalersi di documenti falsi o di altri mezzi fraudolenti idonei a ostacolare l'accertamento e a indurre in errore l'amministrazione finanziaria.
I medesimi soggetti devono astenersi dall'indicare in dichiarazioni relative alle imposte sui redditi o sul valore aggiunto: (i) elementi attivi per un ammontare inferiore a quello effettivo o (ii) elementi passivi fittizi o (iii) crediti e ritenute fittizi.
Devono astenersi dall'emettere o rilasciare fatture o altri documenti per operazioni inesistenti al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto.
Devono astenersi dall'occultare o distruggere in tutto o in parte le scritture contabili, o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari, con il fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi.
Devono astenersi dall'alienare simulatamente o dal compiere altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva da parte dell'amministrazione finanziaria, con il fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte.
Devono altresì astenersi dall'indicare nella documentazione presentata inferiore a quello effettivo o (ii) elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila, con il fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori.
Approvazione da parte del responsabile apicale della gestione contabile e fiscale
Le dichiarazioni e comunicazioni in materia di imposte sui redditi o sul valore aggiunto non devono essere presentate senza la preventiva approvazione e benestare del Chief Financial Officer.
Tracciabilità
La Società deve seguire regole che garantiscano il rispetto della normativa in materia nonché la tracciabilità e trasparenza delle scelte operate, mantenendo a disposizione dell'O.d.V. tutta la documentazione di supporto
Ricorso a servizi di terzi

Nel caso in cui la predisposizione delle dichiarazioni e comunicazioni in materia di imposte sui redditi o sul valore aggiunto fosse affidata a terzi esterni alla Società, i terzi stessi dovranno essere vincolati contrattualmente a rispettare gli obblighi e i divieti di cui ai punti che precedono.
In particolare, in detti contratti deve essere contenuta apposita dichiarazione delle controparti:
a) di essere a conoscenza della normativa di cui al D.lgs. 231/2001 e delle sue implicazioni per la Società;
b) di impegnarsi a rispettare detta normativa e farla rispettare dai propri dipendenti e collaboratori;
c) di non essere mai stati condannati (o avere richiesto il patteggiamento) e di non essere al momento imputati o indagati in procedimenti penali relativi ai Reati Presupposto; nel caso di esistenza di condanna o di procedimento in corso, e sempre che l'accordo sia ritenuto indispensabile e da preferirsi a un contratto con altri soggetti, dovranno essere adottate particolari cautele;
d) di impegno a rispettare il Modello (ed in particolare le prescrizioni della presente Parte Speciale) e il Codice Etico della Società, ovvero, nel caso di enti, di avere adottato un proprio analogo Modello e un Codice Etico che regolamentano la prevenzione dei reati contemplati nel Modello e nel Codice Etico della Società;
e) di impegnarsi in ogni caso ad astenersi dal compiere attività che possano configurare alcuno dei Reati Presupposto o che comunque si pongano in contrasto con la normativa e/o con il Modello;
f) di adeguare il servizio a eventuali richieste della Società fondate sulla necessità di ottemperare alla prevenzione dei Reati Presupposto di cui trattasi.

Inoltre, nei contratti con i consulenti e con i prestatori di servizi deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte dei prestatori delle norme di cui al D.lgs. 231/2001 (quali ad es. clausole risolutive espresse, penali).
N3.2 Procedure
Devono essere osservate le procedure relative alla tenuta della contabilità e alla gestione della materia tributaria, nonché la procedura di tesoreria.
N3.3 Controllo
Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi ai Processi Sensibili di cui trattasi devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente eventuali situazioni di irregolarità o anomalie.

