

# *Digital Bros* digital entertainment

**DIGITAL BROS S.p.A.**

Sede in Milano Via Tortona, 37

Capitale Sociale Euro 5.644.334,80

int. vers.

Codice Fiscale / P. I.V.A. N09554160151

**Modello di organizzazione, gestione e controllo  
ex. d.lgs. 231/2001**



**PARTE SPECIALE**

La presente Parte Speciale è composta da una parte preliminare dedicata alle regole generali cui deve uniformarsi la condotta degli Organi Sociali, dei Dipendenti, dei Partners commerciali, dei Collaboratori o consulenti e dei soggetti esterni che operano in nome e/ o per conto della Società (qui di seguito, per brevità, semplicemente Destinatari del Modello o Destinatari) ed all'individuazione delle aree di attività a rischio; nonché da singole Sezioni corrispondenti ai singoli gruppi di reati richiamati dal Decreto.

Le singole Sezioni sono le seguenti:

Sezione A	Reati contro la Pubblica Amministrazione ed il patrimonio;
Sezione B	Reati societari;
Sezione C	Reati finanziari o abusi di mercato;
Sezione D	Reati contro la personalità individuale ed i reati di omicidio colposo e lesioni colpose gravi e gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro;
Sezione E	Delitti informatici e trattamento illecito di dati;
Sezione F	Delitti contro l'industria e il commercio e in materia di violazione del diritto d'autore;
Sezione G	Delitti aventi finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali e delitti posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9.12.1999;
Sezione H	Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita Reati transazionali e reati tributari;
Sezione I	Impiego di lavoratori stranieri irregolari;
Sezione L	Reati transnazionali;
Sezione M	Altri reati.

Nelle Sezioni A, B, C, D, E, F, G, H, I vengono descritte:

- le potenziali aree a rischio;
- i principi di comportamento e controllo nelle principali aree a rischio;
- i principi per la predisposizione delle procedure per la prevenzione dei reati.

## **1. Regole Generali e Specifiche**

L'enunciazione di regole di condotta e il rinvio all'osservanza del Codice Etico che, giova ricordarlo, è da ritenere a ogni effetto parte integrante del Modello sono finalizzati a diffondere l'etica d'impresa di cui Digital Bros S.p.A. è portatrice, anche alla luce delle considerazioni svolte nella Parte Generale.

### Codice Etico

I Destinatari del Modello sono tenuti all'osservanza del Codice Etico.

### Rispetto delle leggi

I Destinatari del Modello sono tenuti al rispetto delle leggi italiane o di quelle del paese in cui si trovano occasionalmente per ragioni di lavoro o in cui risiedono.

Nessun Destinatario del Modello può costringere o sollecitare altri Destinatari a violare le leggi italiane o di un paese estero ove la Società svolge la propria attività od ha comunque interessi diretti o indiretti.

### Conflitto di interessi

I Dipendenti e i componenti degli Organi Sociali destinatari del Modello devono valutare prima di ogni operazione la possibilità che si manifestino conflitti di interesse, attuali e/o potenziali, e

provvedere affinché il conflitto venga evitato a priori. Sono esempi, non esaustivi e puramente indicativi, di conflitto d'interesse:

- condurre un'operazione in una posizione di vertice e avere interessi economici diretti o indiretti (tramite familiari e parenti) con i fornitori e/o clienti che collaborano all'operazione;
- curare i rapporti con i fornitori e svolgere attività personali o tramite familiari con loro;
- accettare favori da terzi per favorirli nei rapporti con la Società.

Chiunque si trovi in una situazione di conflitto di interesse è tenuto a darne comunicazione al proprio superiore gerarchico, il quale, oltre a informare l'Organismo di Vigilanza, deve valutare e attivare le misure per cui, nonostante il conflitto d'interesse, l'operazione sarà condotta nel rispetto delle abituali condizioni di mercato.

In caso di dubbio o di impossibilità a risolvere il conflitto d'interesse l'operazione deve essere sospesa.

#### Riservatezza

I Destinatari del Modello devono mantenere riservati tutti i dati e le informazioni della Società e del Gruppo acquisiti o trattati in esecuzione dell'attività per la Società, nonché assicurare il pieno e puntuale rispetto delle misure di sicurezza e di protezione.

#### Correttezza

I Destinatari del Modello devono gestire in maniera completa tutte le operazioni, garantendo la trasparenza delle relative informazioni e la legittimità formale e sostanziale di ogni singola operazione o transazione.

#### Imparzialità

I Destinatari del Modello devono evitare di favorire alcun gruppo di interesse o singole persone, nonché astenersi da qualsivoglia discriminazione sul presupposto dell'età, dello stato di salute, del sesso, della religione, della razza o di opinioni politiche e culturali.

#### Comunicazioni all'esterno

I Dipendenti e i componenti degli Organi Sociali devono effettuare tutte le comunicazioni verso l'esterno, nel rispetto delle leggi e delle regole interne della Società e del Gruppo e professionali. Nessun Destinatario può divulgare o utilizzare a profitto proprio o di terzi notizie o informazioni riservate attinenti le attività della Società e del Gruppo.

#### Tutela dei beni aziendali

I Destinatari del Modello, nell'utilizzare i beni della Società, devono operare con diligenza per salvaguardare l'efficienza e la durata dei beni. È vietato l'uso improprio che possa arrecare danni e/o riduzioni di efficienza dei beni dei beni stessi.

#### Regali e benefici

Nessun Destinatario del Modello può offrire denaro, beni, servizi e benefici di qualsiasi genere, né in nome e per conto della Società né a titolo personale, a dipendenti o collaboratori di società od enti, allo scopo di promuovere e acquisire condizioni di favore per la Società nella conduzione di operazioni.

Nessun Destinatario può sollecitare o accettare denaro, beni servizi o benefici di qualsiasi genere in occasione dello svolgimento di attività per la Società.

Quanto sopra vale nei rapporti con persone, società o enti pubblici e privati, in Italia e all'Estero.

In deroga ai divieti sopra menzionati, sono ammessi regali di modico valore purché siano tali da essere interpretati come normali segni di cortesia o connessi con lo svolgimento della propria attività lavorativa e/o professionale.

È inoltre vietata ogni attività che sotto qualsiasi veste - per esempio sponsorizzazioni, incarichi, consulenze, pubblicità - o con attuazione in forma indiretta - per esempio tramite interposte persone - abbia le stesse finalità di acquisire favori per la Società.

## Gestione dei processi e dei flussi finanziari

I Destinatari del Modello devono rispettare gli elementi fondamentali delle specifiche procedure interne previste per i processi di gestione della finanza dispositiva, in quanto trattasi di processi da cui può derivare un utilizzo improprio degli strumenti di provvista e la creazione di cosiddetti “fondi occulti” che possono essere utilizzati per la commissione di reati.

In particolare, le specifiche procedure interne relative alla finanza dispositiva devono fare applicazione dei seguenti principi:

- a) esistenza di attori diversi, operanti nelle seguenti fasi/attività del processo:
  - richiesta della disposizione di pagamento per assolvere l’obbligazione;
  - effettuazione del pagamento;
  - controllo/riconciliazioni a consuntivo;
- b) esistenza di limiti all’autonomo impiego di risorse finanziarie mediante la determinazione di livelli autorizzativi per la disposizione di pagamento, articolati in funzione dell’importo e della natura dell’operazione;
- c) esistenza e diffusione di *specimen* di firma in relazione ai livelli autorizzativi definiti per la disposizione di pagamento;
- d) tracciabilità degli atti e delle singole fasi del processo (con specifico riferimento all’annullamento dei documenti che hanno già originato un pagamento).

In generale, eventuali modalità non *standard* devono essere considerate “in deroga” e, pertanto, devono essere comunicate all’Organismo di Vigilanza.

### A. INDIVIDUAZIONE DEI REATI E DELLE AREE SENSIBILI

L’art. 6, comma 2, lett. a) del D.Lgs. 231/2001 prevede che il Modello debba “individuare le attività nel cui ambito possono essere commessi reati”.

Digital Bros S.p.A. (di seguito anche “**Digital Bros.**” o la “**Società**”) ha analizzato le fattispecie di illeciti perpetrabili nell’ambito della struttura organizzativa della Società ed ha identificato i seguenti reati che concretamente possono comportare la responsabilità della stessa:

- Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico (Art. 24, D.Lgs. n. 231/2001);
- Delitti informatici e trattamento illecito di dati (Art. 24-bis, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 48/2008; modificato dal D.Lgs. n. 7 e 8/2016];
- Delitti di criminalità organizzata (Art. 24-ter, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 94/2009 e modificato dalla L. 69/2015];
- Concussione, induzione indebita a dare o promettere altra utilità e corruzione (Art. 25, D.Lgs. n. 231/2001) [articolo modificato dalla L. n. 190/2012];
- Delitti contro l’industria e il commercio (Art. 25-bis.1, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009];
- Reati societari Art. 25-ter, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 61/2002, modificato dalla L. n. 190/2012 e dalla L. 69/2015];
- Reati con finalità di terrorismo o di eversione dell’ordine democratico previsti dal codice penale e dalle leggi speciali (Art. 25-quater, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 7/2003];
- Delitti contro la personalità individuale (Art. 25-quinquies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 228/2003];
- Reati di abuso di mercato (Art. 25-sexies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 62/2005];
- Reati di 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, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 123/2007];
- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25-octies, D.Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 231/2007; modificato dalla L. n. 186/2014];

- Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009];
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 109/2012];
- Reati tributari (Art. 25-quinquiesdecies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 157/2019].

Per ciascuna delle fattispecie criminose sopra evidenziate la Società ha, quindi, individuato le singole attività sensibili e qualificato i principi di controllo e di comportamento cui devono attenersi tutti coloro che vi operano.

## **B. DEFINIZIONE DEI PRINCIPI GENERALI PER LA REDAZIONE DEI PROTOCOLLI DI PREVENZIONE**

Al fine della redazione/integrazione delle procedure di controllo e prevenzione, di seguito sono riportati i principi procedurali cui devono essere improntate le specifiche procedure per la creazione di c.d. “protocolli di prevenzione”, volti a prevenire la commissione dei reati contemplati nel Modello.

L'approvazione delle procedure deve essere affidata a personale diverso dal responsabile della funzione che svolge l'attività da regolamentare, ma allo stesso tempo deve prevedere il contributo, soprattutto nella fase di controllo, da parte di coloro che dovranno applicarla.

Le procedure devono assicurare il rispetto dei seguenti elementi di controllo:

- **tracciabilità:** deve essere ricostruibile la formazione degli atti e delle fonti informative/documentali utilizzate a supporto dell'attività svolta, a garanzia della trasparenza delle scelte effettuate; ogni informazione deve essere documentata in tutte le fasi, di modo che sia sempre possibile l'attività di verifica e controllo; tale attività di verifica e controllo deve essere a sua volta documentata mediante la redazione di verbali;
- **separazione di compiti:** non deve esserci identità soggettiva tra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- **poteri di firma e poteri autorizzativi:** devono esistere regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi interni, in coerenza con le responsabilità organizzative e gestionali e con una precisa indicazione dei limiti di spesa; le procedure devono, inoltre, prevedere obblighi di rendiconto al superiore gerarchico;
- **archiviazione/tenuta dei documenti:** i documenti riguardanti l'attività devono essere archiviati e conservati, a cura della funzione competente, con modalità tali da non permettere la modificazione successiva, se non con apposita evidenza; deve inoltre essere evitato che venga consentito l'accesso a terzi che non siano espressamente autorizzati;
- **riservatezza:** l'accesso ai documenti già archiviati, di cui al punto precedente, deve essere motivato e consentito solo al soggetto competente in base alle norme interne, o a suo delegato, e all'Organismo di Vigilanza.

Con riferimento sia alle attività c.d. a rischio individuate sia ad ogni singola funzione aziendale preposta, devono essere riportati i seguenti schemi di controllo:

- una breve descrizione delle principali fasi che caratterizzano in genere l'attività;
- una breve descrizione delle principali attività svolte con riferimento, invece, alle singole funzioni aziendali;

- le procedure di controllo, volte a contrastare (ragionevolmente) le possibilità di violazione delle regole contenute nel presente Modello, differenziate, ove necessario e/o possibile, in relazione ai reati previsti;
- i flussi informativi verso l'Organismo di Vigilanza per evidenziare le aree da investigare e tenere sotto controllo.

Per ciascun protocollo di prevenzione deve essere individuato un responsabile che dovrà coincidere con il responsabile della funzione interessata dall'operazione sensibile, il quale dovrà garantire il rispetto delle regole di condotta, dei protocolli e delle procedure aziendali, tenendo prontamente informato l'Organismo di Vigilanza e coordinandosi con lo stesso.

**PARTE SPECIALE**  
**SEZIONE "A"**

**I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE (art. 24 e 25 del D. Lgs. 231/2001)**

In questa parte speciale sono individuate le aree di attività nel cui ambito possono essere commessi i reati di cui al D. Lgs. 231/2001 che riguardano i rapporti con la Pubblica Amministrazione, così come di seguito identificata, e le situazioni in cui questa è comunque coinvolta (reati contro la Pubblica Amministrazione e contro il Patrimonio ex art. 24 e 25 del Decreto).

Si possono identificare quali soggetti della Pubblica Amministrazione, i seguenti enti o categorie di enti:

- enti ed amministrazioni dello Stato ad ordinamento autonomo quali: Ministeri; Camera e Senato; Dipartimento Politiche Comunitarie; Autorità Garante della Concorrenza e del Mercato; Autorità per le Garanzie nelle Comunicazioni; Autorità per l'Energia Elettrica ed il Gas; Banca d'Italia; Consob; Autorità Garante per la Protezione dei Dati Personali; Agenzia delle Entrate; ISVAP – Istituto per la Vigilanza sulle Assicurazioni private e di interesse collettivo;
- Regioni;
- Province;
- Comuni;
- Comunità Montane e loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- Ordini e Collegi Professionali;
- ASL;
- Enti e Monopoli di Stato;
- Borsa Italiana S.p.A.;
- tutti gli enti pubblici non economici nazionali, regionali e locali, quali: INPS; CNR; INAIL; INPDAl; INPDAP; ISTAT; ENASARCO;
- istituti e scuole di ogni ordine e grado e le istituzioni educative.

Per "Pubblica Amministrazione", pertanto, si intendono tutti quei soggetti, privati e di diritto pubblico, che svolgano una "funzione pubblica", un "pubblico servizio" o un "servizio di pubblica necessità".

Per "funzione pubblica" si intendono le attività, disciplinate da norme di diritto pubblico, attinenti le funzioni legislative (Stato, Regioni, ecc.), amministrative (membri delle amministrazioni statali e territoriali, Forze dell'Ordine, membri delle amministrazioni sovranazionali - es. U.E. - membri delle Authorities, dell'Antitrust, delle Camere di Commercio, ecc.) e giudiziarie (Giudici, Ufficiali Giudiziari, organi ausiliari dell'Amministrazione della Giustizia quali curatori o liquidatori fallimentari, ecc.).

Per "pubblico servizio" si intendono le attività di produzione di beni e di servizi di interesse generale ed assoggettate alla vigilanza di un'Autorità Pubblica, e quelle attività volte a garantire i diritti della persona alla vita, alla salute, alla libertà, alla previdenza e assistenza sociale, all'istruzione, alla libertà di comunicazione, ecc., in regime di concessione e/o di convenzione (es. Enti Ospedalieri, ASL, I.N.P.S., I.N.A.I.L., membri dei Consigli Comunali Uffici Postali, Uffici Doganali, Ferrovie, Autostrade, Ente Fieristico ecc.).

Per "servizio di pubblica necessità" si intendono le attività professionali il cui esercizio non è consentito senza previa autorizzazione amministrativa ed abilitazione da parte dello Stato (avvocato e procuratore, notaio, medico, farmacista, ecc.), nel momento in cui il pubblico è per legge tenuto ad avvalersene, ed altre attività, svolte da privati, che presuppongono un'autorizzazione amministrativa (rivendita di tabacchi, agenzie di cambio, ecc.).

Per completezza riportiamo integralmente gli artt. 357, 358 e 359 c.p., in cui ritroviamo le definizioni di "pubblico ufficiale", di "incaricato di pubblico servizio" e di "persone esercenti un servizio di pubblica necessità".

Art. 357 c.p. - Nozione del pubblico ufficiale.

Agli effetti della legge penale, sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione

amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi.

Art. 358 c.p. – Nozione della persona incaricata di un pubblico servizio.

Agli effetti della legge penale, sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di questa ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale.

Art. 359 c.p. – Nozione della persona esercente un servizio di pubblica necessità.

Agli effetti della legge penale, sono persone che esercitano un servizio di pubblica necessità:

- 1) i privati che esercitano professioni forensi o sanitarie, o altre professioni il cui esercizio sia per legge vietato, senza una speciale abilitazione dello Stato, quando dell'opera di essi il pubblico sia per legge obbligato a valersi;
- 2) i privati che, non esercitando una pubblica funzione, né prestando un pubblico servizio, adempiono un servizio dichiarato di pubblica necessità mediante un atto della Pubblica Amministrazione.

Si illustrano sinteticamente qui di seguito le fattispecie previste dagli artt. 24, 25 e 25 - decies del Decreto, trattate nel presente capitolo.

**Malversazione a danno dello Stato (art. 316 bis c.p.)**

Tale ipotesi di reato si configura nel caso in cui, dopo aver ricevuto finanziamenti o contributi da parte dello Stato italiano o altri Enti Pubblici o dall'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate. La condotta, infatti, consiste nel distrarre, anche parzialmente, la somma ottenuta, facendo rilevare che l'attività programmata si sia comunque svolta.

Sanzione pecuniaria applicabile fino a 500 quote. Se dalla commissione del reato l'ente ha conseguito un profitto di rilevante entità o ne è derivato un danno di particolare gravità la sanzione pecuniaria applicabile è compresa tra un minimo di 200 ad un massimo di 600 quote.

**Indebita percezione di erogazioni a danno dello Stato (art. 316 ter c.p.)**

Tale ipotesi di reato si configura nei casi in cui, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute, si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri Enti Pubblici o dall'Unione Europea. Tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato, configurandosi solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato ex art. 640 bis. Sanzione pecuniaria applicabile fino a 500 quote. Se dalla commissione del reato l'ente ha conseguito un profitto di rilevante entità o ne è derivato un danno di particolare gravità la sanzione pecuniaria applicabile è compresa tra un minimo di 200 ad un massimo di 600 quote.

**Truffa (art. 640 c.p.)**

Tale ipotesi di reato si configura nel caso in cui, con artifici o raggiri, si induce taluno in errore e si procura a sé o ad altri un ingiusto profitto con altrui danno.

**Truffa ai danni dello Stato e di altro ente pubblico (art. 640, comma 2, n. 1, c.p.)**

Essa si verifica quando, per ottenere ingiusti profitti, si mettono in atto raggiri o artifici tali da recare un danno allo Stato o ad altri Entipubblici.

Sanzione pecuniaria applicabile fino a 500 quote. Se dalla commissione del reato l'ente ha conseguito un profitto di rilevante entità o ne è derivato un danno di particolare gravità la sanzione pecuniaria applicabile è compresa tra un minimo di 200 ad un massimo di 600 quote.

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

E' un'ipotesi specifica della Truffa in danno dello Stato, di altri enti pubblici o delle Comunità

europee e si concretizza quando la truffa è diretta ad ottenere contributi, finanziamenti, mutui agevolati o altre erogazioni pubbliche. Sanzione pecuniaria applicabile fino a 500 quote. Se dalla commissione del reato l'ente ha conseguito un profitto di rilevante entità o ne è derivato un danno di particolare gravità la sanzione pecuniaria applicabile è compresa tra un minimo di 200 ad un massimo di 600 quote.

#### **Concussione e induzione indebita (art. 317 c.p. 319-quater e art. 322-bis c.p.)**

La concussione è la condotta di un pubblico ufficiale che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

L'induzione indebita a dare o promettere utilità è la condotta di un pubblico ufficiale o di un 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.

La sanzione pecuniaria applicabile è compresa tra un minimo di 300 ad un massimo di 800 quote.

#### **Corruzione per l'esercizio della funzione (art. 318 c.p.)**

Tale fattispecie si verifica quando il **pubblico ufficiale**, che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, **denaro** o altra utilità, o ne accetta la **promessa**.

Si applica una sanzione pecuniaria fino a 200 quote.

#### **Corruzione per un atto d'ufficio o per un atto contrario ai doveri d'ufficio (artt. - 319 c.p., art. 320-321-322-bis c.p.)**

Si verifica quando un pubblico ufficiale accetta una retribuzione che non gli è dovuta (in denaro o altro genere) o la promessa della stessa, per compiere, ritardare od omettere un atto del suo ufficio.

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

Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio. La sanzione pecuniaria applicabile è compresa tra un minimo di 200 ad un massimo di 600 quote.

#### **Corruzione in atti giudiziari (art. 319-ter c.p., art. 320-321-322-bis c.p.)**

Il reato si configura nel caso in cui un soggetto offra o prometta ad un pubblico ufficiale o ad un incaricato di un pubblico servizio denaro o altra utilità al fine di favorire o danneggiare una parte in un processo civile, penale o amministrativo.

Potrà dunque essere chiamata a rispondere del reato la società che, essendo parte in un procedimento giudiziario, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario) al fine di ottenerne la positiva definizione. La sanzione pecuniaria applicabile è compresa tra un minimo di 200 ad un massimo di 600 quote. Se dal compimento del fatto l'ente ne ha conseguito un profitto di rilevante entità la sanzione prevista può essere compresa tra un minimo di 300 ed un massimo di 800 quote.

#### **Istigazione alla corruzione (art. 322 c.p. e art. 322-bis c.p.)**

La pena prevista per tale reato si applica a chiunque offra o prometta denaro o altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per indurlo a compiere un atto contrario o conforme ai doveri d'ufficio, qualora la promessa o l'offerta non vengano accettate. Parimenti, si sanziona la condotta del pubblico agente che solleciti una promessa o un'offerta da parte di un privato.

#### **Traffico di influenze illecite (art. 346-bis c.p.)**

Chiunque, fuori dei casi di concorso nei reati di cui agli articoli 318, 319, 319-ter e nei reati di corruzione di cui all'articolo 322-bis, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come

prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri, è punito con la pena della reclusione da un anno a quattro anni e sei mesi.

La stessa pena si applica a chi indebitamente dà o promette denaro o altra utilità.