N3.4 Procedure
Al fine di mitigare il rischio di commissione dei reati presupposto previsti dall'art. 25-quinquiesdecies e di cui al D.lgs. n.74/2000 è necessario rispettare i seguenti protocolli operativi:
✓i beni e/o servizi oggetto del contratto siano effettivamente venduti all'altra parte coinvolta secondo le modalità, i termini e le condizioni concordate;

✓degli acquisti o delle vendite, dei servizi resi o acquisiti sia conservata adeguata traccia documentale, a cura del responsabile interessato, con archiviazione dei relativi documenti, presso la sede della Società;

✓i pagamenti eseguiti o ricevuti a titolo di corrispettivo siano conformi:
alle vendite/servizi effettivamente resi/ricevuti nonché (ii) alle pattuizioni contenute nel relativo contratto;

✓tutti i pagamenti siano effettuati dietro emissione di fattura o documento equipollente, ove richiesto dalla legge;

✓tutti i pagamenti siano regolarmente contabilizzati conformemente alle disposizioni di legge applicabili;

Si deve inoltre prevedere le seguenti condizioni nelle operazioni commerciali:

✓tracciabilità dell'operazione tramite documentazione e archiviazione (telematica e/o cartacea) di ogni attività del processo da parte della funzione coinvolta;

✓utilizzo del sistema informatico dedicato per la registrazione delle fatture attive e passive, nonché di ogni altro accadimento economico;

✓nessun pagamento o incasso può essere regolato in contanti, salvo che vi sia espressa autorizzazione da parte della Direzione della Società e comunque per importi che non superino somme gestite attraverso la piccola cassa.

Si deve inoltre prevedere che:

La Società deve avvalersi solo di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea.

Sono preventivamente stabiliti, in funzione della natura della prestazione svolta, limiti quantitativi all'erogazione di anticipi di cassa e al rimborso di spese sostenute da parte del personale della Società. Il rimborso delle spese sostenute deve essere richiesto attraverso la compilazione di modulistica specifica e solo previa produzione di idonea documentazione giustificativa delle spese sostenute.

Le risorse finanziarie ottenute come contributo, sovvenzione o finanziamento pubblico devono essere destinate esclusivamente alle iniziative e al conseguimento delle finalità per le quali sono state richieste e ottenute.

L'impiego di tali risorse è sempre motivato dal soggetto richiedente, che ne attesta la coerenza con le finalità per le quali il finanziamento è stato richiesto e ottenuto;

✓ regolamentazione e monitoraggio degli accessi al sistema informatico;

✓ contabilizzazione da parte dell'ufficio responsabile delle sole fatture attive/passive che hanno ricevuto il benestare alla registrazione e al loro pagamento/incasso solo dopo aver ricevuto il benestare del responsabile di funzione;

✓ rilevazione di tutti i fatti amministrativi aziendali che hanno riflesso economico e patrimoniale;

✓ corretto trattamento fiscale delle componenti di reddito, detrazioni e deduzioni secondo quanto previsto dalla normativa fiscale;

✓ rispetto degli adempimenti richiesti dalla normativa in materia di imposte dirette e indirette;

✓ diffusione delle principali novità normative in materia fiscale al personale coinvolto nella gestione della fiscalità;

✓ verifica con un consulente terzo di qualsivoglia implicazione fiscale derivante dall'esecuzione di un'operazione avente carattere ordinario o straordinario. Inoltre, ai fini della corretta gestione degli incassi, devono essere rispettate le seguenti regole procedurali:

✓ al personale è fatto obbligo di segnalare dalla Direzione eventuali clienti/fornitori che effettuano operazioni sospette all'atto dell'acquisizione di informazioni (quali ad esempio dichiarazione di ragioni sociale inesistente, richiesta di pagamenti illeciti e/o fuori campo IVA, emissione di documenti fiscali non corretti, proposta di pagamenti tramite regalie, ecc.);

O. PIANO per la prevenzione ed il contrasto delle molestie in ambito aziendale

La T BRIDGE S.p.A. ha adottato un piano per la prevenzione ed il contrasto delle molestie in ambito lavorativo, nel rispetto della parità di trattamento e della pari dignità di tutti coloro che, direttamente o indirettamente, si interfacciano con la Società.
Il piano trova applicazione in ogni sede aziendale della Società, riconoscendo la violenza e le molestie nel mondo del lavoro come un abuso ed una violazione dei diritti umani e, come tali, esecrabili e sanzionabili.
La Società, pertanto, si impegna ad adottare ogni misura appropriata a prevenire e contrastare tali fenomeni che, in ultima analisi, rappresentano una minaccia alle pari opportunità.
In tale ottica saranno promosse iniziative di formazione volte al perseguimento degli obiettivi indicati e successivamente verranno somministrati sondaggi (cd. Survey) tesi a verificare l'efficacia del piano biennale adottato.
La Società ha istituito pertanto, un canale di comunicazione interno, all'indirizzo di posta elettronica peopleinclusion@t-bridge.it per inoltrare segnalazioni afferenti il tema trattato, con l'obiettivo prefigurato di offrire soluzioni ai vari casi concreti.
La Società ha istituito, altresi, la figura del "Diversity manager", nella persona della Dott.ssa Rosalinda Fantini, per vagliare le comunicazioni inoltrate sulla mail dedicata e verificare la effettiva ed efficace implementazione del piano biennale per la prevenzione ed il contrasto delle molestie.
I comportamenti integranti una violazione del piano biennale di prevenzione saranno oggetto di sanzione disciplinare ai sensi del MOGC adottato dalla Società.
(LETTERA INSERITA CON LA MODIFICA DEL SETTEMBRE 2023)

ALTRI REATI

Per la natura dell'attività e dell'organizzazione della Società T Bridge, si è scelto di non considerare come fattispecie rilevanti all'interno del Modello i reati disciplinati dagli artt. 24 – ter (delitti di criminalità organizzata, anche transnazionali), dall'art 25-quater (delitti con finalità di terrorismo, anche internazionale, o di eversione dell'ordine democratico), dall'art. 25 quater 1. (pratiche di mutilazione degli organi genitali femminili) e 25-sexies (reati a tutela del mercato regolamentato), non considerando ipotizzabili le relative fattispecie di reati nell'ambito dell'attività svolta dalla Società. Altre

fattispecie di reato rientranti in tale categoria, pur contemplate quale presupposto per generare la responsabilità amministrativa delle persone giuridiche, sono le seguenti:

 Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis, D. Lgs. 231/01) (Postilla aggiornamento 2020).

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.)
- Alterazione di moneta (art. 454 c.p.)
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.)
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.)
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.)
- Contraffazione di carta filigranata in uso per la fabbricazione di carta di pubblico credito o di valori di bollo (art. 460 c.p.)
- Uso di valori di bollo contraffatti o alterato (art. 464 c.p.)
- Contraffazione, alterazione o uso di segno distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)
- Fabbricazione e detenzione di filigrana o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata.

Le attività di analisi relative alle tipologie di reati non prese in considerazione, saranno eventualmente svolte successivamente qualora, a seguito di specifiche valutazioni, esse dovessero essere ritenute pertinenti all'Azienda.

A seguito dell'introduzione del D. Lgs. 125 del 21 giugno 2016, che ha modificato l'art. 25 bis del Decreto Legislativo 231 del 2001, si è riconsiderata l'iniziale scelta di esclusione dei reati sopra indicati. Da un'analisi delle fattispecie di reato e da una valutazione delle aree ed attività a rischio commissione delle stesse, si conferma la scelta iniziale di considerare i reati previsti dagli art. 24-ter, 25-bis, 25-quater, 25-quater 1e 25-sexies come fattispecie di reato non rilevanti per la natura dell'attività e per l'organizzazione della Società T Bridge. Inoltre, per i reati di vendita di sostanze alimentari non genuine come genuine (previsto dall'art. 25-bis1 D. Lgs. 231/2001), riduzione o mantenimento in schiavitù o in servitù, prostituzione minorile, pornografia minorile, iniziative turistiche volte allo sfruttamento della prostituzione minorile, tratta di persone, acquisto e alienazione di schiavi (previsti dall'art. 25-quinquies D. Lgs. 231/2001), si è ritenuto il rischio di commissione reato non rilevante, in relazione all'attività e all'organizzazione della Società T Bridge.