La pena è aumentata se il soggetto che indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità riveste la qualifica di pubblico ufficiale o di incaricato di un pubblico servizio.

Le pene sono altresì aumentate se i fatti sono commessi in relazione all'esercizio di attività giudiziarie o per remunerare il pubblico ufficiale o l'incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis in relazione al compimento di un atto contrario ai doveri d'ufficio o all'omissione o al ritardo di un atto del suo ufficio.

Se i fatti sono di particolare tenuità, la pena è diminuita.

### **Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)**

Il reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno a terzi.

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

Si applica all'ente la sanzione pecuniaria fino a 500 quote. Se dalla commissione del reato l'ente ha conseguito un profitto di rilevante entità o ne è derivato un danno di particolare gravità la sanzione pecuniaria applicabile è compresa tra un minimo di 200 ad un massimo di 600 quote.

## **1.A – Potenziali aree a rischio**

In considerazione delle attività svolte da Digital Bros e della struttura interna adottata, ai sensi dell'art. 6 del Decreto, sono individuate le seguenti categorie di operazioni e attività a rischio, nelle quali potrebbero essere commessi i reati previsti dagli artt. 24 e 25 del Decreto:

- a) attività che comportano partecipazione a trattative ed a gare di pubblico appalto;
- b) operazioni relative a finanziamenti agevolati o volte all'ottenimento di agevolazioni e contributi dalla Pubblica Amministrazione;
- c) gestione delle risorse finanziarie;
- d) ottenimento di concessioni e autorizzazioni inerenti all'attività editoriale / radiofonica/ televisiva e di quelle volte alla gestione del patrimonio immobiliare;
- e) comunicazione alla Pubblica Amministrazione di informazioni e dati aziendali;
- f) gestione assunzione del personale;
- g) gestione e assunzione di consulenti esterni;
- h) gestione delle verifiche, ispezioni, controlli posti in essere dalla PA richieste da norme legislative e regolamentari;
- i) gestione dell'attività di contenzioso in tutti i gradi di giudizio, anche attraverso l'ausilio di legali esterni.

## **2.A – Principi di comportamento e controllo nelle principali aree a rischio**

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24 e 25 del D. Lgs. 231/2001); sono altresì proibite le violazioni ai principi ed alle procedure aziendali.

Al fine di evitare il verificarsi dei reati nei confronti della Pubblica Amministrazione e del patrimonio previsti dal Decreto Legislativo n. 231/01, tutti i Destinatari del presente Modello, devono:

- Attenersi alle seguenti condotte:

- a) osservare rigorosamente tutte le leggi, i regolamenti e le procedure che disciplinano i rapporti e/o i contatti con Enti pubblici, Pubbliche Amministrazioni e/o Pubblici Ufficiali e/o Incaricati di Pubblici Servizi;
- b) improntare i rapporti con Enti pubblici, Pubbliche Amministrazioni e/o Pubblici Ufficiali e/o Incaricati di Pubblici Servizi alla massima trasparenza, correttezza ed imparzialità;
- c) verificare, mediante il controllo esercitato dai responsabili delle diverse Aree sui Collaboratori che effettuano attività nei confronti di enti pubblici, che qualsiasi rapporto, anche occasionale, con i medesimi enti sia svolto in modo lecito e regolare;
- d) gestire qualsivoglia rapporto, anche occasionale, con Enti pubblici, Pubbliche Amministrazioni e/o Pubblici Ufficiali e/o Incaricati di Pubblici Servizi in modo lecito e regolare.

- È, inoltre vietato:

- a) usare la propria posizione per ottenere benefici o privilegi per sé o per altri;
- b) richiedere e/o usare contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, dalla Pubblica Amministrazione, da altri enti pubblici o dalla Comunità europea o da altri organismi pubblici di diritto internazionale, mediante la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute;
- c) destinare eventuali somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
- d) corrispondere e/o proporre e/o chiedere a terzi di proporre la corresponsione e/o dazione di denaro o altra utilità a un Pubblico funzionario o a Pubblica Amministrazione o altri pubblici funzionari della Comunità Europea o altri organismi pubblici di diritto internazionale;
- e) offrire doni o gratuite prestazioni al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo offerto eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, ai rappresentanti della PA o a loro familiari non deve essere offerta, né direttamente né indirettamente, qualsiasi forma di regalo, doni o gratuite prestazioni che possano apparire, comunque, connessi al rapporto di affari con la Società o altre società del Gruppo o miranti ad influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società o il Gruppo. Anche in quei paesi in cui offrire regali o doni costituisce una prassi diffusa in segno di cortesia, tali regali devono essere di natura appropriata e non contrastare con le disposizioni di legge; non devono comunque essere interpretati come richiesta di favori in contropartita. In caso di dubbio il Destinatario deve darne tempestiva informazione alla società di appartenenza la quale, nei casi opportuni, sottoporrà la segnalazione al Organismo di Vigilanza; in ogni caso, i regali offerti devono essere documentati in modo adeguato per consentire le verifiche da parte dello stesso. I contributi e i finanziamenti a fini politici e assistenziali devono restare nei limiti consentiti dalla legge ed essere preventivamente autorizzati dal Consiglio di Amministrazione o dalle funzioni aziendali da questo designate;
- f) eseguire prestazioni e riconoscere compensi in favore degli Agenti, dei Partners Commerciali, dei Fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- g) corrispondere e/o proporre la corresponsione e/o chiedere a terzi di proporre la corresponsione e/o dazione di denaro o altra utilità a un Pubblico funzionario nel caso in cui la Società sia parte di un procedimento giudiziario;
- h) porre in essere artifici e/o raggiri, tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea o ad organismi di diritto pubblico internazionale) per realizzare un ingiusto profitto;
- i) eludere i divieti dalla lettera b) alla lettera g), ricevendo o anche solo sollecitando erogazioni a qualsivoglia titolo che, sotto qualsivoglia forma e/o denominazione (ad esempio, sponsorizzazioni, incarichi, consulenze, pubblicità) abbiano, invece, le stesse finalità sopra vietate;
- l) promettere e/o versare somme, promettere e/o concedere beni in natura e/o altri benefici e/o utilità nei rapporti con Rappresentanti delle forze politiche e/o di associazioni portatrici di interessi, per promuovere o favorire interessi della Società, anche a seguito di illecite pressioni;

m) sottrarre, alterare e/o manipolare i dati e i contenuti del sistema informatico o telematico, per ottenere un ingiusto profitto e arrecando danni a terzi.

### **3.A – Principi per la predisposizione delle procedure per la prevenzione dei reati contro la Pubblica Amministrazione**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste specifiche procedure, in forza delle quali:

- a) siano ricostruibili la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- b) non vi sia identità soggettiva fra coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- c) i documenti riguardanti l'attività d'impresa siano archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;
- d) qualora il servizio di archiviazione e/o conservazione dei documenti sia svolto, per conto della Società, da un soggetto ad essa estraneo, il servizio debba essere regolato da un contratto nel quale si preveda, tra l'altro, che il soggetto che presta il servizio alla Società rispetti specifiche procedure di controllo idonee a non permettere la modificazione successiva dei documenti archiviati, se non con apposita evidenza;
- e) l'accesso ai documenti, di cui ai punti precedenti, già archiviati sia sempre motivato e consentito solo al soggetto competente in base alle norme interne, o a suo delegato, al Collegio Sindacale od organo equivalente, alla società di revisione o all'Organismo di Vigilanza;
- f) la scelta di consulenti esterni avvenga sulla base di requisiti di professionalità, indipendenza e competenza e, in riferimento a essi, sia motivata la scelta;
- g) non siano corrisposti compensi, provvigioni o commissioni a Agenti, Partners Commerciali, Collaboratori, Fornitori o a soggetti pubblici in misura non congrua rispetto alle prestazioni rese alla Società e/o comunque non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;
- h) i sistemi di remunerazione premianti ai Dipendenti e Collaboratori rispondano a obiettivi realistici e coerenti con le mansioni e l'attività svolta e con le responsabilità affidate;
- i) la Società, ai fini dell'attuazione delle decisioni di impiego delle risorse finanziarie, si avvalga di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea;
- l) nessun pagamento può essere effettuato in contanti, salvo specifica preventiva autorizzazione da parte della funzione Amministrazione Finanza e Controllo;
- m) le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di concessioni, autorizzazioni o licenze, devono contenere solo elementi assolutamente veritieri;
- n) alle ispezioni giudiziarie, tributarie e amministrative (es. relative al D. Lgs. 81/2008, verifiche tributarie, INPS, ecc.) devono partecipare i soggetti a ciò espressamente delegati. L' Organismo di Vigilanza dovrà essere prontamente informato sull'inizio di ogni attività ispettiva, mediante apposita comunicazione interna, inviata a cura della Direzione aziendale di volta in volta interessata. Di tutto il procedimento relativo all'ispezione devono essere redatti appositi verbali, che verranno conservati dall' Organismo di Vigilanza.

### **4.A – Elenco delle procedure per la prevenzione dei reati contro la Pubblica Amministrazione**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste le seguenti specifiche procedure:

- a) Codice Etico;
- b) Sign Off (H5 Gestione del Personale);
- c) Sign Off (H9 Contratti estimatori e resi di merce);
- d) Sistema ERP (Navision).

L'Organismo di Vigilanza cura che le procedure di cui al presente paragrafo siano idonee al rispetto delle prescrizioni in esso contenute e adeguate alle finalità in precedenza indicate.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

L'Organismo di Vigilanza vigila che nelle società appartenenti al Gruppo siano adottati principi e procedure coerenti con i principi e le procedure fatti propri dalla Società.

## PARTE SPECIALE

### SEZIONE "B"

#### **I REATI SOCIETARI (art. 25 ter del D. Lgs. 231/2001)**

In questa parte speciale sono individuate le aree di attività nel cui ambito possono essere commessi i reati societari di cui al D. Lgs. 231/2001.

Si riporta nel seguito una breve descrizione dei principali reati contemplati nell'art. 25-ter del Decreto, la cui commissione può comportare un beneficio a favore della Società.

#### **False comunicazioni sociali (artt. 2621, 2621-bis e 2622 c.c.)**

Si tratta di due ipotesi criminose che si differenziano per il verificarsi nella seconda delle ipotesi di un danno patrimoniale alla Società, ai soci o ai creditori.

Le due fattispecie si realizzano tramite l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla Legge, dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, idonei ad indurre in errore i destinatari della situazione economica, patrimoniale o finanziaria della Società o del Gruppo al quale essa appartiene, con l'intenzione di ingannare i soci, i creditori o il pubblico; ovvero l'omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla Legge.

Ai sensi dei precedenti articoli così come modificati dalla L. 262/2005 (successivamente modificata ed integrata dal D. Lgs. 303/2006) le fattispecie criminose sopra descritte possono essere commesse anche dai direttori generali e dirigenti preposti alla redazione dei documenti contabili societari.

Si precisa che:

- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- le informazioni false od omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della Società o del Gruppo al quale essa appartiene;
- la responsabilità si estende anche all'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla Società per conto di terzi.

Soggetti attivi del reato sono gli amministratori, se presenti i direttori generali, i sindaci ed i liquidatori (reato proprio).

L'art. 25 – *ter* prevede l'applicazione delle seguenti sanzioni pecuniarie:

- da 200 a 400 quote nel caso di False Comunicazioni Sociali (ex art. 2621 c.c)
- da 100 a 200 quote nel caso di False Comunicazioni Sociali per fatti di lieve entità (ex art. 2621-bis c.c.)
- da 400 a 600 quote nel caso di False Comunicazioni Sociali delle società quotate (ex art. 2622 c.c.)

Se in seguito alla commissione dei reati sopra indicati l'ente ha conseguito un profitto di rilevante entità la sanzione pecuniaria è aumentata di un terzo.

#### **Impedito controllo (artt. 2625 c.c.)**

La condotta consiste nell'impedire od ostacolare, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali.

Il reato, imputabile esclusivamente agli amministratori, è punito più gravemente se la condotta ha causato un danno.

La sanzione pecuniaria applicabile è compresa tra 200 e 360 quote. Se dalla commissione del reato l'ente consegue un profitto di rilevante entità la sanzione pecuniaria è aumentata di un terzo.

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

La condotta tipica prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione, anche mediante il compimento di operazioni simulate, dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli.

La sanzione pecuniaria applicabile è compresa tra 200 e 360 quote. Se dalla commissione del reato l'ente consegue un profitto di rilevante entità la sanzione pecuniaria è aumentata di un terzo.

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

Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.

La sanzione pecuniaria applicabile è compresa tra 200 e 260 quote. Se dalla commissione del reato l'ente consegue un profitto di rilevante entità la sanzione pecuniaria è aumentata di un terzo.

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

Il reato in questione si perfeziona con l'acquisto o la sottoscrizione da parte degli Amministratori, fuori dai casi consentiti dalla legge, di azioni o quote sociali proprie o della società controllante, che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

La sanzione pecuniaria applicabile è compresa tra 200 e 360 quote. Se dalla commissione del reato l'ente consegue un profitto di rilevante entità la sanzione pecuniaria è aumentata di un terzo.

**Operazioni in pregiudizio dei creditori (art. 2629 c.c.)**

La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di Legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o scissioni, che cagionino danno ai creditori.

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

Soggetti attivi del reato sono, anche in questo caso, gli amministratori.

La sanzione pecuniaria applicabile è compresa tra 300 e 660 quote. Se dalla commissione del reato l'ente consegue un profitto di rilevante entità la sanzione pecuniaria è aumentata di un terzo.

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

Questo reato riguarda esclusivamente le società con titoli quotati o diffusi in misura rilevante tra il pubblico, ovvero soggette a vigilanza da parte della Autorità Bancarie, Finanziarie e Assicurative. Pertanto non è rilevante per la Società.

**Formazione fittizia del capitale (art. 2632 c.c.)**

Tale reato si perfeziona nel caso in cui gli amministratori e i soci conferenti formino o aumentino fittiziamente il capitale della società mediante attribuzione di azioni o quote sociali in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti dei beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

La sanzione pecuniaria applicabile è compresa tra 200 e 360 quote. Se dalla commissione del reato l'ente consegue un profitto di rilevante entità la sanzione pecuniaria è aumentata di un terzo.

**Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)**

Il reato si perfeziona con la ripartizione da parte dei liquidatori di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori. Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

La sanzione pecuniaria applicabile è compresa tra 300 e 660 quote. Se dalla commissione del reato l'ente consegue un profitto di rilevante entità la sanzione pecuniaria è aumentata di un terzo.

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

La condotta tipica prevede che si determini con atti simulati o con frode la maggioranza in assemblea, allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Il reato può essere commesso da chiunque ("reato comune"), quindi anche da soggetti esterni alla società.

La sanzione pecuniaria applicabile è compresa tra 300 e 660 quote. Se dalla commissione del reato l'ente consegue un profitto di rilevante entità la sanzione pecuniaria è aumentata di un terzo.

### **Aggiotaggio (art. 2637 c.c.)**

La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare 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 idonee ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

Il reato può essere commesso da chiunque ("reato comune").

La sanzione pecuniaria applicabile è compresa tra 400 e 1.000 quote. Se dalla commissione del reato l'ente consegue un profitto di rilevante entità la sanzione pecuniaria è aumentata di un terzo.

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

L'art. 2638, c.c. individua due ipotesi di reato:

- la prima si realizza attraverso l'esposizione, nelle comunicazioni alle autorità di vigilanza previste dalla Legge (Consob, Isvap, Banca d'Italia), al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza, ovvero con l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima;
- la seconda si realizza con il semplice ostacolo all'esercizio delle funzioni di vigilanza, attuato consapevolmente, in qualsiasi forma, anche omettendo le comunicazioni dovute alle autorità di vigilanza.

In entrambe le modalità descritte i soggetti attivi nella realizzazione del reato sono gli amministratori, se presenti i direttori generali, i sindaci e i liquidatori.

La sanzione pecuniaria applicabile è compresa tra 400 e 800 quote. Se dalla commissione del reato l'ente consegue un profitto di rilevante entità la sanzione pecuniaria è aumentata di un terzo.

### **Corruzione tra privati (nei casi previsti dall'art. 2635 c.c., comma 3)**

Il reato è presupposto della responsabilità amministrativa degli enti di cui al D.lgs. 231/2001 nell'ipotesi in cui taluno, anche per interposta persona, offre promette o dà denaro o altra utilità non dovuti a:

- amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori di società o enti privati 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;
- chi esercita funzioni direttive (diverse da quelle proprie dei soggetti citati) il quale, anche per interposta persona, sollecita o riceve per sé o per altri, denaro o altra utilità non dovuti, o ne accetta la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà;
- persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui sopra.

La sanzione pecuniaria applicabile è da 400 a 600 quote.

### **Istigazione alla corruzione fra privati (art. 2635 bis c.c.)**

Il reato è presupposto della responsabilità amministrativa degli enti di cui al D.lgs. 231/2001 nell'ipotesi in cui taluno offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei 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, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, qualora l'offerta o la promessa non sia accettata.

La sanzione pecuniaria applicabile è da 200 a 400 quote.

### **1.B – Potenziali aree a rischio.**

Gran parte delle attività svolte dalla Digital Bros, nelle aree potenzialmente a rischio, sono regolamentate da procedure interne scritte rispondenti ai criteri imposti dal Decreto.

La formazione ed attuazione delle decisioni degli amministratori sono disciplinate dai principi e dalle prescrizioni contenute nella normativa vigente, dallo Statuto e dal Codice di Autodisciplina.

Le aree di attività considerate più specificatamente a rischio in relazione ai reati societari sono ritenute le seguenti:

1. redazione del bilancio, della relazione sulla gestione, del bilancio consolidato e di altre comunicazioni sociali;
2. operazioni societarie che possano incidere sull'integrità del capitale sociale;
3. le attività soggette a vigilanza da parte delle Autorità Pubbliche;
4. informative e rapporti con gli organi di informazione e stampa.

Eventuali integrazioni alle suddette aree di attività a rischio potranno essere suggerite dall'Amministratore Delegato al Consiglio di Amministrazione.

Sono individuate le seguenti categorie di operazioni e attività a rischio, nelle quali potrebbero essere commessi i reati previsti dall'art. 25-ter del Decreto:

- a) predisposizione di comunicazioni e prospetti informativi riguardanti la situazione economica, patrimoniale e finanziaria della società e del gruppo, ivi inclusi i bilanci e le relazioni periodiche;
- b) rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nei bilanci, nelle relazioni e in altri documenti di impresa;
- c) documentazione, archiviazione e conservazione delle informazioni relative all'attività di impresa;
- d) comunicazioni ad autorità pubbliche di vigilanza;
- e) situazioni di conflitto di interessi degli amministratori;
- f) acquisto, vendita o altre operazioni, in qualsiasi forma concluse su strumenti finanziari non quotati;
- g) gestione dei rapporti con la società di revisione;
- h) comunicazione di informazioni relative a strumenti finanziari non quotati.

### **2. B – Principi di comportamento e controllo nelle principali aree a rischio**

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 ter del D. Lgs. 231/2001); sono altresì proibite le violazioni ai principi ed alle procedure aziendali.

Al fine di evitare il verificarsi dei reati societari previsti dal D. Lgs. 231/01, tutti i Destinatari del presente Modello devono:

- Attenersi alle seguenti condotte:

- a) agire, ciascuno secondo la propria funzione, in osservanza dei principi di correttezza, trasparenza e collaborazione, nonché secondo le procedure statutariamente previste;
- b) mantenere una condotta improntata ai principi di correttezza, trasparenza e collaborazione nello svolgimento delle procedure volte alla formazione del bilancio, delle situazioni contabili periodiche e delle comunicazioni sociali in generale;
- c) mantenere una condotta improntata ai principi di correttezza, trasparenza e collaborazione nell'acquisizione, elaborazione e comunicazione delle informazioni destinate a consentire agli Azionisti ed agli Investitori di formarsi opinioni e/o giudizi sulla situazione patrimoniale, economica e finanziaria della Società;
- d) fornire informazioni veritiere ed appropriate sulla situazione economica, patrimoniale e finanziaria della Società;
- e) assicurare il regolare funzionamento della Società e degli Organi sociali, agevolando e garantendo ogni forma di controllo interno e promuovendo la libera formazione ed assunzione delle decisioni collegiali;
- f) osservare scrupolosamente tutte le norme di legge poste a tutela dell'integrità del capitale sociale;
- g) rispettare, in caso di riduzione del capitale sociale, di fusione e/o di scissione, le norme di legge poste a tutela dei creditori;
- h) osservare le procedure interne previste per la selezione e/o gestione dei rapporti con gli altri Destinatari del Modello;

- i) collaborare per il conseguimento dell'oggetto sociale;
- l) osservare le leggi in materia di tutela della concorrenza e del mercato e vigilare sulla perfetta osservanza delle stesse, nonché collaborare con le Autorità regolatrici del mercato e con le altre Autorità di Vigilanza;
- m) improntare le informazioni su strumenti finanziari non quotati al rispetto del diritto all'informazione, secondo criteri di accuratezza, coerenza con i principi e le politiche della Società ed in conformità con le leggi, le regole e le pratiche di condotta professionale.
- È, inoltre vietato:
- a) predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Digital Bros e del Gruppo nel suo insieme, nonché sull'evoluzione delle relative attività, sugli strumenti finanziari della Società e sui relativi diritti;
- b) omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società e del Gruppo nel suo insieme;
- c) alterare o, comunque, riportare in modo non corretto i dati e le informazioni destinati alla stesura di prospetti informativi;
- e) restituire conferimenti ai soci o esentare i soci dall'effettuarli, al di fuori dei casi specificatamente previsti dalla legge;
- f) ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve (anche non costituite con utili) che non possono per legge essere distribuite;
- g) acquistare o sottoscrivere azioni della Società fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge;
- h) effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;
- i) procedere in ogni modo a formazione o aumento fittizi del capitale sociale;
- l) ripartire i beni sociali tra i soci – in fase di liquidazione – prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli;
- m) tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale o della società di revisione;
- n) porre in essere, in occasione di assemblee, atti simulati o fraudolenti, finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- o) omettere di effettuare, con la dovuta chiarezza, completezza e tempestività, nei confronti delle Autorità in questione, tutte le comunicazioni, periodiche e non, previste dalla legge e dalla ulteriore normativa di settore, nonché la trasmissione dei dati e documenti previsti dalle norme in vigore e/o specificamente richiesti dalle predette Autorità;
- p) esporre in tali comunicazioni e nella documentazione trasmessa fatti non rispondenti al vero oppure occultare fatti concernenti la situazione economica, patrimoniale o finanziaria della Società e del Gruppo nel suo insieme;
- q) porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle Autorità pubbliche di Vigilanza, anche in sede di ispezione (espressa opposizione, rifiuti pretestuosi, comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);
- r) pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento o ingannatorio suscettibili di determinare riflessi su strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato ed idonei ad alterarne sensibilmente il prezzo.

### **3.B – Principi per la predisposizione delle procedure per la prevenzione dei reati societari**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste specifiche procedure, in forza delle quali:

- a) siano ricostruibili la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;

- b) non vi sia identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- c) i documenti riguardanti l'attività d'impresa siano archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;
- d) qualora il servizio di archiviazione e/o conservazione dei documenti sia svolto, per conto della Società, da un soggetto ad essa estraneo, il servizio deve essere regolato da un contratto nel quale si preveda, tra l'altro, che il soggetto che presta il servizio alla Società rispetti specifiche procedure di controllo idonee a non permettere la modificazione successiva dei documenti archiviati, se non con apposita evidenza;
- e) l'accesso ai documenti, di cui ai punti precedenti, già archiviati sia sempre motivato e consentito solo al soggetto competente in base alle norme interne, o a suo delegato, al Collegio Sindacale o organo equivalente, alla società di revisione o all'Organismo di Vigilanza;
- f) la scelta di consulenti esterni, ancorché selezionati localmente, avvenga sulla base di requisiti di professionalità, indipendenza e competenza e, in riferimento a essi sia motivata la scelta;
- g) non siano corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, agenti in misura non congrua rispetto alle prestazioni rese alla Società e non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;
- h) i sistemi di remunerazione premianti ai Dipendenti e Collaboratori rispondano a obiettivi realistici e coerenti con le mansioni e l'attività svolta e con le responsabilità affidate;
- i) la Società, ai fini dell'attuazione delle decisioni di impiego delle risorse finanziarie, si avvalga di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea;
- l) nessun pagamento può essere effettuato in contanti, salvo specifica autorizzazione da parte della funzione Amministrazione;
- m) le informazioni relative strumenti finanziari non quotati diffuse al pubblico devono provenire da fonti certe ed univoche e da elaborazioni complete ed accurate.

#### **4.B – Elenco delle procedure per la prevenzione dei reati societari**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste le seguenti specifiche procedure:

- a) Codice Etico;
- b) Procedura in materia di internal dealing;
- c) Procedura per la gestione delle informazioni privilegiate;
- d) Principi Contabili Gruppo Digital Bros 2018;
- e) Procedura per la rilevazione degli accadimenti aziendali 2013;
- f) Sign Off (H9 Contratti estimatori e resi di merce);
- g) Sistema ERP (Navision).

L'Organismo di Vigilanza cura che le procedure di cui al presente paragrafo siano idonee al rispetto delle prescrizioni in esso contenute e adeguate alle finalità in precedenza indicate.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

L'Organismo di Vigilanza vigila che nelle società appartenenti al Gruppo siano adottati principi e procedure coerenti con i principi e le procedure fatti propri dalla Società.

## PARTE SPECIALE

### SEZIONE “C”

#### **I REATI FINANZIARI O DI ABUSO DI MERCATO**

**(art. 25 sexies del D. Lgs. 231/2001 e art. 187-quinquies del TUF)**

In questa parte speciale sono individuate le aree di attività nel cui ambito possono essere commessi i reati finanziari o di abuso di mercato di cui al D. Lgs. 231/2001.

Si riportano di seguito una breve descrizione dei principali reati contemplati nell’art. 25-sexies del Decreto la cui commissione possa comunque comportare un beneficio da parte della Società.

#### **Abuso di informazioni privilegiate (art. 184 del TUF),**

l’illecito si commette nel caso in cui, nell’ambito della Società, qualcuno, in possesso di un’informazione privilegiata - in ragione della sua qualità di membro di organi di amministrazione, direzione o di controllo dell’emittente, della partecipazione al capitale dell’emittente, ovvero dell’esercizio di un’attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio - acquisti, venda o compia operazioni per conto proprio o di terzi su strumenti finanziari utilizzando l’informazione privilegiata posseduta; oppure comunichi l’informazione privilegiata posseduta ad altri, al di fuori del normale esercizio del lavoro; oppure raccomandi o induca altri al compimento di talune delle operazioni sopra indicate.

L’informazione è privilegiata se concerne, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, non è ancora stata resa pubblica, ha carattere preciso, ed è idonea, se resa pubblica, ad influire in modo sensibile sul prezzo dello strumento finanziario interessato dall’informazione.

Un’informazione si ritiene di carattere preciso se rispetta due condizioni: si riferisce ad un complesso di circostanze esistente o che si possa ragionevolmente prevedere che verrà ad esistenza o ad un evento verificatosi o che si possa ragionevolmente prevedere che si verificherà; ed è sufficientemente specifica da consentire di trarre conclusioni sul possibile effetto del complesso di circostanze o dell’evento come sopra descritto sui prezzi degli strumenti finanziari.

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

Per “strumenti finanziari” si intendono gli strumenti finanziari di cui all’art. 1 del TUF, 2° comma, ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altro Paese dell’Unione europea, nonché qualsiasi altro strumento ammesso o per il quale è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato di un Paese dell’Unione europea.

#### **Abuso di informazioni privilegiate (art. 187-bis del TUF),**

Il reato si commette qualora chiunque all’interno della Società, in possesso di una informazione privilegiata in ragione della sua qualità di membro di organi di amministrazione, direzione o di controllo dell’emittente, della partecipazione al capitale dell’emittente, ovvero dell’esercizio di un’attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio, o di chi, per qualunque ragione in possesso di informazioni privilegiate, conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse, acquisti, venda o compia operazioni per conto proprio o di terzi su strumenti finanziari utilizzando l’informazione privilegiata posseduta; oppure comunichi l’informazione privilegiata posseduta ad altri al di fuori del normale esercizio del lavoro; oppure raccomandi o induca altri al compimento di talune delle operazioni sopra indicate. Sono fatte salve le sanzioni penali quando il fatto costituisce reato. Per la definizione di informazione privilegiata e di strumenti finanziari si rinvia a quanto stabilito al punto precedente.

Il concetto di informazione privilegiata rappresenta il fulcro attorno al quale ruota l’intera disciplina sull’*insider trading* e quella concernente l’informazione societaria disciplinata nel Titolo III, Capo I, art. 114 e seguenti del TUF e nel Regolamento Emittenti n. 11971/1999.

Secondo quanto previsto dall'art. 181 del TUF si ritengono di carattere privilegiato le informazioni aventi le seguenti caratteristiche (qui di seguito le "Informazioni Privilegiate"):

di carattere preciso, nel senso che:

- deve trattarsi di informazioni inerenti a circostanze o eventi esistenti o verificatisi o a circostanze o eventi che ragionevolmente possa prevedersi che verranno ad esistenza o che si verificheranno (il riferimento è ai casi in cui la notizia è in via di formazione e riguarda eventi non ancora verificatisi, si pensi al caso caratterizzato dalla notizia che una società quotata stia per lanciare un'OPA, oppure il caso riguardante un piano strategico di riposizionamento produttivo della società emittente i titoli);
- deve trattarsi di informazioni specifiche, vale a dire che l'informazione deve essere sufficientemente esplicita e dettagliata, in modo che chi la impiega sia posto in condizione di ritenere che dall'uso potranno effettivamente verificarsi quegli effetti sul prezzo degli strumenti finanziari;
- non ancora rese pubbliche;
- concernenti, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari (*corporate information*, relative alla situazione economica patrimoniale o a vicende organizzative dell'emittente; *market information*);
- *price sensitive* secondo l'investitore ragionevole, nel senso che, se rese pubbliche, potrebbero influire in modo sensibile sul prezzo degli strumenti finanziari.

Il recepimento della normativa comunitaria in materia di abusi di mercato ha apportato rilevanti innovazioni al sistema informativo previsto per le società quotate. In particolare, il Regolamento (UE) 596/2014 e la Direttiva 2014/57/UE intervengono incisivamente sul comparto degli abusi di mercato, attraverso scelte politico-criminali nette che risentono delle elaborazioni sovranazionali sulla "materia penale" e disegnano un sistema sanzionatorio unitario rispettoso del principio del *ne bis in idem*. Direttiva e Regolamento sono dunque destinati a conformare il diritto punitivo interno sia per quanto concerne la fattispecie di abuso di informazioni privilegiate, sia con riguardo all'ipotesi di manipolazione del mercato.

#### **Manipolazione del mercato (art. 185 TUF)**

La fattispecie punisce chiunque diffonde notizie false (c.d. aggio taggio informativo) o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari (ammessi o per i quali sia stata presentata richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altro paese dell'Unione Europea) (c.d. aggio taggio negoziativo). Con riferimento alla diffusione di informazioni false o fuorvianti, preme ribadire che questo tipo di manipolazione del mercato comprende anche i casi in cui la creazione di un'indicazione fuorviante derivi dall'inosservanza degli obblighi di comunicazione da parte dell'emittente o di altri soggetti obbligati.

La Legge Comunitaria 2004, ha introdotto il sistema del cd. "doppio binario" per cui, alle ipotesi penali di abuso di informazioni privilegiate e di manipolazione del mercato descritte possono sommarsi ipotesi di illecito amministrativo per gli stessi reati previste dalla Parte V, Titolo I – *Bis*, capo III del TUF agli artt. 187 *bis* e 187 *ter*.

Le prime saranno accertate e sanzionate dalla magistratura penale, le seconde direttamente ed autonomamente dalla Consob.

La "responsabilità dell'ente", oltre che ai delitti, è estesa anche a tali ipotesi di illecito amministrativo, in virtù di quanto previsto l'art. 187-*quinquies* TUF.

Le definizioni degli illeciti amministrativi relativi all'abuso di informazioni privilegiate ed alla manipolazione del mercato riprendono quelle delineate nelle rispettive fattispecie penali ma hanno una portata più ampia ed inoltre se ne distinguono richiedendo, quale elemento soggettivo anche la sola colpa e non necessariamente il dolo.

A tale titolo l'ente è responsabile del pagamento di una somma pari all'importo della sanzione amministrativa irrogata - per gli illeciti amministrativi di abuso di informazioni privilegiate (sanzione che può arrivare fino a quindici milioni di Euro e che è aumentata fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dall'illecito quando, per le qualità personali del colpevole ovvero per l'entità del prodotto o del profitto conseguito dall'illecito, essa appaia inadeguata anche se applicata nel massimo) e di manipolazione del mercato (sanzione che

può arrivare fino a venticinque milioni di Euro e che è aumentata fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dall'illecito quando, per le qualità personali del colpevole, per l'entità del prodotto o del profitto conseguito dall'illecito ovvero per gli effetti prodotti sul mercato, essa appaia inadeguata anche se applicata nel massimo) commessi nel suo interesse o a suo vantaggio.

Anche in tal caso, se il prodotto o il profitto conseguito dall'ente è di rilevante entità, la sanzione potrà essere aumentata fino a dieci volte tale prodotto o profitto.

#### **Manipolazione del mercato, (art. 187-ter del TUF),**

La disposizione di cui all'art. 187-ter TUF amplia le condotte rilevanti ai fini dell'applicabilità delle sanzioni amministrative rispetto a quelle penalmente sanzionate dalla corrispondente fattispecie delittuosa e punisce chiunque, tramite qualsiasi mezzo di informazione, diffonde informazioni, voci o notizie false o fuorvianti che forniscano o “*siano suscettibili di fornire indicazioni false ovvero fuorvianti in merito agli strumenti finanziari*”, a prescindere quindi dagli effetti (laddove l'art. 185 TUF richiede, ai fini della sanzionabilità delle condotte, che le notizie false siano “*concretamente idonee*” ad alterare i prezzi).

Anche in questo caso il dolo non è richiesto come requisito soggettivo generale.

La definizione dell'illecito amministrativo relativo alla manipolazione di mercato risulta dunque più dettagliata rispetto all'illecito penale e comprende:

- a) le operazioni od ordini di compravendita che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari;
- b) le operazioni od ordini di compravendita che consentono, tramite l'azione di una o più persone che agiscono di concerto, di fissare il prezzo di mercato di uno o più strumenti finanziari ad un livello anomalo o artificiale;
- c) le operazioni od ordini di compravendita che utilizzino artifici od ogni altro tipo di inganno o di espediente;
- d) gli altri artifici idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

Il comma 4 dell'articolo in esame prevede che non può essere assoggettato a sanzione amministrativa chi dimostra di aver agito per motivi legittimi e in conformità alle prassi di mercato ammesse nel mercato interessato.

#### **Falso in prospetto (art. 173-bis TUF)**

Tale ipotesi di reato consiste nell'espone false informazioni ovvero nell'occultare dati o notizie all'interno dei prospetti (per tali intendendosi i documenti richiesti ai fini della sollecitazione all'investimento o dell'ammissione alla quotazione nei mercati regolamentati, ovvero da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio) secondo modalità idonee ad indurre in errore i destinatari dei prospetti stessi.

Si precisa che:

- deve sussistere l'intenzione di ingannare i destinatari dei prospetti;
- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto.

Il reato è costruito come un reato comune, che può essere commesso da “chiunque” ponga in essere la condotta criminosa.

#### **1.C – Potenziali aree a rischio**

In considerazione

- delle attività svolte dalla Digital Bros e considerato che la Digital Bros sin dall'ottobre 2000 è quotata presso il mercato gestito e regolamentato da Borsa Italiana S.p.A. e la conseguente negoziazione di strumenti finanziari della Digital Bros in mercati regolamentati
- delle attività aventi ad oggetto l'acquisto, la vendita o altre operazioni su strumenti finanziari di cui all'art. 180 lett. a) e b) del TUF;
- delle attività di gestione dei rapporti con gli investitori, gli analisti finanziari, giornalisti e con altri rappresentanti dei mezzi di comunicazione di massa;
- dell'attività di redazione dei documenti informativi e dei comunicati concernenti la Digital Bros e le società appartenenti al Gruppo, destinati al pubblico per legge o per decisione della società;

– dell’attività di comunicazione al pubblico dei documenti informativi, dei comunicati concernenti la Società e il Gruppo, nonché di ogni informazione privilegiata ai sensi dell’art. 181 del TUF;

– di ogni altra area di attività o di procedure della società o di società appartenenti al Gruppo che siano collegate alla nascita, alla formazione e alla comunicazione, interna o esterna, di informazioni privilegiate di cui all’art. 181 del TUF;

– dell’attività di gestione di Informazioni Privilegiate ad esempio, nuovi prodotti/servizi e mercati, dati contabili di periodo, dati previsionali e obiettivi quantitativi concernenti l’andamento della gestione, comunicazioni relative ad operazioni di fusione/scissione e a nuove iniziative di particolare rilievo ovvero a trattative e/o accordi in merito all’acquisizione e/o cessione di *asset* significativi, dati quantitativi riguardanti la distribuzione di prodotti, la conclusione di particolari licenze, attività di M&A;

sono individuate le seguenti categorie di operazioni e attività a rischio, nelle quali potrebbero essere commessi i reati previsti dagli artt. 25 sexies del Decreto o gli illeciti amministrativi previsti dall’art. 187-quinquies del TUF:

a) redazione e diffusione sia a mezzo stampa che online e trasmissioni radiofoniche di articoli e notizie di carattere giornalistico relative a strumenti finanziari di cui all’art. 180 lett. a) del TUF o alle società e gruppi loro emittenti;

b) acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto azioni proprie della Società, delle società controllate o delle società controllanti, incluse tra gli strumenti finanziari di cui all’art. 180 lett. a) del TUF;

c) acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto altri strumenti finanziari di cui all’art. 180 lett. a) del TUF emessi dalla Società, da società controllanti, controllate o collegate;

d) acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari diversi da quelli di cui alla lettera precedente, il cui valore sia collegato a tali strumenti finanziari (c.d. derivati);

e) acquisto, vendita o altre operazioni, in qualsiasi forma concluse, aventi ad oggetto strumenti finanziari di cui all’art. 180, lett. a) e b) del TUF, diversi da quelli di cui alle lettere precedenti, ammessi alla negoziazione, o per i quali è stata presentata una richiesta di ammissione alla negoziazione, in un mercato regolamentato italiano o di altro Paese dell’Unione europea, nonché qualsiasi altro strumento ammesso o per il quale è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato di un Paese dell’Unione europea;

f) redazione dei documenti informativi, dei comunicati, di materiale informativo in qualunque forma predisposti, normalmente destinati ad investitori, analisti finanziari, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o al pubblico in generale;

g) organizzazione e partecipazione a incontri, in qualunque forma tenuti, con investitori, analisti finanziari, giornalisti e altri rappresentanti dei mezzi di comunicazione di massa;

h) comunicazione a terzi e al mercato di informazioni concernenti la società e le società appartenenti al Gruppo, non ancora comunicate al pubblico e destinate alla diffusione, per legge o per decisione della società;

i) processi di gestione delle informazioni privilegiate.

## **2.C – Principi di comportamento e controllo nelle principali aree a rischio**

Tutte le attività, nell’ambito delle categorie di operazioni a rischio devono essere svolte in conformità delle leggi, procedure e regolamenti vigenti, al Modello, al Codice di Autodisciplina ed ai valori e alle politiche e regole della Digital Bros.

I seguenti principi si applicano nell’ambito della Digital Bros a tutti i Destinatari del presente Modello.

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 sexies del D. Lgs. 231/2001 e gli illeciti amministrativi previsti dall’art. 187-quinquies del TUF); sono altresì proibite le violazioni ai principi ed alle procedure aziendali.

Fermo restando quanto sopra, per tutti gli amministratori, sindaci e Dipendenti della Digital Bros e delle società del gruppo, è vietato:

- 1) utilizzare Informazioni Privilegiate, come di seguito definite, in funzione della propria posizione all'interno del Gruppo o per il fatto di essere in rapporti d'affari con il Gruppo, per negoziare, direttamente o indirettamente, azioni della Digital Bros, di società clienti o concorrenti, o di altre società o comunque per trarne un vantaggio personale, così come per favorire soggetti terzi o la società o altre società del Gruppo;
- 2) rivelare a terzi Informazioni Privilegiate relative al Gruppo, se non nei casi in cui tale rivelazione sia richiesta da leggi, da altre disposizioni regolamentari o da specifici accordi contrattuali con cui le controparti si siano impegnate a utilizzarle esclusivamente per i fini per i quali dette informazioni sono trasmesse e a mantenerne la confidenzialità;
- 3) partecipare a gruppi di discussione o chat room su Internet aventi ad oggetto strumenti finanziari o emittenti strumenti finanziari e nei quali vi sia uno scambio di informazioni concernenti il Gruppo, le sue società, società concorrenti o strumenti finanziari emessi da tali soggetti, a meno che non si tratti di incontri istituzionali per i quali sia stata già compiuta una verifica di legittimità da parte delle funzioni competenti o vi sia uno scambio di informazioni il cui carattere non privilegiato sia evidente;
- 4) agire di concerto per acquisire una posizione dominante sull'offerta o sulla domanda di uno strumento finanziario che abbia l'effetto di fissare, direttamente o indirettamente, i prezzi di acquisto o di vendita o determinare altre condizioni commerciali non corrette;
- 5) acquistare o vendere strumenti finanziari alla chiusura del mercato con l'effetto di ingannare gli investitori che operano sulla base dei prezzi di chiusura;
- 6) diffondere una valutazione su uno strumento finanziario (o indirettamente sul suo emittente) dopo aver precedentemente preso posizione sullo strumento finanziario, beneficiando di conseguenza dell'impatto della valutazione diffusa sul prezzo di detto strumento, senza avere allo stesso tempo comunicato al pubblico, in modo corretto ed efficace, l'esistenza di tale conflitto di interesse;
- 7) effettuare operazioni di acquisto o di vendita di uno strumento finanziario senza che si determini alcuna variazione negli interessi o nei diritti o nei rischi di mercato del beneficiario delle operazioni o dei beneficiari che agiscono di concerto o in modo collusivo;
- 8) inserire ordini, specie nei mercati telematici, a prezzi più alti (bassi) di quelli delle proposte presenti dal lato degli acquisti (vendite) al fine di fornire indicazioni fuorvianti dell'esistenza di una domanda (offerta) sullo strumento finanziario a tali prezzi più elevati (bassi);
- 9) acquistare o vendere intenzionalmente strumenti finanziari o contratti derivati verso la fine delle negoziazioni in modo da alterare il prezzo finale dello strumento finanziario o del contratto derivato;
- 10) colludere sul mercato secondario dopo un collocamento effettuato nell'ambito di un'offerta al pubblico;
- 11) concludere operazioni o impartire ordini in modo tale da evitare che i prezzi di mercato degli strumenti finanziari del Gruppo scendano al di sotto di un certo livello, principalmente per sottrarsi alle conseguenze negative derivanti dal connesso peggioramento del rating degli strumenti finanziari emessi. Questo comportamento deve essere tenuto distinto dalla conclusione di operazioni rientranti nei programmi di acquisto di azioni proprie o nella stabilizzazione degli strumenti finanziari previsti dalla normativa;
- 12) concludere operazioni in un mercato su uno strumento finanziario con la finalità di influenzare impropriamente il prezzo dello stesso strumento finanziario o di altri strumenti finanziari collegati negoziati sullo stesso o su altri mercati;
- 13) concludere un'operazione o una serie di operazioni per nascondere quale sia la vera proprietà di uno strumento finanziario, tramite la comunicazione al pubblico, in violazione alle norme che regolano la trasparenza degli assetti proprietari, della proprietà di strumenti finanziari a nome di altri soggetti collusi (questo comportamento non riguarda i casi in cui esistono motivi legittimi che consentono l'intestazione degli strumenti finanziari in nome di un soggetto diverso dal proprietario. Inoltre, una scorretta comunicazione di una partecipazione rilevante non implica necessariamente una manipolazione del mercato);
- 14) diffondere informazioni di mercato false o fuorvianti tramite mezzi di comunicazione, compreso Internet, o tramite qualsiasi altro mezzo;

- 15) aprire una posizione lunga su uno strumento finanziario ed effettuare ulteriori acquisti e/o diffondere fuorvianti informazioni positive sullo strumento finanziario in modo da aumentarne il prezzo;
- 16) prendere una posizione ribassista su uno strumento finanziario ed effettuare un'ulteriore attività di vendita e/o diffondere fuorvianti informazioni negative sullo strumento finanziario in modo da ridurre il prezzo;
- 17) aprire una posizione su uno strumento finanziario e chiuderla immediatamente dopo che è stata resa nota al pubblico;
- 18) operare creando inusuali concentrazioni di operazioni in concerto con altri soggetti su un particolare strumento finanziario;
- 19) vendere tutti i titoli che si possiedono in portafoglio per investire la liquidità ricavata su uno specifico strumento finanziario;
- 20) richiedere l'immediata esecuzione di un ordine senza curarsi del prezzo al quale l'ordine verrebbe eseguito;
- 21) realizzare un'inusuale operatività sulle azioni di una società prima dell'annuncio di Informazioni Privilegiate relative alla società;
- 22) realizzare operazioni senza alcuna altra apparente motivazione che quella di aumentare o ridurre il prezzo di uno strumento finanziario o di aumentare i quantitativi scambiati su uno strumento finanziario;
- 23) richiedere l'esecuzione di ordini che, a causa delle loro dimensioni rispetto alla liquidità di uno specifico strumento finanziario, avranno chiaramente un impatto significativo sulla domanda o sull'offerta o sul prezzo o sulla valutazione di tale strumento finanziario, specie quando tali ordini portano alla esecuzione di operazioni nei periodi di negoziazione utili alla determinazione di prezzi di riferimento, ad esempio verso la chiusura delle negoziazioni;
- 24) realizzare operazioni che sembrano avere la finalità di aumentare il prezzo di uno strumento finanziario nei giorni precedenti all'emissione di uno strumento finanziario derivato collegato o di uno strumento finanziario convertibile;
- 25) realizzare operazioni che, proprio nei giorni precedenti l'emissione di uno strumento finanziario derivato collegato o di uno strumento finanziario convertibile, sembrano avere la finalità di sostenere il prezzo dello strumento finanziario in presenza di un andamento discendente dei prezzi di tale strumento finanziario;
- 26) realizzare operazioni che sembrano tentare di modificare la valutazione di una posizione senza che venga modificata, in aumento o in diminuzione, la dimensione della posizione stessa;
- 27) realizzare operazioni che sembrano cercare di aumentare o ridurre il prezzo medio ponderato del giorno o di un periodo della sessione di negoziazione;
- 28) effettuare operazioni che sembrano cercare di aggirare gli accorgimenti previsti dai meccanismi di negoziazione (ad esempio, con riferimento ai limiti quantitativi, ai parametri relativi al differenziale tra le proposte di acquisto e di vendita, ai trading halt sui prezzi, ecc.);
- 29) cancellare ordini per quantitativi importanti pochi secondi prima del termine dell'asta a chiamata elettronica determinando una significativa variazione del prezzo teorico dell'asta e, quindi, del prezzo dell'asta;
- 30) effettuare operazioni che nel giorno di scadenza di uno strumento finanziario derivato sembrano finalizzate a far passare il prezzo dello strumento finanziario sottostante al di sopra del prezzo di esercizio dello strumento finanziario derivato;
- 31) effettuare operazioni che sembrano cercare di modificare il prezzo di regolamento di uno strumento finanziario quando questo prezzo è utilizzato come riferimento per il calcolo dei margini.