VALUTAZIONE RISCHIO COMMISSIONE DEI REATI PRESUPPOSTO INTRODOTTI DAL 2016 AL 2020 NELLE AREE/ATTIVITA' DI T BRIDGE S.p.A..

A seguito di analisi e valutazione rischio commissione reati presupposto, che ad oggi hanno ampliato l'elenco dei reati precedentemente previsti dalla normativa risulta che:

In merito al reato di ‘’Perimetro informatico”, introdotto dall’art. 1 comma 11 D.L. N. 105/2019, è emerso che sono coinvolte le aree/attività a rischio già individuate nell'ambito del presente Modello e che i principi generali e i protocolli specifici di prevenzione già adottati, in particolare quelli previsti per la prevenzione dei reati ex art. 24, 25 e 24 bis D. Lgs. 231/2001, sono sufficienti ed idonee a contenere il rischio commissione reati al di sotto della soglia ritenuta tollerabile dalla società;
In merito ai reati tributari, introdotti dall’art. 39, comma 2, D.L. 26 ottobre 2019, n. 124, convertito, con modificazioni, dalla L. 19 dicembre 2019, n. 157, i principi generali e i protocolli specifici già adottati, in particolar modo per la mitigazione del rischio commissione dei reati presupposto ex artt. 24, 25, art. 25-ter D. Lgs. 231/2001, non sono state ritenute di per sé sufficienti e si è ritenuto di adottare uno specifico protocollo di prevenzione e controllo al fine di rendere accettabile e sufficientemente mitigato il rischio commissione reati tributari (Lett. O del presente modello;
In merito al reato di ‘’Traffico illecito di influenze”, introdotto ad integrazione nell’art. 25 del D. Lgs. 231/2001 dalla L. n. 3 del 09 gennaio 2019, all’esito dell’analisi e valutazione, il rischio commissione di questo reato è reso accettabile dai principi generali e dai protocolli speciali già adottati ed implementati dalla società e dai suoi vertici apicali;
In merito all’art. 24 ter
In merito al rischio commissione reati presupposto che hanno ampliato le previsioni dell’art. 25-bis1 D. Lgs. 231/2001, (Vendita di sostanze alimentari non genuine come genuine art. 516 c.p. e Vendita di prodotti industriali con segni mendaci art. 517), è emerso che il primo non investe alcuna aria/attività della T Bridge ed il secondo è caratterizzato da un rischio sufficientemente mitigato e controllato dai principi generali e dai protocolli speciali già adottati dalla società;
In merito al rischio commissione reati ex artt. 600, 600 bis, 600 ter, 601, 602, 603 bis e 609 undecies c.p., introdotti dalle modifiche intervenute all’art. 25-quinquies del D. Lgs. 231/2001, lo stesso è risultato essere sufficientemente mitigato e controllato dai principi generali e dai protocolli speciali già adottati dalla società;
Stessa considerazione di sopra al punto 6, in merito ai nuovi reati che hanno ampliato la previsione dell’art. 25-duodecies, il cui rischio commissione risulta sufficientemente mitigato e controllato dai principi generali e dai protocolli speciali già adottati dalla società;
In merito ai reati presupposto previsti dagli art. 24-bis (Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento), 25-quater (Delitti con finalità di terrorismo o di eversione dell'ordine democratico), art. 25-sexies (Abusi di mercato), art. 25-terdecies (Razzismo e xenofobia) ed art. 25-quaterdecies (Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati), all’esito di analisi e valutazione rischio commissione, lo stesso risulta non investire numerose aree/attività di T Bridge e di essere sufficientemente mitigato e controllato dai principi generali e dai protocolli speciali già adottati dalla società.