### **3.C – Principi per la redazione delle procedure per la prevenzione dei reati finanziari o di abuso di mercato**

Per le attività principali nell'ambito delle categorie di operazioni a rischio sopra individuate le procedure specifiche devono prevedere che:

- a) siano ricostruibili i procedimenti mediante i quali sono elaborate e assunte le decisioni, la formazione degli atti e i relativi livelli autorizzativi, in modo che sia garantita la trasparenza delle scelte effettuate e le motivazioni che le hanno ispirate;

- b) non vi si identifichino soggettivamente fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza documentale delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- c) i documenti riguardanti le informazioni privilegiate o destinate a divenire privilegiate siano archiviati e conservati, a cura della funzione competente o del responsabile incaricato, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza dell'accesso ai documenti già archiviati, di cui alle due lettere precedenti; l'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate in base alle norme interne;
- d) siano identificate, all'interno della società, le informazioni privilegiate o destinate a diventare privilegiate, nonché i criteri idonei a qualificare le informazioni come privilegiate o destinate a divenire tali. La precisazione dei criteri di identificazione delle informazioni privilegiate o destinate a divenire tali, devono essere effettuate a cura delle funzioni societarie competenti e sottoposte al parere dell'Organismo di Vigilanza. Devono inoltre essere adottate misure per proteggere, conservare e aggiornare le informazioni e, laddove, queste riguardino procedimenti a più fasi, integrare il contenuto delle informazioni stesse;
- e) sia assicurata la riservatezza delle informazioni privilegiate o destinate a diventare privilegiate, all'interno della società, sia nel caso in cui l'informazione si trovi su supporto informatico sia che si trovi su supporto cartaceo;
- f) siano assicurate misure idonee ad evitare la comunicazione impropria e non autorizzata all'interno o all'esterno della società delle informazioni privilegiate o destinate a diventare privilegiate. Le misure idonee possono essere dichiarazioni di impegno a rispettare la riservatezza delle informazioni stesse, rilasciate dalle persone che hanno legittimo accesso alle informazioni ovvero di natura tecnologica, al fine di evitare la duplicazione, la trasmissione o l'asportazione indebita di documenti nell'accezione di cui all'art. 491-bis c.p. - di qualsivoglia natura, contenenti le informazioni privilegiate o destinate a diventare privilegiate o la loro indebita apprensione;
- g) siano identificate le persone che, in ragione dell'attività lavorativa o professionale ovvero in ragione delle funzioni svolte, gestiscono le informazioni privilegiate o destinate a divenire privilegiate;
- h) siano identificate le persone che, in ragione dell'attività lavorativa o professionale ovvero in ragione delle funzioni svolte, hanno accesso alle informazioni privilegiate o destinate a divenire privilegiate;
- i) siano assicurate misure idonee ad evitare la comunicazione selettiva di informazioni privilegiate e destinate a divenire privilegiate;
- l) siano previste misure volte a vietare, in determinati periodi dell'esercizio sociale che precedono o sono successivi alla diffusione di informazioni privilegiate da parte della società, il compimento di operazioni (c.d. blocking periods) aventi ad oggetto strumenti finanziari emessi dalla società o a questi collegati, da parte dei soggetti che svolgono funzioni di amministrazione, di controllo o di direzione nella Società e dei dirigenti che abbiano regolare accesso a informazioni privilegiate e detengano il potere di adottare decisioni di gestione che possono incidere sull'evoluzione e sulle prospettive future della Società (c.d. «persone rilevanti»);
- m) sia assicurata la veridicità, la completezza e la correttezza delle informazioni comunicate a investitori, analisti finanziari, giornalisti e altri rappresentanti dei mezzi di comunicazione di massa o il pubblico in generale;
- n) i rapporti con investitori, analisti finanziari, giornalisti, altri rappresentanti dei mezzi di comunicazione di massa o con il pubblico in generale siano tenuti esclusivamente da soggetti appartenenti alle funzioni competenti, nel rispetto dei tempi e delle modalità stabilite dalla legge, dalle Autorità di Vigilanza del mercato e dalle procedure contemplate dal sistema di controllo interno;
- o) siano stabilite misure idonee per verificare e controllare in via preventiva la legittimazione alla partecipazione e i contenuti da trattare negli incontri, in qualunque forma tenuti, con investitori, analisti finanziari, giornalisti o altri rappresentanti dei mezzi di comunicazione di massa.

#### **4.C – Elenco delle procedure per la prevenzione dei reati finanziari o di abuso di mercato**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste le seguenti specifiche procedure:

- a) Codice Etico;
- b) Procedura in materia di internal dealing;
- c) Procedura per la gestione delle informazioni privilegiate.

L'Organismo di Vigilanza cura che le procedure di cui al presente paragrafo siano idonee al rispetto delle prescrizioni in esso contenute e adeguate alle finalità in precedenza indicate.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

L'Organismo di Vigilanza vigila che nelle società appartenenti al Gruppo siano adottati principi e procedure coerenti con i principi e le procedure fatti propri dalla Società.

**PARTE SPECIALE**  
**SEZIONE “D”**

**I REATI CONTRO LA PERSONALITA' INDIVIDUALE ED I REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI E GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO**  
**(artt. 25-quinquies, 25-septies del D. Lgs. 231/2001)**

La Legge 3 agosto 2007, n. 123, con l'inserimento nel Decreto 231/2001 dell'art. 25-septies, ha esteso il regime della responsabilità amministrativa delle persone giuridiche alle ipotesi di omicidio colposo e lesioni colpose gravi o gravissime (articoli 589 e 590, comma 3, c.p.), commessi con violazione delle norme antinfortunistiche e sulla tutela della salute sul lavoro.

Le sanzioni previste dal Decreto potranno essere applicate esclusivamente qualora i reati siano stati commessi nell'interesse o a vantaggio dell'Ente (anche potenziale), ovvero quando la violazione delle norme antinfortunistiche sia finalizzata ad un risparmio, in termini non soltanto strettamente economici, per la Società.

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

Il reato si configura quando chiunque causa per colpa la morte di una persona. Nel caso di morte di una o più persone e di lesioni di una o più persone è applicata la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo.

Nel caso in cui il delitto venga commesso in violazione delle norme sulla tutela della salute e sicurezza sul lavoro, è prevista l'applicazione di una sanzione pecuniaria compresa tra 250 e 500 quote e/o di una sanzione interdittiva per una durata non inferiore a tre mesi e non superiore ad un anno.

Invece, nel caso in cui il reato venga commesso con violazione delle norme in materia di salute e sicurezza sul lavoro di cui al decreto legislativo attuativo della delega di cui alla L. 3 agosto 2007, n. 123 (D.Lgs. n. 81/2008), la sanzione è pari a 1000 quote.

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

Il reato si configura quando chiunque causa per colpa una lesione personale. Nel caso di lesioni di una o più persone è applicata la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo.

La lesione personale è grave (art. 583 c.p.) se:

- dal fatto deriva una malattia che mette in pericolo la vita della persona offesa, oppure una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;
- il fatto produce l'indebolimento permanente di un senso o di un organo.

La lesione personale è gravissima (art. 583 c.p.), se dal fatto deriva:

- una malattia certamente o probabilmente insanabile;
- la perdita di un senso;
- la perdita di un arto, o una mutilazione che renda l'arto inservibile, oppure la perdita dell'uso di un organo o della capacità di procreare, oppure una permanente e grave difficoltà del linguaggio;
- la deformazione, oppure lo sfregio permanente del viso.

Nel caso in cui la lesione personale sia almeno grave e commessa in violazione delle norme sulla tutela della salute e sicurezza sul lavoro, è prevista l'applicazione di una sanzione pecuniaria in misura non superiore a 250 quote e/o di una sanzione interdittiva per una durata non superiore a sei mesi.

**Riduzione o mantenimento in schiavitù o in servitù (art. 600 cod. pen.)**

Vi incorre chiunque esercita su una persona poteri corrispondenti a quelli del diritto di proprietà ovvero chiunque riduce o mantiene una persona in uno stato di soggezione continuativa,

costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento.

**Prostituzione minorile (art. 600-bis cod. pen.)**

Tale ipotesi di reato si configura nei confronti di chiunque induca alla prostituzione una persona di età inferiore agli anni diciotto ovvero ne favorisca o sfrutti la prostituzione.

**Pornografia minorile (art. 600-ter cod. pen.)**

Tale ipotesi di reato si configura nei confronti di chiunque sfrutti minori degli anni diciotto al fine di realizzare esibizioni pornografiche o di produrre materiale pornografico ovvero chiunque faccia commercio del materiale pornografico di cui al primo comma.

La fattispecie punisce anche chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisca, divulghi o pubblicizzi il materiale pornografico di cui al primo comma, ovvero distribuisca o divulghi notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto; ovvero chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, consapevolmente ceda ad altri, anche a titolo gratuito, materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto.

**Detenzione di materiale pornografico (art. 600-quater cod. pen.)**

Tale ipotesi di reato si configura nei confronti di chiunque, al di fuori delle ipotesi previste nell'articolo 600-ter cod. pen., consapevolmente si procuri o disponga di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto.

**Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies cod. pen.)**

Tale ipotesi di reato si configura nei confronti di chiunque organizzi o propagandi viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori o comunque comprendenti tale attività.

**Tratta di persone (art. 601 cod. pen.)**

Tale ipotesi di reato si configura nei confronti di chiunque commetta tratta di persona che si trova nelle condizioni di cui all'articolo 600 cod. pen. ovvero, al fine di commettere i delitti di cui al medesimo articolo, la induca mediante inganno o la costringa mediante violenza, minaccia, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante promessa o dazione di somme di denaro o di altri vantaggi alla persona che su di essa ha autorità, a fare ingresso o a soggiornare o a uscire dal territorio dello Stato o a trasferirsi al suo interno.

**Acquisto e alienazione di schiavi (art. 602 cod. pen.)**

Tale ipotesi di reato si configura nei confronti di chiunque, fuori dei casi indicati nell'articolo 601 cod. pen., acquisti o alieni o ceda una persona che si trova in una delle condizioni di cui all'articolo 600 cod. pen.

Per quanto attiene ai reati sopra considerati, va tenuto presente che possono essere ritenuti responsabili degli stessi non solo i soggetti che direttamente realizzino le fattispecie criminose, ma anche i soggetti che consapevolmente agevolino, anche solo finanziariamente, la medesima condotta.

Di conseguenza, potrebbero rientrare nell'ipotesi di reato sopra considerate, le eventuali erogazioni di risorse economiche in favore di soggetti terzi, effettuate da parte dell'Ente con la consapevolezza che le erogazioni stesse possano essere utilizzate da tali soggetti per finalità criminose.

**Intermediazione illecita e sfruttamento del lavoro (art. 603 bis cod. pen.)**

La norma punisce chiunque:

- recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;

- utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.

E' prevista un'aggravante se i fatti sono commessi mediante violenza o minaccia.

Gli indici dello sfruttamento sono:

- la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;
- la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
- la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
- la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

#### **Adescamento di minorenni (art. 609-undecies cod. pen.)**

Vi incorre chiunque, allo scopo di commettere i reati di cui agli articoli 600, 600-bis, 600-ter e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-quater, 609-quinquies e 609-octies, adesci un minore di anni sedici. Per adescamento si intende qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione.

#### **1.D - Potenziali aree a rischio**

L'ambito della tutela della salute e della sicurezza del lavoro è già ampiamente disciplinato (Dlgs 81/2008) e l'adeguamento alle previsioni normative viene oggi assolto, su incarico del datore di lavoro, dal responsabile del servizio di prevenzione e protezione (RSPP) della Società.

Nell'ottica di un'armonizzazione tra quanto già effettuato nell'ambito della prevenzione degli infortuni sul lavoro e quanto previsto dal D.Lgs. 231/2001, la Società deve fare in modo che si dia piena attuazione alle procedure già inserite nel piano della sicurezza dai rischi professionali e della prevenzione degli infortuni sul lavoro.

In considerazione delle attività svolte dalla Digital Bros e della struttura interna adottata, ai sensi dell'art. 6 del Decreto, nonché sulla base del documento di valutazione dei rischi, predisposto ai sensi del D. Lgs. 81/2008 e sue successive modifiche ed integrazioni., sono individuate le seguenti categorie di operazioni e attività a rischio, nelle quali potrebbero essere commessi i reati previsti dall'art. 25 septies del Decreto:

- a) attività di produzione e sviluppo dei videogiochi presso eventuali fornitori;
- b) attività presso i magazzini della Società;
- c) attività di manutenzione di impianti e macchinari tramite l'impiego di personale interno o esterno alla Società;
- d) attività di manutenzione e nuove realizzazioni dei fabbricati e degli impianti della Società o in uso alla stessa inclusi i locali adibiti ad ufficio;
- e) attività di manutenzione e movimentazione di mobili, arredi e delle attrezzature ad uso della Società;
- f) attività lavorative con utilizzo di videoterminali;
- g) accesso, transito e permanenza nei locali in uso alla Società, nello svolgimento delle sue attività da parte di Dipendenti e soggetti esterni.

#### **2.D - Principi di comportamento e controllo nelle principali aree a rischio**

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-septies del D. Lgs. 231/2001); sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

Al fine di evitare il verificarsi dei reati di cui alla presente Parte Speciale tutti i Destinatari del presente Modello devono attenersi alle specifiche regole e procedure che sono e saranno predisposte ai sensi del D. Lgs. 81/2008 e sue successive modifiche ed integrazioni.

Fermo restando quanto sopra i Destinatari del presente Modello devono:

- Attenersi alle seguenti condotte:

- a) osservare rigorosamente tutte le leggi e i regolamenti e procedure in materia di sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro che disciplinano l'accesso, il transito e lo svolgimento delle attività lavorative presso i locali in uso alla Società;
- b) partecipare ai corsi organizzati dalla Società in materia di sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro, ecologia e sullo svolgimento delle specifiche mansioni, ai quali saranno invitati;
- c) fornire adeguati dispositivi di protezione individuali ai propri dipendenti, conformi alle normative vigenti e in funzione delle mansioni da quelli svolte;
- d) identificare e delimitare il perimetro delle aree di lavoro interessate alle attività a rischio di manutenzione e nuova realizzazione in modo da impedire l'accesso a tali aree a soggetti non autorizzati ai lavori;
- e) seguire, nella redazione, sottoscrizione ed esecuzione dei contratti, le regole di sicurezza che sono e saranno diffuse dalla Società;
- f) i Fornitori e gli altri Destinatari esterni alla Società, ove richiesto da norme e regolamenti, in base alla natura del bene e servizio prestato, devono dare evidenza del rispetto da parte loro delle normative sulla sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro;
- g) segnalare alle funzioni competenti eventuali inefficienze dei dispositivi di protezione individuali ovvero di altri presidi a tutela della sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro.
- h) attenersi nello sviluppo dei contenuti e nella diffusione degli stessi ai Codici di Condotta delle associazioni di categoria per la salvaguardia dei minori e la coerenza della pubblicità rispetto alla classificazione per età e per contenuto dei giochi.

- È, inoltre vietato:

- a) utilizzare, nello svolgimento della attività identificate a rischio macchinari, attrezzature, strumenti utensili, materiali e dispositivi di protezione individuali non adeguati e non conformi alle normative vigenti per le specifiche operazioni da svolgere;
- b) disattivare o rendere anche parzialmente inefficienti dispositivi individuali o collettivi di protezione;
- c) nell'ambito degli interventi e attività di cui si è incaricati, svolgere attività ed operazioni al di fuori delle aree specificatamente identificate per gli interventi richiesti;
- d) accedere ad aree di lavoro alle quali non si è autorizzati;
- e) per i fornitori, utilizzare macchinari e attrezzature, strumenti utensili, materiali e dispositivi di protezione individuali di proprietà della Società.

### **3.D - Principi per la predisposizione delle procedure per la prevenzione dei reati contro la personalità individuale ed i reati di omicidio colposo e lesioni colpose gravi e gravissime**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, e nell'ambito specifico della gestione della sicurezza sul lavoro e della tutela dell'igiene e salute sul lavoro, nel rispetto di quanto previsto ai sensi del D. Lgs. 81/2008 e sue successive modifiche ed integrazioni, sono previste specifiche procedure, in forza delle quali:

- a) vengano periodicamente individuati dalla Società in materia di sicurezza e tutela dell'igiene e salute sul lavoro, tenendo in adeguata considerazione: la struttura aziendale, la natura delle attività, l'ubicazione dei locali e delle aree di lavoro, l'organizzazione del personale, le specifiche sostanze, macchinari, attrezzature e impianti impiegati nelle attività e i relativi cicli di produzione;
- b) venga aggiornato, periodicamente ed in occasione di significative modifiche organizzative, il documento di valutazione dei rischi, redatto ai sensi del D. Lgs. 81/2008 e sue successive modifiche ed integrazioni;
- c) la Società, e le funzioni da essa delegate, nella valutazione dei rischi adottati criteri oggettivi, documentati e ripetibili, considerando, per ogni specifico rischio come sopra individuato, la

- probabilità di accadimento, la dimensione dell'impatto del danno possibile, i risultati di rilievi ambientali e la storia degli infortuni verificatisi nello svolgimento della specifica attività;
- d) vengano definiti e periodicamente aggiornati il piano di intervento delle azioni di prevenzione e protezione sulla base del risultato della valutazione dei rischi effettuata, nonché i programmi di informazione e formazione dei lavoratori ai fini della sicurezza e della protezione della loro salute;
  - e) la Società, e le funzioni da essa delegate, proponga e diffonda adeguate procedure volte alla tutela della sicurezza sul lavoro e alla tutela dell'igiene e salute sul lavoro nonché le indicazioni sulle adeguate misure di prevenzione e protezione da adottare, tenendo in adeguata considerazione quanto descritto nei punti precedenti e la normativa vigente in materia di sicurezza e tutela dell'igiene e salute sul lavoro;
  - f) i dirigenti e i preposti siano tenuti a sorvegliare sull'effettivo rispetto delle procedure proposte e diffuse ai sensi del D. Lgs. 81/2008 e sue successive modifiche ed integrazioni e sulla adozione delle adeguate misure di prevenzione e protezione, comunicando tempestivamente all'Organismo di Vigilanza eventuali eccezioni e criticità;
  - g) venga definito il metodo di individuazione, segnalazione e comportamento da tenere in caso di emergenze, sia per gli addetti alla gestione delle specifiche emergenze che per gli altri soggetti che possono esserne coinvolti;
  - h) i lavoratori in base agli specifici rischi individuati a cui sono soggetti ricevano adeguata informazione e formazione in merito alle misure di prevenzione e protezione da adottare nello svolgimento delle proprie attività e gestione delle emergenze, in base alla normativa vigente in materia di sicurezza e tutela dell'igiene e salute sul lavoro e delle procedure proposte e diffuse dal Servizio Prevenzione e Protezione;
  - i) non siano corrisposti compensi a Fornitori in misura non congrua rispetto alle prestazioni rese alla Società e/o comunque non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;
  - l) alle ispezioni giudiziarie e amministrative (es. relative al D. Lgs. 81/2008, ecc.) devono partecipare i soggetti a ciò espressamente delegati. L'Organismo di Vigilanza dovrà essere prontamente informato sull'inizio di ogni attività ispettiva, mediante apposita comunicazione interna, inviata a cura della direzione aziendale di volta in volta interessata. Di tutto il procedimento relativo all'ispezione devono essere redatti appositi verbali, che verranno conservati dall'Organismo di Vigilanza;
  - m) siano previsti obblighi di riporto periodico all'Organismo di Vigilanza per le valutazioni di competenza con riguardo a quanto previsto dal presente modello.

Inoltre

- n) vengano i contenuti dei videogiochi, preventivamente alla messa in commercio dei prodotti, sottoposti alla classificazione delle agenzie di Rating segnalando all'Organismo di Vigilanza i prodotti per i quali la classificazione ottenuta sia stata solo per un pubblico adulto (Pegi + 18 – Adults).

#### **4.D – Elenco delle procedure per la prevenzione dei reati contro la personalità individuale e omicidio colposo e lesioni colpose gravi e gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste le seguenti specifiche procedure:

- a) Codice Etico;
- b) Sign Off (H5 Gestione del Personale);
- c) Sign Off (H2 Acquisti non di materiali destinati alla rivendita);
- d) DVR magazzino;
- e) DVR sede amministrativa;
- f) Norme di comportamento da tenere nei locali della logistica DIGITAL BROS.

L'Organismo di Vigilanza cura che le procedure di cui al presente paragrafo siano idonee al rispetto delle prescrizioni in esso contenute e adeguate alle finalità in precedenza indicate.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

L'Organismo di Vigilanza vigila che nelle società appartenenti al Gruppo siano adottati principi e procedure coerenti con i principi e le procedure fatti propri dalla Società.

**PARTE SPECIALE**  
**SEZIONE “E”**  
**DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI**  
**(art. 24-bis del D. Lgs. 231/2001)**

La legge 18 marzo 2008, n. 48 ha ratificato ed eseguito la Convenzione di Budapest del 23 novembre 2001, promossa dal Consiglio d’Europa in tema di criminalità informatica, e riguardante, in particolare, i reati commessi avvalendosi in qualsiasi modo di un sistema informatico od in suo danno, ovvero che pongano in qualsiasi modo l’esigenza di raccogliere prove in forma informatica.

L’art. 7 della legge 48/2008 ha introdotto nel D.Lgs. 231/2001 l’art. 24-bis che prevede ulteriori forme di responsabilità delle persone giuridiche in dipendenza della commissione di numerosi reati informatici.

L’art. 24-bis prevede i seguenti reati, di seguito indicati.

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

La norma stabilisce che tutti i delitti relativi alla falsità in atti disciplinati dal Codice Penale (cfr. Capo III, Titolo VII, Libro II), tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un Documento Informatico, pubblico o privato, avente efficacia probatoria (in quanto rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti).

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

Tale reato si realizza quando un soggetto 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.

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

Tale reato si realizza quando un soggetto, 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.

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

Tale reato si realizza quando un soggetto, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l’interruzione, totale o parziale, o l’alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

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

Tale ipotesi di reato si configura qualora un soggetto fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione.

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

Il reato si configura quando un soggetto, 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.

**Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)** Il reato si configura quando un soggetto distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui. La pena è aumentata se il fatto è commesso con abuso della qualità di operatore del sistema.

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

Tale reato si realizza quando un soggetto commetta 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.

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

Questo reato si realizza quando un soggetto 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. La pena è aumentata se il fatto è commesso con abuso della qualità di operatore del sistema.

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

Questo reato si configura quando la condotta di cui al precedente art. 635-quater cod. pen. è diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è aumentata.

La pena è aumentata anche se il fatto è commesso con abuso della qualità di operatore del sistema.

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

Il reato si configura quando un soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

**Indebito utilizzo di carte di credito o di pagamento (art. 55 comma 9 D.Lgs 231/07)**

Tale reato si realizza quando un soggetto, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abilita al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

### **Trattamento illecito di dati (art. 167 D.Lgs 196/03)**

Tale ipotesi di reato si configura qualora un soggetto, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento, alla comunicazione o alla diffusione di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130 del D.Lgs. 196/03, ovvero in applicazione dell'articolo 129 del D.Lgs. 196/03.

Il reato si realizza anche nell'ipotesi in cui un soggetto, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45 del D.Lgs. 196/03.

**Falsità nelle dichiarazioni e notificazioni al Garante (art. 168 D.Lgs 196/03)** Questo reato si configura quando un soggetto, nella notificazione di cui all'articolo 37 del D.Lgs 196/03 o in comunicazioni, atti, e documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi.

### **Inosservanza dei provvedimenti del Garante (art. 170 D.Lgs 196/03)**

Tale ipotesi di reato si configura qualora un soggetto, pur essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2 (*Garanzia dati sensibili*), 90 (*Trattamento dei dati genetici*), 150, commi 1 e 2 (*Provvedimenti a seguito del ricorso*), e 143, comma 1, lettera c (*Procedimento per i reclami*) del D.Lgs 296/03.

### **Altre fattispecie (art. 171 D.Lgs 196/03)**

Tali reati si configurano nella violazione delle disposizioni di cui agli articoli 113, comma 1 (Raccolta di dati e pertinenza), e 114 (Controllo a distanza) del D.Lgs 196/03.

La prima violazione riguarda il datore di lavoro, per il quale è fatto divieto, sia ai fini dell'assunzione sia nel corso dello svolgimento del rapporto di lavoro nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, L'altro violazione riguarda l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori nel rispetto di quanto disposto all'art. 4 della legge 20 maggio 1970, n. 300.

In relazione alla commissione di tali reati, sono previste sia sanzioni pecuniarie e che sanzioni interdittive.

Si precisa in ogni caso che la commissione di uno dei Delitti Informatici sopra descritti assume rilevanza, per le finalità di cui al Decreto, solo qualora la condotta, indipendentemente dalla natura aziendale o meno del dato/informazioni/programma/sistema informatico o telematico, possa determinare un interesse o vantaggio per la Società.

Pertanto, nell'ambito della descrizione delle singole fattispecie criminose, si è tenuto conto di tale rilevante aspetto per l'elaborazione dei casi pratici proposti.

### **Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 105/2019)**

Tale fattispecie si applica a chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b) (censimento reti, sistemi informativi e servizi informatici comprensivo di architettura e componentistica), o al comma 6, lettera a) del D.L. 105/2019 (affidamento forniture di beni e di servizi ICT e relativi test), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c) del decreto (attuati dalla presidenza del Consiglio dei Ministri o dal Ministero dello Sviluppo Economico), 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) del decreto (reti, sistemi informativi e servizi informatici), o ai fini delle comunicazioni di cui al comma 6, lettera a) del decreto, o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) del decreto od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto.

Si applica la sanzione pecuniaria sino a 400 quote.

### **1.E Potenziali aree di rischio**

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio per le attività della Digital Bros risultano essere, ai fini della presente Parte Speciale “E” del Modello, le seguenti:

- a) tutte le attività aziendali svolte dai Destinatari tramite l'utilizzo dei Sistemi Informativi aziendali, del servizio di posta elettronica e dell'accesso ad Internet;
- b) gestione dei Sistemi Informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT nonché la Sicurezza Informatica;

### **2.E Principi di comportamento e controllo nelle principali aree a rischio.**

Obiettivo della presente Parte Speciale è che i Destinatari si attengano – nella misura in cui gli stessi siano coinvolti nello svolgimento delle attività rientranti nelle aree a rischio e in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti di Digital Bros a regole di condotta conformi a quanto prescritto nella stessa al fine di prevenire e impedire il verificarsi dei Delitti Informatici.

Tutte le attività, nell'ambito delle categorie di operazioni a rischio devono essere svolte in conformità delle leggi, procedure e regolamenti vigenti, al Modello, al Codice di Autodisciplina ed ai valori e alle politiche e regole della Digital Bros.

I seguenti principi si applicano nell'ambito della Digital Bros a tutti i Destinatari del presente Modello.

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24 bis del D. Lgs. 231/2001); sono altresì proibite le violazioni ai principi ed alle procedure aziendali.

Fermo restando quanto sopra, per tutti gli amministratori, sindaci e Dipendenti della Digital Bros e delle società del gruppo:

- i. è vietato connettere ai sistemi informatici di Digital Bros, personal computer, periferiche, altre apparecchiature o installare software senza preventiva autorizzazione del soggetto aziendale responsabile individuato;
- ii. è vietato in qualunque modo modificare la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;
- iii. è vietato acquisire, possedere o utilizzare strumenti software e/o hardware – se non per casi debitamente autorizzati ovvero in ipotesi in cui tali software e/o hardware siano utilizzati per il monitoraggio della sicurezza dei sistemi informativi aziendali – che potrebbero essere adoperati abusivamente per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le credenziali, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);
- iv. è vietato ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate da Digital Bros;
- v. è vietato divulgare, cedere o condividere con personale interno o esterno a Digital Bros le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- vi. è vietato accedere abusivamente ad un sistema informatico altrui – ovvero nella disponibilità di altri Dipendenti o terzi – nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;
- vii. è vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- viii. è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;

- ix. è vietato comunicare a persone non autorizzate, interne o esterne a Digital Bros, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
- x. è proibito mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti Virus o altri programmi in grado di danneggiare o intercettare dati;
- xi. è vietato lo Spamming come pure ogni azione di risposta al medesimo;
- xii. è vietato inviare attraverso un sistema informatico aziendale qualsiasi informazione o dato, previa alterazione o falsificazione dei medesimi.

### **3.E - Principi per la predisposizione delle procedure per la prevenzione dei delitti informatici e trattamento illecito di dati**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, e nell'ambito specifico della gestione delle reti e della tutela dei dati, nel rispetto di quanto previsto dalle normative specifiche, sono previste particolari procedure, in forza delle quali sono definite regole, procedure ed istruzioni operative adottate da Digital Bros in tema di Sicurezza Informatica che riguardino, a titolo esemplificativo:

- (i) uso accettabile delle risorse informatiche;
- (ii) controllo degli accessi logici alle risorse informatiche;
- (iii) gestione degli incidenti di sicurezza delle informazioni e reazione ai medesimi;
- (iv) sicurezza della rete e delle comunicazioni.
- (v) governo della sicurezza delle informazioni (relativo ad esempio, alla determinazione dei piani di sicurezza dei sistemi informativi, alla segnalazione e la risposta agli incidenti di sicurezza delle informazioni, alla formazione e sensibilizzazione per la sicurezza delle informazioni, etc.);
- (vi) controlli di sicurezza specifici per tipologia di asset informativo (relativi ad esempio alla selezione di contromisure per piattaforme e sistemi, applicazione, database, etc.);
- (vii) controlli di sicurezza indipendenti dalla tipologia di asset, volti ad indirizzare i comportamenti e le azioni operative degli esponenti aziendali (ad esempio in relazione all'uso accettabile delle risorse informative, alla gestione dei diritti di accesso alle risorse, alla tracciabilità degli eventi, etc.).

Al fine di garantire adeguati presidi nell'ambito delle singole aree a rischio, si prevedono qui di seguito le regole che devono essere rispettate da Digital Bros, dagli esponenti aziendali nonché dagli altri soggetti eventualmente autorizzati nell'ambito delle suddette aree, fermo restando che l'attuazione delle stesse è contenuta nelle policy, procedure aziendali e documenti organizzativi.

In particolare:

- (a) informare adeguatamente i Dipendenti, nonché gli stagisti e gli altri soggetti come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei sistemi informativi, dell'importanza di mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi;
- (b) prevedere attività di formazione e addestramento periodico in favore dei Dipendenti, diversificate in ragione delle rispettive mansioni, nonché, in misura ridotta, in favore degli stagisti e degli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;
- (c) far sottoscrivere ai Dipendenti, nonché agli stagisti e agli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei sistemi informativi, uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo e tutela delle risorse informatiche aziendali;
- (d) informare i Dipendenti, nonché gli stagisti e gli altri soggetti – come ad esempio i collaboratori esterni – eventualmente autorizzati all'utilizzo dei sistemi informativi, della necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;
- (e) impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
- (f) limitare gli accessi alle stanze server unicamente al personale autorizzato;

- (g) proteggere, per quanto possibile, ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;
- (h) dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
- (i) impedire l'installazione e l'utilizzo di software non approvati da Digital Bros e non correlati con l'attività professionale espletata per la stessa;
- (j) limitare l'accesso alle aree ed ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di Virus capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti e, in ogni caso, implementare – in presenza di accordi sindacali – presidi volti ad individuare eventuali accessi o sessioni anomale, previa individuazione degli “indici di anomalia” e predisposizione di flussi informativi tra le Funzioni competenti nel caso in cui vengano riscontrate le suddette anomalie;
- (k) impedire l'installazione e l'utilizzo, sui sistemi informatici di Digital Bros, di software Peer to Peer mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di file (quali filmati, documenti, canzoni, Virus, etc.) senza alcuna possibilità di controllo da parte di Digital Bros;
- (l) qualora per la connessione alla rete Internet si utilizzino collegamenti wireless, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni a Digital Bros, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai Dipendenti;
- (m) prevedere un procedimento di autenticazione mediante l'utilizzo di credenziali al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei Dipendenti, degli stagisti e degli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi;
- (n) limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Dipendenti, degli stagisti e degli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi;
- (o) monitorare centralmente in tempo reale i sistemi anti-intrusione e di controllo degli accessi ai siti aziendali e gestire le autorizzazioni;
- (p) gestire il processo di identificazione ed autorizzazione all'accesso alle risorse ICT aziendali;
- (q) gestire i processi/procedure di escalation interne ed esterne in occasione di situazioni di emergenza e/o crisi, con il supporto delle Direzioni/Funzioni responsabili interessate;
- (r) svolgere analisi di vulnerabilità;
- (s) produrre report a supporto del vertice aziendale;
- (t) sovrintendere ai sistemi di protezione attiva e passiva delle risorse umane e materiali di Digital Bros

#### **4.E – Elenco delle procedure per la prevenzione dei delitti informatici e trattamento illecito di dati**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste le seguenti specifiche procedure:

a) Codice Etico

b) Policy Gruppo Digital Bros per l'utilizzo dei Sistemi ICT.

L'Organismo di Vigilanza cura che le procedure di cui al presente paragrafo siano idonee al rispetto delle prescrizioni in esso contenute e adeguate alle finalità in precedenza indicate.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

L'Organismo di Vigilanza vigila che nelle società appartenenti al Gruppo siano adottati principi e procedure coerenti con i principi e le procedure fatti propri dalla Società.

## PARTE SPECIALE

### SEZIONE "F"

#### **DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO E DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE**

**(artt. 25-bis.1 e 25-novies del D. Lgs. 231/2001)**

Nella normativa introdotta con la Legge n. 99/09 del 23 luglio 2009 "Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia" che introduce (art. 15, co. 7) nel D.Lgs. 231/01 l'articolo 25-bis.1 "Delitti contro l'industria e il commercio" e 25-novies "Delitti in materia di violazione del diritto d'autore", si prevedono due importanti strumenti di contrasto al fenomeno della contraffazione di marchi e brevetti industriali: la confisca obbligatoria (anche per equivalente) e l'applicabilità della responsabilità amministrativa degli enti anche a tale categoria di delitti.

Si riportano di seguito una breve descrizione dei principali reati di cui alla presente Sezione F:

#### **Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali (Art. 473 c.p.)**

Chiunque contraffaccia o altera i marchi o segni distintivi, nazionali o esteri, delle opere dell'ingegno o dei prodotti industriali, ovvero, senza essere concorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati, è punito con la reclusione fino a tre anni e con la multa fino a euro 2.065.

Alla stessa pena soggiace chi contraffaccia o altera brevetti, disegni o modelli industriali, nazionali o esteri, ovvero, senza essere concorso nella contraffazione o alterazione, fa uso di tali brevetti, disegni o modelli contraffatti o alterati.

Le disposizioni precedenti si applicano sempre che siano state osservate le norme delle leggi interne o delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale.

#### **Introduzione nello Stato e commercio di prodotti con segni falsi (Art. 474 c.p.)**

Chiunque, fuori dei casi di concorso nei delitti preveduti dall'articolo precedente, introduce nel territorio dello Stato per farne commercio, detiene per vendere, o pone in vendita, o mette altrimenti in circolazione opere dell'ingegno o prodotti industriali, con marchi o segni distintivi, nazionali o esteri, contraffatti o alterati, è punito con la reclusione fino a due anni e con la multa fino a euro 2.065. Si applica la disposizione dell'ultimo capoverso dell'articolo precedente.

#### **Turbata libertà dell'industria o del commercio (Art. 513 c.p.)**

Chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio è punito, a querela della persona offesa, se il fatto non costituisce un più grave reato, con la reclusione fino a due anni e con la multa da euro 103 a euro 1.032.

#### **Illecita concorrenza con minaccia o violenza (Art. 513-bis. c.p.)**

Chiunque nell'esercizio di un'attività commerciale, industriale o comunque produttiva, compie atti di concorrenza con violenza o minaccia è punito con la reclusione da due a sei anni. La pena è aumentata se gli atti di concorrenza riguardano un'attività finanziaria in tutto o in parte ed in qualsiasi modo dallo Stato o da altri enti pubblici.

#### **Frodi contro le industrie nazionali (Art. 514)**

Chiunque, ponendo in vendita o mettendo altrimenti in circolazione, sui mercati nazionali o esteri, prodotti industriali, con nomi, marchi o segni distintivi contraffatti o alterati, cagiona un nocumento all'industria nazionale è punito con la reclusione da uno a cinque anni e con la multa non inferiore a euro 516.

Se per i marchi o segni distintivi sono state osservate le norme delle leggi interne o delle convenzioni internazionali sulla tutela della proprietà industriale, la pena è aumentata e non si applicano le disposizioni degli articoli 473 e 474.

### **Frode nell'esercizio del commercio (Art. 515 c.p.)**

Chiunque, nell'esercizio di un'attività commerciale, ovvero in uno spaccio aperto al pubblico, consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita, è punito, qualora il fatto non costituisca un più grave delitto, con la reclusione fino a due anni o con la multa fino a euro 2.065. Se si tratta di oggetti preziosi, la pena è della reclusione fino a tre anni o della multa non inferiore a euro 103.

### **Vendita di sostanze alimentari non genuine come genuine (Art. 516 c.p.)**

Chiunque pone in vendita o mette altrimenti in commercio come genuine sostanze alimentari non genuine è punito con la reclusione fino a sei mesi o con la multa fino a euro 1.032.

### **Vendita di prodotti industriali con segni mendaci (Art. 517 c.p.)**

Chiunque pone in vendita o mette altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto, è punito, se il fatto non è previsto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa fino a ventimila euro.

### **Art. 171 comma 1 lettera a –bis) e c) Legge 22 aprile 1941 n. 633**

Salvo quanto disposto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;

c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;

1-bis. Chiunque commette la violazione di cui al primo comma, lettera a-bis), è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato. La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore. La violazione delle disposizioni di cui al terzo ed al quarto comma dell'articolo 68 comporta la sospensione della attività di fotocopia, xerocopia o analogo sistema di riproduzione da sei mesi ad un anno nonché la sanzione amministrativa pecuniaria da euro 1.032 a euro 5.164.

### **Art. 171-bis Legge 22 aprile 1941 n. 633**

1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

### **Art. 171-ter Legge 22 aprile 1941 n. 633**

1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro:

a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;

b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;

c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);

d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;

f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto.

f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102 quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

2. È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 chiunque:

a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;

a-bis) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;

b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;

c) promuove o organizza le attività illecite di cui al comma 1.

3. La pena è diminuita se il fatto è di particolare tenuità.

4. La condanna per uno dei reati previsti nel comma 1 comporta:

- a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;
- b) la pubblicazione della sentenza in uno o più quotidiani, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;
- c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici.

#### **Art. 171-septies Legge 22 aprile 1941 n. 633**

1. La pena di cui all'articolo 171-ter, comma 1, si applica anche:

- a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;
- b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.

#### **Art. 171-octies Legge 22 aprile 1941 n. 633**

1. Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

2. La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

#### **1.F. Potenziali aree a rischio**

In considerazione della tipologia di attività svolta da Digital Bros, è astrattamente ipotizzabile la commissione dei seguenti reati:

art. 513 “Turbata libertà dell'industria o del commercio”: violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio;

art. 515 “Frode nell'esercizio del commercio”: nell'esercizio di un'attività commerciale, ovvero in uno spaccio aperto al pubblico, consegna all'acquirente di una cosa mobile per un'altra, ovvero di una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita;

art. 517 “Vendita di prodotti industriali con segni mendaci”: vendita o distribuzione di opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto;

art. 517-ter “Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale”: fabbricazione o messa in opera industrialmente di oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso potendo conoscere dell'esistenza del titolo di proprietà industriale, o altresì, al fine di trarne profitto, introduzione nel territorio dello Stato, detenzione per la vendita, vendita con offerta diretta ai consumatori o messa comunque in circolazione di beni di cui sopra;

art. 171, l. 633/1941 comma 1 lett a) bis: 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 3: 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-bis l. 633/1941 comma 1: abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in

locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori;

art. 171-bis l. 633/1941 comma 2: 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-ter l. 633/1941: 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-septies l. 633/1941: mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione;

art. 171-octies 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.

## **2. F- Principi di comportamento e controllo nelle principali aree a rischio**

Obiettivo della presente Parte Speciale è che i Destinatari si attengano – nella misura in cui gli stessi siano coinvolti nello svolgimento delle attività rientranti nelle aree a rischio e in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti di Digital Bros a regole di condotta conformi a quanto prescritto nella stessa al fine di prevenire e impedire il verificarsi dei Delitti contro l'industria e il commercio e Delitti in materia di violazione del diritto d'autore.

Tutte le attività, nell'ambito delle categorie di operazioni a rischio devono essere svolte in conformità delle leggi, procedure e regolamenti vigenti, al Modello, al Codice di Autodisciplina ed ai valori e alle politiche e regole della Digital Bros.

I seguenti principi si applicano nell'ambito della Digital Bros a tutti i Destinatari del presente Modello.

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate; sono altresì proibite le violazioni ai principi ed alle procedure aziendali.

Fermo restando quanto sopra, per tutti gli amministratori, sindaci e Dipendenti della Digital Bros e delle società del gruppo è fatto divieto di:

- 1) contraffare e/o alterare segni distintivi altrui o comunque utilizzare segni distintivi, marchi altrui senza averne acquisito la titolarità;
- 2) commercializzare prodotti con segni falsi, contraffatti o comunque derivati da segni distintivi altrui tale da determinarne la confusione sull'origine, la provenienza o la qualità;
- 3) raggiungere intese e/o accordi con terze parti tali da poter turbare l'esercizio del libero commercio e del mercato;
- 4) effettuare attività tali da poter essere configurate quali attività di concorrenza mediante l'utilizzo di minacce o violenze anche di carattere psicologico;
- 5) effettuare la commercializzazione di prodotti con qualità, provenienza diversa da quella dichiarata;
- 6) duplicare, distribuire e/o vendere o comunque detenere a scopo commerciale programmi contenuti in supporti non contrassegnati dalla SIAE e/o comunque tutelati dal diritto d'autore;
- 7) riprodurre, copiare, presentare al pubblico i contenuti delle banche dati o comunque ne violi, o favorisca la violazione da parte di terzi, della segretezza;

- 8) contraffare i contrassegni della SIAE al fine di porre in commercio prodotti per i quali tale contrassegno è prescritto;
- 9) installare e/o commercializzare e/o sviluppare sistemi di decodificazione che consentono l'accesso a sistemi di pagamento senza dar corso al pagamento del canone dovuto;
- 10) alterare le informazioni elettroniche;
- 11) omettere le dovute comunicazioni alla SIAE anche in merito ai supporti non soggetti al contrassegno
- 12) Riprodurre, vendere, importare, promuovere, installare e qualsiasi utilizzo (pubblico o privato) di apparati, o parte di essi, atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo in qualsiasi forma.

### **3.F - Principi per la predisposizione delle procedure per la prevenzione dei delitti di cui alla presente sezione.**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, e nell'ambito specifico della gestione dei contenuti e delle opere dell'ingegno e delle attività commerciali in genere, nel rispetto di quanto previsto dalle normative specifiche, sono previste particolari procedure, in forza delle quali sono definite regole, procedure ed istruzioni operative adottate da Digital Bros, a titolo esemplificativo:

- (i) controllo dei contenuti utilizzati nello sviluppo dei videogiochi e contrattualizzazione dell'acquisizione di essi;
- (ii) gestione delle comunicazioni e informative a SIAE mediante funzione dedicata e preventiva alla commercializzazione dei prodotti;
- (iii) coinvolgimento della funzione legale per ogni eventuale comunicazione relativa a potenziale violazione delle normative in materia di diritto d'autore;
- (iv) standardizzazione delle proposte commerciali e clausole contrattuali di manleva da parte dei fornitori di licenze e/o segni distintivi e/o contenuti;
- (v) verifica preliminare nell'utilizzo di marchi e/o nomi per i prodotti commercializzati.

### **4.F – Elenco delle procedure per la prevenzione dei delitti contro l'industria e il commercio e delitti in materia di violazione del diritto d'autore**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste le seguenti specifiche procedure:

- a) Codice Etico;
- b) Sistema ERP;
- c) Sign Off (H6 Acquisti di materiali destinati alla rivendita);
- d) Sign Off (H2 Acquisti non di materiali destinati alla rivendita);
- e) Policy Gruppo Digital Bros per l'utilizzo dei Sistemi ICT.

Al fine di garantire adeguati presidi nell'ambito delle singole aree a rischio l'Organismo di Vigilanza cura che le procedure in essere siano idonee al rispetto delle prescrizioni in esso contenute e adeguate alle finalità indicate.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

## PARTE SPECIALE

### SEZIONE "G"

**DELITTI AVENTI FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO PREVISTI DAL CODICE PENALE E DALLE LEGGI SPECIALI E DELITTI POSTI IN ESSERE IN VIOLAZIONE DI QUANTO PREVISTO DALL'ARTICOLO 2 DELLA CONVENZIONE INTERNAZIONALE PER LA REPRESSIONE DEL FINANZIAMENTO DEL TERRORISMO FATTA A NEW YORK IL 9.12.1999**

**(art. 25-quater del D. Lgs. 231/2001)**

La presente Parte Speciale, con riferimento ai reati previsti dall'art. 25-quater del Decreto 231 (di seguito anche i "Reati in materia di terrorismo o di eversione dell'ordine democratico"), illustra i comportamenti che devono essere tenuti dai Destinatari del Modello che operano nelle relative aree a rischio.

L'art. 25-quater del Decreto 231 è stato introdotto nell'ambito della responsabilità amministrativa delle associazioni, delle persone giuridiche e degli enti anche privi di personalità giuridica dall'art. 3 della legge n. 7/2003 di ratifica ed esecuzione della "Convenzione internazionale per la repressione del finanziamento del terrorismo" stipulata a New York il 9 dicembre 1999 (per semplicità, la Convenzione), ed è volto a sanzionare l'ente in caso di commissione di delitti con finalità di terrorismo o di eversione dell'ordine democratico qualora commessi nell'interesse o a vantaggio dell'ente stesso.

Come da indicazioni fornite dalla stessa Convenzione in merito agli elementi costitutivi della nozione, penalmente rilevante, di "atto terroristico" (o eversivo), è da ricomprendersi come tale ogni atto:

- diretto contro la vita o l'incolumità di civili o – in contesti bellici – contro ogni altra persona che non prenda parte attiva alle ostilità in una situazione di conflitto armato;
- finalizzato a diffondere il terrore o procurare danni fra la popolazione civile, ingenerando un diffuso stato d'intimidazione e di insicurezza suscettibile di essere percepita a livello collettivo, o ancora a costringere uno Stato o un'organizzazione internazionale a compiere od omettere un atto;
- animato da motivazioni di natura politica, religiosa e/o ideologica.

Anche in ossequio al principio di legalità, possono rientrare nell'ambito della Convenzione in oggetto solo gli atti e le condotte che sono puniti da norme espressamente dirette alla repressione dei fenomeni terroristici e/o eversivi.

Le principali caratteristiche correlate ai contenuti dell'art. 25-quater del Decreto 231, che in parte lo distinguono, nelle logiche, dai contenuti degli articoli relativi alle altre fattispecie di reato previste e sanzionate dal Decreto 231, sono le seguenti:

- l'articolo contiene un riferimento "aperto" e, come tale, non tipizzato né tipizzabile alle fattispecie di reato che costituiscono il c.d. "reato-presupposto" per la configurabilità della responsabilità dell'ente. Nel testo non è incluso un elenco dettagliato dei reati per i quali è prevista la responsabilità dell'ente, ma ci si limita a richiamare, al primo comma, i delitti previsti dal codice penale e dalle leggi speciali ed, al terzo comma, i delitti diversi da quelli disciplinati al comma 1 ma posti in essere in violazione di quanto stabilito dall'art. 2 della Convenzione;
- per diretta conseguenza, le sanzioni eventualmente inflitte all'ente sono determinate in misura variabile e condizionata all'individuazione della singola fattispecie di reato costituente il presupposto per l'imputabilità in capo all'ente dei reati di cui all'art. 25-quater.

Si ritiene, pertanto, opportuno elencare le diverse fattispecie di reato che possono portare ad ipotesi di responsabilità da parte dell'ente, distinguendole sulla base delle differenti fonti normative citate.

A margine delle singole fattispecie, ove ritenuto anche solo astrattamente ipotizzabile, sono stati riportati possibili esempi di realizzazione del reato; tuttavia, per dovere di completezza, sono state riportate anche fattispecie che – in linea teorica ed astratta – più difficilmente potranno essere ricondotte ad ipotesi di responsabilità diretta dell'ente.

Si riporta di seguito una breve descrizione dei reati contenuti nell'art. 25-quater del Decreto 231 e ritenuti astrattamente ipotizzabili per la Società, oltre a una breve esposizione delle principali possibili modalità di attuazione dei suddetti reati.

### **Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (Art. 270 bis c.p.)**

“Chiunque promuove, costituisce, organizza o dirige associazioni che si propongono il compito di atti di violenza con fini di eversione dell'ordine democratico è punito con la reclusione da sette a quindici anni. Chiunque partecipa a tali associazioni è punito con la reclusione da quattro a otto anni”.

Tale ipotesi di reato si configura nei confronti di chiunque promuova, costituisca, organizzi, diriga o finanzi associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico. Ai fini della legge penale, la finalità di terrorismo ricorre anche quando gli atti di violenza siano rivolti contro uno Stato estero, un'istituzione e un organismo internazionale. Ai fini che qui rilevano, l'imputabilità dell'ente potrebbe essere ravvisata – a titolo di mero esempio - in caso di finanziamento diretto erogato consapevolmente dalla Società ad un'organizzazione terroristica, in cambio di favori, protezione del personale in zone considerate a “rischio terrorismo” o lavori su commessa.

### **Assistenza agli associati (art. 270-ter c.p.)**

Chiunque, fuori dei casi di concorso nel reato o di favoreggiamento, dà rifugio o fornisce vitto, ospitalità, mezzi di trasporto, strumenti di comunicazione a taluna delle persone che partecipano alle associazioni indicate negli articoli 270 e 270-bis c.p. è punito con la reclusione fino a quattro anni. La pena è aumentata se l'assistenza è prestata continuativamente. Non è punibile chi commette il fatto in favore di un prossimo congiunto.

Tale ipotesi di reato si configura nei confronti di chiunque, fuori dei casi di concorso nel reato o di favoreggiamento, dia rifugio o fornisca vitto, ospitalità, mezzi di trasporto, strumenti di comunicazione a taluna delle persone che partecipano alle associazioni indicate negli articoli 270 e 270-bis del codice penale. Non è punibile chi commette il fatto in favore di un prossimo congiunto. Ai fini del Decreto 231, si potrebbe rinvenire l'imputabilità dell'ente nel caso in cui venga consapevolmente offerto un supporto a membri di un'organizzazione terroristica, quale fornitura di mezzi di trasporto, comunicazione, ecc. anche in cambio di protezione per il personale e/o fornitura di personale a basso costo

### **Condotte con finalità di terrorismo (Art. 270 sexies c.p.)**

“Sono considerate con finalità di terrorismo le condotte che, per la loro natura o contesto, possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia”.

Si configurano come attuate con finalità di terrorismo le condotte che, per la loro natura o contesto, possano arrecare grave danno ad un Paese o ad un'organizzazione internazionale e siano compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture pubbliche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia. La lettera dell'articolo in esame è stata chiaramente concepita quale formula c.d. “di chiusura” volta a ricomprendere l'intero panorama delle condotte che, ancorché non tipizzate, sono comunque realizzate per finalità di terrorismo e, in senso più ampio, di eversione e destabilizzazione dell'ordine costituito.

Gli altri reati previsti dall'art. 25-quater del Decreto 231 non sono, allo stato attuale, valutati come rilevanti in quanto la probabilità di commissione di tali reati è stata ritenuta remota. La Società si riserva di aggiornare il presente Modello nel caso in cui dovesse emergere la rilevanza di uno o più dei suddetti reati di seguito elencati:

associazioni sovversive (art. 270 c.p.);

addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-quinquies c.p.);

arruolamento con finalità di terrorismo anche internazionale (art. 270-quater c.p.);

attentato per finalità terroristiche o di eversione (art. 280 c.p.);

sequestro di persona a scopo di terrorismo o di eversione (art. 289 c.p.);

istigazione a commettere uno dei delitti contro la personalità dello Stato (art. 302 c.p.);  
cospirazione politica mediante accordo e cospirazione politica mediante associazione (artt. 304 e 305 c.p.).  
banda armata, formazione e partecipazione; assistenza ai partecipi di cospirazione o di banda armata (artt. 306 e 307 c.p.).

L'art. 25-quater del Decreto 231 contiene un espresso riferimento altresì alle Leggi speciali che, unitamente alle fattispecie espressamente disciplinate dal codice penale, possono comportare un coinvolgimento della Società in fatti di terrorismo o eversione dell'ordine democratico. Nel dettaglio, le leggi speciali suscettibili di attenzione sono le seguenti:

L. 6 febbraio 1980, n. 15 (conversione in legge, con modificazioni, del decreto-legge 15 dicembre 1979, n. 625, concernente misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica);

L. 10 maggio 1976, n. 342 (repressione dei delitti contro la sicurezza della navigazione aerea);

L. 28 dicembre 1989, n. 422 (reati diretti contro la sicurezza della navigazione marittima e dei reati diretti contro la sicurezza delle installazioni fisse sulla piattaforma intercontinentale).

I reati rientranti nell'ambito di applicazione della Convenzione sono quelli diretti a fornire, direttamente o indirettamente, ma comunque volontariamente, fondi a favore di soggetti che intendano porre in essere reati di terrorismo. In particolare, la Convenzione rinvia ai reati previsti da altre convenzioni internazionali, tra i quali: il dirottamento di aeromobili, gli attentati contro personale diplomatico, il sequestro di ostaggi, l'illecita realizzazione di ordigni nucleari, i dirottamenti di navi, l'esplosione di ordigni, ecc.

Ai sensi dell'art. 2, espressamente richiamato dall'art. 25-quater del Decreto 231, commette un reato chiunque con qualsiasi mezzo, direttamente o indirettamente, illegalmente e intenzionalmente, fornisca o raccolga fondi con l'intento di utilizzarli o sapendo che sono destinati ad essere utilizzati, integralmente o parzialmente, al fine di compiere: (i) un atto che costituisca reato ai sensi di e come definito in uno dei trattati elencati nell'allegato della Convenzione, ovvero (ii) qualsiasi altro atto diretto a causare la morte o gravi lesioni fisiche ad un civile, o a qualsiasi altra persona che non abbia parte attiva in situazioni di conflitto armato, quando la finalità di tale atto sia quella di intimidire una popolazione, o di obbligare un governo o un'organizzazione internazionale a compiere o ad astenersi dal compiere qualcosa.

Perché un atto possa comportare una delle suddette fattispecie non è necessario che i fondi siano effettivamente utilizzati per compiere quanto descritto ai punti (i) e (ii).

Commette ugualmente reato chiunque tenti di commettere i reati sopra previsti.

Commette altresì un reato chiunque:

- a) prenda parte in qualità di complice al compimento di un reato di cui sopra;
- b) organizzi o diriga altre persone al fine di commettere un reato di cui sopra;
- c) contribuisca al compimento di uno o più reati di cui sopra con un gruppo di persone che agiscono con una finalità comune. Tale contributo deve essere intenzionale e:
  - i. deve essere compiuto al fine di facilitare l'attività o la finalità criminale del gruppo, laddove tale attività o finalità implicino la commissione del reato; o
  - ii. deve essere fornito con la piena consapevolezza che l'intento del gruppo è di compiere un reato.

Le disposizioni del codice penale, le Leggi speciali e l'art. 2 della Convenzione presentano, nella definizione delle fattispecie sopra riportate, un significativo tratto comune, fondamentale per l'effettiva imputabilità diretta alla Società dei reati di cui all'art. 25-quater.

In particolare, l'elemento soggettivo dei reati presupposto risulta essere sempre e comunque il dolo, generico o specifico, a seconda delle differenti ipotesi delittuose.

Pertanto, perché si realizzino le fattispecie descritte, è necessario che il soggetto agente abbia coscienza dell'evento antigiusuridico e lo voglia realizzare attraverso una condotta a lui attribuibile; affinché si possano configurare le fattispecie di reato in esame, dunque, è necessario che:

- il soggetto agente sia consapevole di concedere supporto e/o finanziamento ad organizzazioni terroristiche (eversive),
- che abbia intenzione di favorirne, promuovere e/o supportarne l'attività,
- abbia coscienza del carattere terroristico dell'attività che verrà realizzata grazie alla sua condotta.

Peraltro, sarebbe altresì configurabile il perfezionamento della fattispecie criminosa, qualora il soggetto agisca a titolo di dolo eventuale. In tal caso, l'agente dovrebbe prevedere ed accettare il rischio del verificarsi dell'evento,

pur non volendolo direttamente. La previsione del rischio del verificarsi dell'evento e la determinazione volontaria nell'adottare la condotta criminosa devono comunque desumersi da elementi univoci e obiettivi.

Si ricorda che, a differenza di quanto previsto dalle altre disposizioni contenute nel Decreto 231, in relazione ai delitti aventi finalità di terrorismo o di eversione dell'ordine democratico la norma opera un rinvio generale "aperto" a tutte le ipotesi – attuali e future – di reati terroristici ed eversivi, mediante un richiamo agli articoli del codice penale, alle Leggi speciali in materia, nonché all'art. 2 della Convenzione per la repressione del finanziamento del terrorismo che prevede la punibilità di "chiunque, con qualsiasi mezzo, direttamente o indirettamente, illegalmente ed intenzionalmente, fornisca o raccolga fondi con l'intento di utilizzarli, anche solo parzialmente, al fine di compiere atti sinteticamente qualificabili come di natura terroristica".

Ai sensi di quanto previsto dall'art. 25-quater del Decreto 231, in relazione alla commissione dei delitti aventi finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle Leggi speciali o posti in essere in violazione dell'art. 2 della Convenzione per la repressione del finanziamento del terrorismo, da parte dei soggetti apicali e/o dei soggetti sottoposti, qualora dagli stessi derivi all'ente un interesse o un vantaggio, si applicano alla Società le seguenti sanzioni:

- a) sanzioni pecuniarie
  - i. se il delitto è punito con la pena della reclusione inferiore a dieci anni, da duecento a settecento quote;
  - ii. se il delitto è punito con la pena della reclusione non inferiore a dieci anni o con l'ergastolo, da quattrocento a mille quote;
- b) sanzioni interdittive
  - i. nei casi di condanna, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2 del Decreto 231/01, per una durata non inferiore ad un anno;
  - ii. se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei suddetti delitti, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'articolo 16, comma 3 del Decreto 231.

Alle sanzioni sopraccitate vanno in ogni caso considerate le ulteriori forme di sanzione per gli illeciti amministrativi dipendenti da reato previste dalla normativa di riferimento:

- la confisca del prezzo o del profitto del reato, sempre disposta con la sentenza di condanna, salvo che per la parte che può essere restituita al danneggiato;
- la pubblicazione della sentenza di condanna (una sola volta, per estratto o per intero, in uno o più giornali indicati dal giudice nella sentenza nonché mediante affissione nel comune ove l'ente ha la sede principale), che può essere disposta quando nei confronti dell'ente viene applicata una sanzione interdittiva.

### **1.G – Potenziali aree a rischio**

In considerazione delle attività svolte da Digital Bros e della struttura interna adottata sono individuate nelle funzioni gestione acquisti servizi e beni, gestione personale, amministrazione, contabilità e bilancio, tesoreria.

### **2.G – Principi di comportamento e controllo nelle principali aree a rischio**

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.), i soggetti aziendali coinvolti nell'area a rischio "gestione acquisti di beni e servizi" sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all'art. 25-quater del Decreto 231, al rispetto delle regole e procedure aziendali emesse a regolamentazione di tale area a rischio. Tali regole e procedure prevedono controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio, tra i quali, ad esempio:

un processo di selezione basata su una procedura di ricerca e selezione dei nuovi potenziali fornitori, nella quale sono definiti i parametri di valutazione, l'esigenza e le certificazioni richieste al fornitore;

l'accettazione formale del fornitore da parte del responsabile di funzione in caso di termini di pagamento richiesti differenti dagli standard;

la previsione di un processo strutturato di qualifica dei fornitori;

in caso di trasportatori, un processo di selezione basato sulla contrattazione periodica delle tariffe di trasporto, in sede di riunioni coi principali players, al termine delle quali vengono accettate e sottoscritte le condizioni di trasporto pattuite;

in caso di consulenti, un processo di selezione comparativo fra almeno tre differenti soggetti, guidato da parametri qualitativi e quantitativi di volta in volta definiti e valutati tramite la presa visione di differenti preventivi richiesti;

in caso di fornitori e servizi di consulenza “creativi”, un processo di selezione basato sull’emissione di un bando di gara per importi superiori alla soglia definita e l’invio ad ogni potenziale nuovo fornitore di un brief con indicazione delle specifiche di progetto;

la regolazione dei rapporti coi fornitori di servizi (comprese le agenzie di public relations e di comunicazione) tramite sottoscrizione di contratti autorizzati da soggetti dotati di idonea procura o dal rappresentante legale della Società ed all’interno dei quali sono definiti i compensi per il servizio reso e le modalità di corresponsione del compenso;

l’autorizzazione formale delle richieste di acquisto da parte del responsabile della funzione richiedente;

l’autorizzazione formale delle fatture di acquisto dei servizi da parte del responsabile della funzione richiedente;

la verifica, in fase di sviluppo di un nuovo prodotto, del fatto che il costo definito sia in linea con il target costo definito nel brief predisposto dalla funzione Marketing per il lancio di ogni nuovo prodotto;

la predisposizione di un calendario delle attività per il lancio di nuovi prodotti;

l’autorizzazione per l’inserimento di una nuova anagrafica di prodotto e la verifica circa la correttezza, l’accuratezza e la completezza dei dati anagrafici inseriti nel sistema contabile-gestionale della Società;

l’autorizzazione degli ordini di acquisto da parte di adeguato livello manageriale, con successiva archiviazione cartacea della documentazione.

Nell’espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.), i soggetti aziendali coinvolti nell’area a rischio “gestione personale” sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all’art. 25-quater del Decreto 231, al rispetto delle regole e procedure aziendali emesse a regolamentazione di tale area a rischio. Tali regole e procedure prevedono controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio, tra i quali, ad esempio:

la definizione di ruoli, responsabilità e modalità operative relative alla formalizzazione di un budget annuale da destinare a nuove assunzioni;

la formalizzazione del piano delle assunzioni in sede di definizione del budget annuale;

un processo di ricerca del personale regolamentato, che prevede l’identificazione di canali di selezione specifici, scelti in base alle condizioni di ricerca ed ai requirements necessari per ricoprire il ruolo richiesto;

la verifica in merito a potenziali conflitti di interesse del candidato, potenziali procedimenti penali in corso e/o la presenza del nominativo in liste di riferimento anti terrorismo;

la compilazione di un form specifico da usare in sede di colloquio contenente le motivazioni relative alla scelta del candidato;

la definizione dei documenti richiesti al momento dell’assunzione;

la consegna di nuovi dipendenti del codice di condotta;

l’accettazione della lettera di dimissioni da parte di adeguato livello manageriale;

la definizione strutturata delle politiche di valutazione del personale e sviluppo di carriera in base a specifiche linee guida che stabiliscono, tra gli altri, i seguenti aspetti:

- i criteri di valutazione delle risorse
- i piani di carriera per figura professionale
- le modalità, le responsabilità e le autorizzazioni collegate al processo di valutazione periodica delle performance del personale
- le retribuzioni base e variabili, con formalizzazione delle valutazioni che giustificano l'erogazione di bonus / incrementi salariali
- l’allineamento dell’inquadramento contrattuale con la media di mercato e con le fasce di retribuzioni stabilite
- l’autorizzazione delle retribuzioni da parte di adeguato livello manageriale;

- la definizione di un processo strutturato di pianificazione e svolgimento delle attività di formazione, sulla base dello sviluppo dei piani di carriera, con identificazione di ruoli, responsabilità e modalità operative in merito all'erogazione della formazione;
- il monitoraggio delle attività di formazione.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.), i soggetti aziendali coinvolti nell'area a rischio "amministrazione, contabilità e bilancio" sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all'art. 25-quater del Decreto 231, al rispetto delle regole e procedure aziendali emesse a regolamentazione di tale area a rischio. Tali regole e procedure prevedono controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio, tra i quali, ad esempio:

- la definizione del flusso autorizzativo per la richiesta dell'apertura o della modifica di un nuovo conto, da parte dei responsabili amministrativi delle Società del gruppo al responsabile amministrativo della capogruppo che deve autorizzare ogni richiesta;
- la restrizione degli accessi sul sistema contabile-gestionale per i soli addetti autorizzati a creare e/o modificare il piano dei conti;
- la previsione di un modulo pre-definito per la richiesta di apertura e/o modifica di un conto, che deve essere archiviato presso l'ufficio amministrativo della Società;
- la verifica mensile del bilancio di verifica al fine di identificare possibili conti obsoleti che debbano essere eliminati dal piano dei conti;
- l'autorizzazione formale in merito all'apertura delle anagrafiche fornitori e clienti da parte del responsabile del richiedente, secondo procedura definita;
- la definizione delle informazioni necessarie ai fini dell'apertura/modifica delle anagrafiche;
- la verifica periodica in merito alle aperture / modifiche effettuate alle anagrafiche al fine di verificare la corrispondenza con quelle autorizzate;
- i controlli, sia in occasione dell'inserimento anagrafico sia in fasi successive di monitoraggio, in merito alla corrispondenza dei nominativi dei fornitori in anagrafica con i nominativi di individui direttamente o indirettamente collegabili ad organizzazioni terroristiche elencati in apposite black list (UIF, UE, OFAC);
- le verifiche in merito alla piena coincidenza tra destinatari/ ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- la verifica di corrispondenza tra fattura passiva e ordine di acquisto prima della registrazione della fattura stessa;
- il blocco al pagamento prima dell'autorizzazione dello stesso da parte della funzione richiedente per le fatture passive prive di ordine;
- l'emissione di fatture attive solo in seguito alla comunicazione dei dati di fatturazione forniti dalle funzioni responsabili;
- i flussi autorizzativi per l'acquisizione/dismissione di cespiti;

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.), i soggetti aziendali coinvolti nell'area a rischio "tesoreria" sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all'art. 25- quater del Decreto 231, al rispetto delle regole e procedure aziendali emesse a regolamentazione di tale area a rischio. Tali regole e procedure prevedono controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area a rischio, tra i quali, ad esempio:

- l'autorizzazione in base alle procure esistenti ed a deleghe formali per l'apertura/chiusura di conti correnti bancari;
- la verifica da parte del responsabile amministrativo delle disposizioni di pagamento prima dell'invio ai procuratori per l'autorizzazione;
- le utenze e le password per l'accesso al sistema di home banking disponibili solo ai procuratori;
- l'autorizzazione dei pagamenti in conformità alle procure conferite dalla Società;
- le verifiche di accertamento in merito alla coincidenza tra destinatari dei pagamenti e controparti effettivamente coinvolte nelle transazioni;

- le verifiche di accertamento in merito alla correttezza delle informazioni tra gli ordinanti dei pagamenti e le controparti effettivamente coinvolte nelle transazioni;
- le riconciliazioni bancarie mensili da parte degli addetti amministrativi e controllo delle stesse da parte del responsabile della amministrazione;
- l'autorizzazione delle riconciliazioni bancarie da parte di adeguato livello manageriale e l'archiviazione della documentazione di supporto;
- le modalità operative per autorizzare e gestire gli investimenti finanziari;
- l'autorizzazione da parte del CFO e/o del CEO, titolari di apposite procure, per le operazioni relative ad investimenti, acquisizioni o dismissioni finanziarie.

Tutte le attività sensibili ricomprese nelle aree a rischio reato devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure di Digital Bros, nonché le regole contenute nel presente Modello.

In generale, il sistema di organizzazione, gestione e controllo della Società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività sopra descritte e, in generale, delle proprie funzioni, gli Organi Sociali, gli amministratori, i dipendenti, i procuratori di Digital Bros, nonché i collaboratori e tutte le altre controparti contrattuali, devono conoscere e rispettare:

- la normativa italiana e straniera applicabile alle attività svolte;
- le disposizioni contenute nel presente Modello;
- il Codice Etico Aziendale;
- le procedure e le linee guida di Digital Bros nonché tutta la documentazione attinente il sistema di organizzazione, gestione e controllo della Società.

### **3.G Principi per la predisposizione delle procedure per la prevenzione dei delitti aventi finalità di terrorismo o di eversione dell'ordine democratico.**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste specifiche procedure, in forza delle quali:

- a) siano ricostruibili la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- b) non vi sia identità soggettiva fra coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- c) i documenti riguardanti l'attività d'impresa siano archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;
- d) qualora il servizio di archiviazione e/o conservazione dei documenti sia svolto, per conto della Società, da un soggetto ad essa estraneo, il servizio debba essere regolato da un contratto nel quale si preveda, tra l'altro, che il soggetto che presta il servizio alla Società rispetti specifiche procedure di controllo idonee a non permettere la modificazione successiva dei documenti archiviati, se non con apposita evidenza;
- e) l'accesso ai documenti, di cui ai punti precedenti, già archiviati sia sempre motivato e consentito solo al soggetto competente in base alle norme interne, o a suo delegato, al Collegio Sindacale od organo equivalente, alla società di revisione o all'Organismo di Vigilanza;
- f) la scelta di consulenti esterni avvenga sulla base di requisiti di professionalità, indipendenza e competenza e, in riferimento a essi, sia motivata la scelta come stabilito dal Codice Etico,
- g) non siano corrisposti compensi, provvigioni o commissioni a Agenti, Partners Commerciali, Collaboratori, Fornitori o a soggetti pubblici in misura non congrua rispetto alle prestazioni rese alla Società e/o comunque non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;
- h) i sistemi di remunerazione premianti ai Dipendenti e Collaboratori rispondano a obiettivi realistici e coerenti con le mansioni e l'attività svolta e con le responsabilità affidate;

i) la Società, ai fini dell'attuazione delle decisioni di impiego delle risorse finanziarie, si avvalga di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea;

l) nessun pagamento può essere effettuato in contanti, salvo specifica preventiva autorizzazione da parte della funzione Amministrazione Finanza e Controllo;

m) come previsto dal Codice Etico, i rapporti con i terzi (clienti, fornitori, collaboratori esterni, partner, consulenti, ecc.) dovranno essere improntati a lealtà, correttezza, trasparenza e tracciabilità, nel rispetto dello spirito di collaborazione; l'osservanza di tali principi dovrà altresì essere richiesta ai terzi, i quali dovranno essere portati a conoscenza del presente Codice Etico.

n) gli Organi Sociali, i dipendenti e i procuratori di Digital Bros nonché i collaboratori e tutte le altre controparti contrattuali, nell'ambito delle attività da essi svolte, devono rispettare, inoltre, le regole di comportamento di seguito indicate:

- le operazioni contabili devono essere perfettamente tracciabili, nel pieno rispetto delle procedure contabili disposte dalla Società;
- sono vietate operazioni finanziarie e/o commerciali con controparti che utilizzano strutture societarie opache e/o che impediscono l'identificazione univoca dell'assetto societario (proprietà) e/o dei reali beneficiari dell'operazione;
- sono vietate operazioni con soggetti (persone fisiche / giuridiche) già inseriti nelle Liste diramate dalle Autorità nazionali (UIF) ed internazionali (OFAC; UE) di soggetti sospettati di legami con organizzazioni terroristiche nazionali e/o internazionali, nonché con Banche e/o intermediari finanziari censiti nelle medesime liste;
- eventuali transazioni finanziarie con trust, società anonime e strutture giuridiche volte a celare l'assetto societario devono essere considerate tra gli indici di anomalia suscettibili di essere portati all'attenzione dell'Organismo di Vigilanza;
- in caso di visite ispettive e/o richieste di informazioni da parte di Autorità investigative in merito ad indagini in materia di riciclaggio e contrasto al finanziamento del terrorismo, è fatto obbligo di avvertire gli Amministratori e l'Organismo di Vigilanza e fornire alle Autorità tutta la documentazione richiesta.

#### **4.G – Elenco delle procedure per la prevenzione dei delitti aventi finalità di terrorismo o di eversione dell'ordine democratico.**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste le seguenti specifiche procedure:

a) Codice Etico;

b) Sign Off (H5 Gestione del Personale);

c) Sign Off (H2 Acquisti non di materiali destinati alla rivendita).

L'Organismo di Vigilanza cura che le procedure di cui al presente paragrafo siano idonee al rispetto delle prescrizioni in esso contenute e adeguate alle finalità in precedenza indicate.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

L'Organismo di Vigilanza vigila che nelle società appartenenti al Gruppo siano adottati principi e procedure coerenti con i principi e le procedure fatti propri dalla Società, ai fini della prevenzione degli abusi di mercato.

**PARTE SPECIALE**  
**SEZIONE "H"**

**REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O  
UTILITÀ DI PROVENIENZA ILLECITA, NONCHE' AUTORICICLAGGIO E REATI  
TRIBUTARI**

**(art. 25-octies e art. 25-quinquiesdecies del D. Lgs. 231/2001)**

La responsabilità amministrativa di un Ente sorge anche in relazione ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché, a seguito dell'introduzione dell'art. 25-quinquiesdecies, anche in relazione ad alcune fattispecie delittuose in materia tributaria.

Il D.Lgs. 21 novembre 2007, n. 231 è intervenuto inserendo l'art. 25-octies, disposizione che estende il regime della responsabilità amministrativa delle persone giuridiche (D.Lgs. 231/2001) alle ipotesi di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (artt. 648, 648-bis e 648-ter del codice penale).

In particolare, al comma 1 dell'art. 25-octies è previsto che si applica all'Ente la sanzione pecuniaria da 200 a 800 quote (ai sensi dell'art. 10 del D.Lgs. 231/2001). Nel caso in cui il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni si applica la sanzione pecuniaria da 400 a 1000 quote.

Il comma 2 prevede inoltre che "nei casi di condanna per uno dei delitti di cui al comma 1 si applicano all'Ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore a due anni".

Per quanto concerne l'art. 25-quinquiesdecies, la responsabilità amministrativa prevista dal D.Lgs. 231/2001 viene estesa anche in caso di commissione di una tra le seguenti fattispecie previste dal D.Lgs. 74/2000: delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 commi 1 e 2-bis) con sanzione; delitto di dichiarazione fraudolenta mediante altri artifici (art. 3); delitto di emissione di fatture o altri documenti per operazioni inesistenti (art. 8 commi 1 e 2-bis); delitto di occultamento o distruzione di documenti contabili (art. 10); delitto di sottrazione fraudolenta al pagamento di imposte (art. 11).

Di seguito è fornita una breve descrizione dei principali reati contemplati dall'art. 25-octies e 25-quinquiesdecies del Decreto.

**Ricettazione (art. 648 c.p.)**

Il reato si configura, fuori dei casi di concorso nel reato, quando, al fine di procurare a sé o ad altri un profitto, è acquistato, ricevuto od occultato denaro o cose provenienti da un qualsiasi delitto.

La condotta criminosa si configura anche nei confronti di chi s'intromette nel fare acquistare, ricevere od occultare denaro o cose provenienti da un qualsiasi delitto.

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

Il reato si configura, fuori dei casi di concorso nel reato, quando si sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero si compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

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

Il reato si configura, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, quando si impegna in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

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

Il delitto di autoriciclaggio si realizza quando chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative,

il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Fuori dei casi di cui sopra, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale.

**Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, commi 1 e 2-bis, D. Lgs. n. 74/2000)***“1. È punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.*

...

*2-bis. Se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.”*

La fattispecie appena descritta può essere integrata innanzitutto in occasione della contabilizzazione e dunque dichiarazione di una fattura per un'operazione mai realizzata.

Accanto a questa, il reato tributario in commento viene altresì posto in essere in altre ipotesi come, in primo luogo, nel caso di operazioni effettivamente realizzate, ma per importi inferiori rispetto a quelli riportati in fattura. Per quanto concerne l'imposta sul valore aggiunto, il reato può essere commesso anche quando vi è diversità tra il soggetto che ha effettuato l'operazione e quello che compare in fattura.

Altri casi di condotte integranti l'applicazione della responsabilità da reato riguardano l'impiego di documenti che, seppur non qualificabili come fatture in senso proprio, assumono rilevanza ai fini fiscali (si pensi, ad esempio, alle note spese, ecc.).

In caso di commissione della fattispecie di cui al primo comma, la sanzione pecuniaria è fino a 500 quote; per il caso della fattispecie di cui al comma 2-bis, la sanzione pecuniaria è fino a 400 quote.

#### **Dichiarazione fraudolenta mediante altri artifici (art. 3 D. Lgs. n. 74/2000)**

*“1. Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:*

*a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;*  
*b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.*

*2. Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.*

*3. Ai fini dell'applicazione della disposizione del comma 1, non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.”*

La fattispecie in esame può essere integrata da chi, col chiaro fine di evadere le imposte menzionate, indica nelle dichiarazioni per le imposte medesime degli elementi attivi con un importo inferiore rispetto a quello effettivo o elementi passivi fittizi o crediti e ritenute fittizi. Per fare ciò, è necessario che il soggetto agente compia operazioni simulate oppure si avvalga di documenti falsi oppure faccia ricorso ad altri mezzi fraudolenti tali da fuorviare l'amministrazione finanziaria nell'attività di accertamento.

La sanzione pecuniaria applicabile è fino a 500 quote.

**Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 commi 1 e 2-bis D.Lgs. 74/2000)**

*“1. È punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.*

...

*2-bis. Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.”*

La fattispecie in esame viene integrata quando il soggetto agente, attraverso l'emissione o il rilascio di fatture od altri documenti per operazioni inesistenti, consente a terzi di evadere i redditi o l'imposta sul valore aggiunto.

**Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. 74/2000)**

*“Salvo che il fatto costituisca più grave reato, è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge 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.”*

Tale fattispecie può essere integrata attraverso l'occultamento o la distruzione totale o parziale di scritture contabili o documenti di cui è obbligatoria la conservazione. È altresì necessario che mediante tale occultamento e tale distruzione, il soggetto agente consenta l'evasione delle imposte sui redditi o sull'imposta sul valore aggiunto, oppure permetta l'evasione a soggetti terzi.

La fattispecie può essere esclusa quando il risultato economico della società può essere ricostruito ed accertato mediante altra documentazione conservata.

**Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. 74/2000)**

*“1. È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.*

*2. È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.”*

L'ipotesi di reato di cui al presente articolo viene integrata in caso di alienazione o uso di atti simulati o fraudolenti idonei ad evitare il pagamento di debiti tributari e ad impedire all'amministrazione finanziaria di svolgere efficacemente attività recuperatoria.

**1.H – Potenziali aree a rischio**

In considerazione delle attività svolte dalla Digital Bros le principali aree di rischio sono individuate:

- Gestione degli acquisti
- Gestione delle risorse finanziarie e dei flussi finanziari in entrata e in uscita
- Operazioni infragruppo, con parti correlate o in potenziale conflitto di interesse e Operazioni straordinarie

- Gestione delle consulenze

La Società si è dotata di specifiche procedure interne per la gestione di tali attività che descrivono, tra l'altro, le singole fasi dei vari processi in modo da assicurare il rispetto della normativa e la formalizzazione dei controlli e delle azioni conseguenti intraprese.

Il presente Modello di Organizzazione Gestione e Controllo, per tutto ciò che riguarda il rispetto del D.Lgs. 231/2007 e delle ulteriori norme collegate, rimanda alle suddette procedure interne di volta in volta in vigore.

### **Gestione degli acquisti**

Il processo di gestione degli acquisti è relativo alle attività inerenti l'acquisizione di beni o servizi.

Oltre a quanto già indicato nella Parte Speciale A (Reati contro la PA) in merito a tale processo, gli ulteriori elementi di controllo sono quelli di seguito indicati.

Tutti i soggetti coinvolti nella gestione degli acquisti devono effettuare la verifica dell'attendibilità commerciale e professionale dei fornitori e partner commerciali/finanziari, sulla base di indici rilevanti (es. dati pregiudizievoli pubblici, protesti, procedure concorsuali; acquisizione di informazioni commerciali sull'azienda, sui soci e sugli amministratori tramite società specializzate; entità del prezzo sproporzionata rispetto ai valori medi di mercato).

In caso di stipula di contratti, i soggetti coinvolti nel processo devono verificare che gli stessi contratti con i suddetti soggetti terzi contengano apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. 231/2001 e di impegno al suo rispetto, con indicazione delle relative conseguenze in caso di violazione (ad es. penali, risoluzione, ecc.).

Tutti i Destinatari devono tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori/clienti/partner.

### **Gestione delle risorse finanziarie e dei flussi finanziari in entrata e in uscita**

Il processo riguarda la gestione delle risorse finanziarie aziendali e degli incassi e pagamenti. Oltre a quanto già indicato nella Parte Speciale A (Reati contro la PA) in merito a tale processo, gli ulteriori elementi di controllo sono quelli di seguito indicati.

Il sistema di controllo si basa su livelli autorizzativi definiti, sulla separazione di ruolo nelle fasi chiave del processo, sulla registrazione e sulla tracciabilità dei vari atti e sulla valutazione complessiva delle attività svolte.

Solamente i soggetti muniti degli specifici poteri (es. Amministratore Delegato) e coloro da questi incaricati possono disporre delle risorse finanziarie e delle relative modalità di effettuazione dei pagamenti (ad es. mediante operazioni su conto corrente bancario, emissione assegni, note spese, ecc.).

Gli addetti dell'ufficio tesoreria devono verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni. Tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese).

Il responsabile dell'ufficio tesoreria effettua periodicamente verifiche sulla tesoreria (rispetto delle soglie per i pagamenti per contanti, eventuale utilizzo di libretti al portatore per la gestione della liquidità, ecc.) al fine di accertare il rispetto della normativa in materia di antiriciclaggio.

1. Per la registrazione e la tracciabilità delle varie fasi del processo, tutta l'attività svolta deve essere registrata e tracciata, anche tramite l'archiviazione della documentazione cartacea inerente al fine di consentire la ricostruzione delle responsabilità.

2. Al fine di poter effettuare una valutazione complessiva dell'attività svolta, la Società richiede a tutti i soggetti coinvolti rendicontare periodicamente in merito.

Nella gestione delle consulenze Si ricorda che gli incarichi conferiti ai Consulenti devono essere redatti per iscritto, con l'indicazione del compenso pattuito.

L'individuazione e la scelta del consulente, a garanzia degli standard qualitativi richiesti per le prestazioni professionali, deve sempre essere fondata su capacità tecniche e professionali, rispettare requisiti di obiettività,

imparzialità e trasparenza nonché pertinenza e congruità della spesa stabilita. Infine devono sempre essere rispettate le disposizioni sull'assenza di conflitto d'interessi.

I soggetti individuati devono essere figure la cui professionalità e competenza siano rispondenti al ruolo da svolgere. Per ogni incarico deve sempre essere presente una dichiarazione di conoscenza della normativa di cui al D.Lgs. 231/2001 e di impegno al suo rispetto, con indicazione delle relative conseguenze in caso di violazione (ad es. penali, risoluzione, ecc.).

### **Adeguata verifica della clientela**

La Società ha l'obbligo di effettuare una adeguata verifica della clientela in relazione ai rapporti e alle operazioni inerenti allo svolgimento dell'attività professionale e, in particolare, nei seguenti casi:

- a) quando si instaura un rapporto;
- b) quando sono eseguite operazioni occasionali, disposte dai clienti che comportino la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che siano effettuate con una operazione unica o con più operazioni che appaiono tra di loro collegate per realizzare un'operazione frazionata.

Gli obblighi di adeguata verifica della clientela consistono nelle seguenti attività:

- a) identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente;
- b) identificare l'eventuale titolare effettivo e verificarne l'identità;
- c) ottenere informazioni sullo scopo e sulla natura prevista del rapporto continuativo o della prestazione professionale;
- d) svolgere un controllo costante nel corso del rapporto continuativo o della prestazione professionale.

Gli obblighi di adeguata verifica della clientela si attuano nei confronti di tutti i nuovi clienti. Per la clientela già acquisita i suddetti obblighi si applicano al primo contatto utile, fatta salva la valutazione del rischio presente.

E' data facoltà alla Società di avvalersi degli obblighi semplificati di adeguata verifica quando il suo cliente è un ente creditizio o finanziario, una società quotata in borsa o un ufficio della pubblica amministrazione purché dimostri di aver raccolto informazioni sufficienti per tale beneficio e abbia concretamente svolto un'effettiva analisi dei rischi di riciclaggio relativamente alle operazioni svolte, in quanto la Società è comunque soggetta agli obblighi di adeguata verifica e di registrazione ordinari nel caso in cui possa esserci un sospetto di riciclaggio, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile. Inoltre la Società non può avvalersi della facoltà di utilizzare un'adeguata verifica semplificata nel caso in cui non sia in grado di dimostrare di aver raccolto tutte le informazioni sufficienti per stabilire se il cliente può beneficiare di tali esenzioni e di aver analizzato i rischi di riciclaggio delle operazioni svolte.

La Società è tenuta a conservare i documenti ed a registrare le informazioni che ha acquisito per assolvere gli obblighi di adeguata verifica della clientela affinché possano essere utilizzati per qualsiasi indagine su eventuali operazioni di riciclaggio o di finanziamento del terrorismo o analisi effettuate dalla UIF o da qualsiasi altra Autorità competente.

Nei casi in cui la Società si avvalga della facoltà di adeguata verifica semplificata, dal 04 Novembre 2009, giorno dell'entrata in vigore del "Decreto Legislativo 25 settembre 2009, n.151 – disposizioni integrative e correttive del decreto legislativo 21 novembre 2007, n. 231, recante attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, nonché della direttiva 2006/70/CE che reca misure di esecuzione" che ha introdotto l'art. 36 comma 6-bis, potrà essere esentata dagli obblighi di registrazione purché sia in grado di dimostrare l'iter di valutazione e conservi evidenza delle informazioni e della documentazione a supporto della verifica effettuata sull'applicabilità di tale esenzione al cliente.

La Società sarà sempre tenuta a registrazione nel caso in cui:

- non possa avvalersi dell'adeguata verifica semplificata
- non sia in grado di dimostrare di poter avvalersi dell'esenzione
- vi sia il sospetto di riciclaggio o di finanziamento del terrorismo
- abbia motivo di ritenere che l'identificazione effettuata non sia attendibile
- non riesca ad acquisire le informazioni necessarie per la valutazione.

Nei casi in cui non possa avvantaggiarsi dell'esenzione dovrà registrare e conservare per un periodo di dieci anni, le seguenti informazioni:

- con riferimento ai rapporti instaurati: la data di instaurazione, i dati identificativi del cliente e del titolare effettivo, unitamente alle generalità dei delegati a operare per conto del titolare del rapporto e il codice del rapporto ove previsto;
- con riferimento a tutte le operazioni di importo pari o superiore a € 15.000 euro, indipendentemente del fatto che si tratti di un'operazione unica o di più operazioni che appaiono tra di loro collegate per realizzare un'operazione frazionata: la data, la causale, l'importo, la tipologia dell'operazione, i mezzi di pagamento e i dati identificativi del soggetto che effettua l'operazione e del soggetto per conto del quale eventualmente opera. alle attività sono analiticamente disciplinate dalle procedure vigenti approvate dalla Società, alle quali si rimanda.

Il sistema di controllo si basa su livelli autorizzativi definiti, sulla registrazione e sulla tracciabilità delle varie fasi del processo:

1. L'ufficio tesoreria tramite la modulistica interna deve raccogliere tutte le informazioni e la documentazione prevista dalle procedure interne, nonché svolgere un controllo costante nel corso del rapporto continuativo o della prestazione professionale.
2. L'ufficio tesoreria si accerta che siano stati utilizzati e debitamente compilati tutti i documenti approvati dalla Società, nonché sia stata fornita dal cliente tutta la documentazione richiesta, e provvede alla archiviazione dei documenti cartacei e/o elettronici.
3. L'ufficio tesoreria verifica che le procedure adottate siano adeguate al rispetto della normativa vigente, e che siano effettivamente applicate dalla Società.
4. I soggetti coinvolti nel processo devono garantire la registrazione delle varie fasi del processo e la loro tracciabilità, tramite l'utilizzo dei sistemi informativi adottati dalla Società o la conservazione e archiviazione della documentazione prodotta.
5. Al fine di poter effettuare una valutazione complessiva dell'attività svolta, la Società richiede a tutti i soggetti coinvolti rendicontare periodicamente in merito.

### **Obblighi di astensione**

Quando la Società non è in grado di rispettare gli obblighi di adeguata verifica della clientela, non può instaurare il rapporto continuativo né eseguire operazioni o prestazioni professionali e deve porre fine al rapporto continuativo o alla prestazione professionale già in essere e valutano se effettuare una segnalazione alla UIF.

Nel caso in cui non sia possibile rispettare gli obblighi di adeguata verifica relativamente a rapporti continuativi già in essere, operazioni o prestazioni professionali in corso di realizzazione, la Società restituisce al cliente i fondi, gli strumenti e le altre disponibilità finanziarie di spettanza, liquidandone il relativo importo tramite bonifico su un conto corrente bancario indicato dal cliente stesso.

Inoltre, prima di effettuare la segnalazione di operazione sospetta alla UIF, la Società si astiene dall'eseguire le operazioni per le quali sospetta vi sia una relazione con il riciclaggio o con il finanziamento del terrorismo.

Nei casi in cui l'astensione non sia possibile in quanto sussiste un obbligo di legge di ricevere l'atto ovvero l'esecuzione dell'operazione per sua natura non possa essere rinviata o l'astensione possa ostacolare le indagini, permane l'obbligo di immediata segnalazione di operazione sospetta.

Il sistema di controllo si basa su livelli autorizzativi definiti, sulla registrazione e sulla tracciabilità delle varie fasi del processo:

1. L'ufficio tesoreria, accertata l'impossibilità da parte della Società di adempiere agli obblighi di adeguata verifica della clientela, informa tempestivamente tutti i soggetti coinvolti che la Società non può instaurare il rapporto continuativo né eseguire operazioni o prestazioni professionali e deve porre fine al rapporto continuativo o alla prestazione professionale già in essere.
2. Contestualmente, l'ufficio tesoreria valutano anche se effettuare una segnalazione alla UIF e comunica l'esito delle proprie decisioni al legale rappresentante. Prima di effettuare la segnalazione di operazione sospetta alla UIF, la Società si astiene dall'eseguire le operazioni per le quali sospetta vi sia una relazione con il riciclaggio o con il finanziamento del terrorismo.

Nei casi in cui l'astensione non sia possibile in quanto sussiste un obbligo di legge di ricevere l'atto ovvero l'esecuzione dell'operazione per sua natura non possa essere rinviata o l'astensione possa ostacolare le indagini, permane l'obbligo di immediata segnalazione di operazione sospetta.

3. Con il supporto delle varie funzioni della Società, L'ufficio tesoreria provvede a restituire al cliente i fondi, gli strumenti e le altre disponibilità finanziarie di spettanza, liquidandone il relativo importo tramite bonifico su un conto corrente bancario indicato dal cliente stesso. Il trasferimento dei fondi è accompagnato da un messaggio che indica alla controparte bancaria che le somme sono restituite al cliente per l'impossibilità di rispettare gli obblighi di adeguata verifica della clientela.

4. I soggetti coinvolti nel processo devono garantire la registrazione delle varie fasi del processo e la loro tracciabilità, tramite l'utilizzo dei sistemi informativi adottati dalla Società o la conservazione e archiviazione della documentazione prodotta.

5. Al fine di poter effettuare una valutazione complessiva dell'attività svolta, la Società richiede a tutti i soggetti coinvolti rendicontare periodicamente in merito.

### **Registrazione delle informazioni e tenuta dell'Archivio Unico Informatico**

La Società deve conservare i documenti e registrare le informazioni acquisite per assolvere gli obblighi di adeguata verifica della clientela affinché possano essere utilizzati per qualsiasi indagine su eventuali operazioni di riciclaggio o di finanziamento del terrorismo o per corrispondenti analisi effettuate dalla UIF o da qualsiasi altra Autorità competente.

Le informazioni previste dalla normativa vigente e dalle procedure interne sono registrate tempestivamente e, comunque, non oltre il trentesimo giorno successivo al compimento dell'operazione ovvero all'apertura, alla variazione e alla chiusura del rapporto continuativo ovvero all'accettazione dell'incarico professionale, all'eventuale conoscenza successiva di ulteriori informazioni, o al termine della prestazione professionale. L'Archivio Unico Informatico è formato e gestito in modo tale da assicurare la chiarezza, la completezza e l'immediatezza delle informazioni, la loro conservazione secondo criteri uniformi, il mantenimento della storicità delle informazioni, la possibilità di desumere evidenze integrate, la facilità di consultazione. E' strutturato in modo tale da contenere gli oneri gravanti sui diversi destinatari, tenere conto delle peculiarità operative dei diversi destinatari e semplificare le registrazioni.

Il sistema di controllo si basa su livelli autorizzativi definiti, sulla registrazione e sulla tracciabilità delle varie fasi del processo.

1. Il responsabile dell'ufficio tesoreria è la funzione preposta alla raccolta di tutta la documentazione necessaria per gli adempimenti agli obblighi di registrazione. Ricevuta tutta la documentazione, il responsabile dell'ufficio tesoreria provvede tempestivamente alle dovute registrazioni nell'Archivio Unico Informatico e comunque entro 30 giorni.

2. Il responsabile dell'ufficio tesoreria si accerta che il flusso informativo e documentale sia adeguato al rispetto degli obblighi di registrazione, e verifica che la Società abbia ottemperato agli obblighi di registrazione, nei tempi e nei modi stabiliti dalla normativa vigente.

3. I soggetti coinvolti nel processo devono garantire la registrazione delle varie fasi del processo e la loro tracciabilità, tramite l'utilizzo dei sistemi informativi adottati dalla Società o la conservazione e archiviazione della documentazione prodotta.

4. Al fine di poter effettuare una valutazione complessiva dell'attività svolta, la Società richiede a tutti i soggetti coinvolti rendicontare periodicamente in merito.

### **Segnalazione di operazioni sospette**

La Società deve inviare alla UIF una segnalazione di operazione sospetta quando sa, sospetta o ha motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo. Il sospetto è desunto dalle caratteristiche, entità, natura dell'operazione o da qualsivoglia altra circostanza conosciuta in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi a disposizione dei segnalanti, acquisiti nell'ambito dell'attività svolta ovvero a seguito del conferimento di un incarico.

Al fine di agevolare l'individuazione delle operazioni sospette, su proposta della UIF sono emanati e periodicamente aggiornati indicatori di anomalia, ai quali si rimanda.

Il sistema di controllo si basa su livelli autorizzativi definiti, sulla registrazione e sulla tracciabilità delle varie fasi del processo.

1. Chiunque ravvisi una ipotesi di operazione sospetta, informa tempestivamente il proprio superiore che effettua una prima valutazione e successivamente trasmette all'ufficio tesoreria tutte le informazioni di cui dispone.
2. L'ufficio tesoreria esamina le comunicazioni ricevute e, se necessario o opportuno, effettua i necessari approfondimenti anche tramite il supporto delle altre funzioni aziendali.
3. Nel caso in cui l'ufficio tesoreria valuti fondate le comunicazioni ricevute, deve effettuare la segnalazione di operazione sospetta appena viene a conoscenza degli elementi di sospetto, ove possibile prima di eseguire l'operazione.
4. L'ufficio tesoreria informa il legale rappresentante di tutte le segnalazioni di operazioni sospette effettuate e non effettuate.
- 5 I soggetti coinvolti nel processo devono garantire la registrazione delle varie fasi del processo e la loro tracciabilità, tramite l'utilizzo dei sistemi informativi adottati dalla Società o la conservazione e archiviazione della documentazione prodotta.
6. Al fine di poter effettuare una valutazione complessiva dell'attività svolta, la Società richiede a tutti i soggetti coinvolti rendicontare periodicamente in merito.

## **2.H – Principi di comportamento e controllo nelle principali aree a rischio**

Tutti i Destinatari del Modello, se coinvolti nello svolgimento di attività a rischio, devono:

- rispettare il Codice Etico;
- rispettare le procedure aziendali relative alle suddette attività a rischio;
- assicurare lo sviluppo e la gestione operativa degli strumenti utilizzati nelle attività di contrasto al riciclaggio;
- verificare e garantire l'aggiornamento / manutenzione / diffusione delle liste interne di soggetti/Paesi/merci interessati da provvedimenti restrittivi;
- nel caso di valutazione di clienti/fornitori/partners, collaborare con le altre funzioni aziendali e, ove consentito dalla normativa vigente, scambiare le informazioni finalizzate alla completa ed adeguata conoscenza.

Tutti i soggetti coinvolti nelle varie attività interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nella presente sezione.

I compiti dell'Organismo di Vigilanza, in relazione alla prevenzione dei reati elencati nella presente Parte Speciale, sono da intendersi tutti quelli facenti parte del Regolamento dell'OdV e, qualora non fossero compresi nel predetto Regolamento, di quelli successivamente indicati:

- verifica dell'osservanza, dell'attuazione e dell'adeguatezza del Modello (Parte Generale e Speciale) in ottica di prevenzione della commissione dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita;
- vigilanza sull'effettiva applicazione della Parte Generale del Modello e della presente Parte Speciale e rilevazione delle deviazioni comportamentali dei Destinatari qualora riscontrati dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- comunicazione di eventuali violazioni del Modello o della presente Parte Speciale agli organi competenti e aggiornamento del Modello.

## **3.H – Principi per la redazione delle procedure per la prevenzione dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita e dei reati tributari.**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste

specifiche procedure, in forza delle quali:

- a) siano ricostruibili la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
  - b) non vi sia identità soggettiva fra coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
  - c) i documenti riguardanti l'attività d'impresa siano archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;
  - d) la scelta di consulenti esterni avvenga sulla base di requisiti di professionalità, indipendenza e competenza e, in riferimento a essi, sia motivata la scelta come stabilito dal Codice Etico,
  - e) si realizzi la formalizzazione del piano delle assunzioni in sede di definizione del budget annuale; la selezione avvenga in base ad un processo definito che prevede un colloquio con l'amministrazione del personale e uno con il responsabile della funzione competente;
  - f) l'ufficio del personale verifichi preventivamente in merito a potenziali conflitti di interesse del candidato da assumere, potenziali procedimenti penali in corso e/o la presenza del nominativo in liste di riferimento anti terrorismo;
  - g) la scelta di nuovi fornitori avvenga in base ad un processo di selezione basato su una procedura di ricerca e selezione, nella quale sono definiti i parametri di valutazione, l'esigenza e le certificazioni richieste al fornitore e conseguentemente con la previsione di un processo strutturato di qualifica dei fornitori;
  - h) ci sia evidenza dell'accettazione formale del fornitore da parte del responsabile di funzione in caso di termini di pagamento richiesti differenti dagli standard;
  - i) si realizzi la tracciabilità del flusso autorizzativo per la richiesta dell'apertura o della modifica di un nuovo conto, da parte dei Responsabili amministrativi delle Società del gruppo al responsabile amministrativo della capogruppo che deve autorizzare ogni richiesta;
- la Società, ai fini dell'attuazione delle decisioni di impiego delle risorse finanziarie, si avvalga di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea;
- l) nessun pagamento può essere effettuato in contanti, salvo specifica preventiva autorizzazione da parte della funzione Amministrazione Finanza e Controllo;
  - m) come previsto dal Codice Etico, i rapporti con i terzi (clienti, fornitori, collaboratori esterni, partner, consulenti, ecc.) dovranno essere improntati a lealtà, correttezza, trasparenza e tracciabilità, nel rispetto dello spirito di collaborazione; l'osservanza di tali principi dovrà altresì essere richiesta ai terzi, i quali dovranno essere portati a conoscenza del presente Codice Etico;
  - n) gli Organi Sociali, i dipendenti e i procuratori di Digital Bros nonché i collaboratori e tutte le altre controparti contrattuali, nell'ambito delle attività da essi svolte, devono rispettare, inoltre, le regole di comportamento di seguito indicate:
    - le operazioni contabili devono essere perfettamente tracciabili, nel pieno rispetto delle procedure contabili disposte dalla Società;
    - sono vietate operazioni finanziarie e/o commerciali con controparti che utilizzano strutture societarie opache e/o che impediscono l'identificazione univoca dell'assetto societario (proprietà) e/o dei reali beneficiari dell'operazione;
  - o) il responsabile della tesoreria effettui i controlli, sia in occasione dell'inserimento anagrafico sia in fasi successive di monitoraggio, in merito alla corrispondenza dei nominativi dei fornitori in anagrafica con i nominativi di individui direttamente o indirettamente collegabili ad organizzazioni terroristiche elencati in apposite black list (UIF, UE, OFAC);
  - p) il responsabile della tesoreria effettui le verifiche in merito alla piena coincidenza tra destinatari/ ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni e verifichi le disposizioni di pagamento prima dell'invio ai procuratori per l'autorizzazione;
  - q) le utenze e le password per l'accesso al sistema di home banking siano disponibili solo ai procuratori;
  - r) si realizzino le riconciliazioni bancarie mensili da parte degli addetti della tesoreria e controllo delle stesse da parte del responsabile amministrativo;

s) si definisca un limite definito circa le erogazioni liberali, che devono sempre rispettare le soglie definite a livello di budget ed essere tracciate tramite richieste di acquisto cartacee debitamente firmate da parte di adeguato livello manageriale e autorizzate, nel complessivo importo, dal Consiglio di Amministrazione; Eventuali transazioni finanziarie con trust, società anonime e strutture giuridiche volte a celare l'assetto societario devono essere considerate tra gli indici di anomalia suscettibili di essere portati all'attenzione dell'Organismo di Vigilanza;

In caso di visite ispettive e/o richieste di informazioni da parte di Autorità investigative in merito ad indagini in materia di riciclaggio e contrasto al finanziamento del terrorismo, è fatto obbligo di avvertire gli Amministratori e l'Organismo di Vigilanza e fornire alle Autorità tutta la documentazione richiesta.

#### **4.H – Elenco delle procedure per la prevenzione dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita e dei reati tributari.**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste le seguenti specifiche procedure:

- a) Codice Etico;
- b) Sign Off;
- c) Procedura in merito alla realizzazione di operazioni significative e in cui un amministratore risulti portatore di interesse;
- d) Regolamento per l'uso di auto aziendali date in uso promiscuo;
- e) Procedura per la disciplina delle operazioni con parti correlate
- f) Sistema ERP (Navision);
- g) Sign Off (H3 Intercompany);
- h) Sign Off (H5 Gestione del Personale);
- i) Sign Off (H6 Acquisti di materiali destinati alla rivendita);
- l) Sign Off (H7 Vendita Servizi);
- m) Sign Off (H8 Gestione listini);
- n) Sign Off (H9 Contratti estimatori e resi di merce);
- o) Sign Off (H10 Sales & Cogs report).
- p) Policy Gruppo Digital Bros per l'utilizzo dei Sistemi ICT.

L'Organismo di Vigilanza cura che le procedure di cui al presente paragrafo siano idonee al rispetto delle prescrizioni in esso contenute e adeguate alle finalità in precedenza indicate.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

L'Organismo di Vigilanza vigila che nelle società appartenenti al Gruppo siano adottati principi e procedure coerenti con i principi e le procedure fatti propri dalla Società.

**PARTE SPECIALE**  
**SEZIONE "I"**  
**IMPIEGO DI LAVORATORI STRANIERI**  
**(art. 25-duodecies del D. Lgs. 231/2001)**

Con l'entrata in vigore del D.Lgs. n. 109/2012, recante norme in attuazione della direttiva 2009/52/CE sulle norme minime relative a sanzioni e provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare, è stato introdotto nel D.Lgs. 231/2001 il nuovo art. 25-*duodecies*, con la rubrica: "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare". Si ampliano quindi le fattispecie di reato che possono portare alla responsabilità amministrativa delle società in sede penale.

Il nuovo art. 25-*duodecies* prevede che in relazione alla commissione del delitto di cui all'articolo 22, comma 12-bis, del decreto legislativo 25 luglio 1998, n. 286 si applica all'Ente la sanzione pecuniaria da pecuniaria da 100 a 200 quote, entro il limite di 150.000 euro.

Il riferimento puntuale è all'art. 22 comma 12 del D.lgs. 286/98 disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero.

In particolare si fa riferimento al datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, o il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, oppure sia revocato o annullato.

Le pene per il fatto previsto dal comma 12 sono aumentate da un terzo alla metà:

- a) se i lavoratori occupati sono in numero superiore a tre;
- b) se i lavoratori occupati sono minori in età non lavorativa;
- c) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-bis del codice penale.

**Disposizioni contro le immigrazioni clandestine (Decreto Legislativo 25 luglio 1998, n. 286, art. 12 comma 3, 3-bis, 3-ter e 5)**

La norma punisce, salvo che il fatto costituisca più grave reato, chiunque, in violazione delle disposizioni del presente testo unico, promuove, dirige, organizza, finanzia o effettua il trasporto di stranieri nel territorio dello Stato ovvero compie altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente nel caso in cui:

- a) il fatto riguarda l'ingresso o la permanenza illegale nel territorio dello Stato di cinque o più persone;
- b) la persona trasportata è stata esposta a pericolo per la sua vita o per la sua incolumità per procurarne l'ingresso o la permanenza illegale;
- c) la persona trasportata è stata sottoposta a trattamento inumano o degradante per procurarne l'ingresso o la permanenza illegale;
- d) il fatto è commesso da tre o più persone in concorso tra loro o utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti;
- e) gli autori del fatto hanno la disponibilità di armi o materie esplosive.

Se i fatti di cui sopra sono commessi ricorrendo due o più delle ipotesi di cui alle lettere a), b), c), d) ed e) la pena è aumentata.

La pena è altresì aumentata se i fatti di cui al primo capoverso:

- sono commessi al fine di reclutare persone da destinare alla prostituzione o comunque allo sfruttamento sessuale o lavorativo ovvero riguardano l'ingresso di minori da impiegare in attività illecite al fine di favorirne lo sfruttamento;
- sono commessi al fine di trarne profitto, anche indiretto.

Fuori dei casi sopra esposti, e salvo che il fatto non costituisca più grave reato, è punito chiunque, al fine di trarre un ingiusto profitto dalla condizione di illegalità dello straniero o nell'ambito delle attività punite a norma del presente articolo, favorisce la permanenza di questi nel territorio dello Stato in violazione delle

norme del Decreto Legislativo 25 luglio 1998, n. 286. Quando il fatto è commesso in concorso da due o più persone, ovvero riguarda la permanenza di cinque o più persone, la pena è aumentata.

Per i delitti di cui all'art. 12, commi 3, 3-bis e 3-ter, si applica la sanzione pecuniaria da 400 a 1000 quote nonché le sanzioni interdittive previste dall'art. 9, comma 2 del D.Lgs. 231/2001 per una durata non inferiore ad un anno. Per il delitto di cui all'art. 12, comma 5, si applica la sanzione pecuniaria da 100 a 200 quote nonché le sanzioni interdittive previste dall'art. 9, comma 2 del D.Lgs. 231/2001 per una durata non inferiore ad un anno.

### **1.1 – Potenziali aree a rischio**

In considerazione delle attività svolte dalla Digital Bros le principali aree di rischio sono individuate nell'attività di gestione del personale.

Il processo di selezione, assunzione e gestione del personale è formato da tutte le attività necessarie alla costituzione del rapporto di lavoro tra la Società e una persona fisica e alla successiva gestione.

### **2.1 – Principi di comportamento e controllo nelle principali aree a rischio**

Nella fase di assunzione del lavoratore straniero è compito degli addetti all'ufficio personale verificare la regolarità del permesso di soggiorno.

Il Datore di Lavoro deve informare il lavoratore straniero di provvedere tempestivamente a comunicare alla Società ogni modifica al permesso di soggiorno (es. revoca, annullamento).

Gli addetti all'ufficio personale devono monitorare le scadenze del permesso di soggiorno, in modo da richiedere al lavoratore straniero la copia della richiesta di rinnovo del permesso, nei termini stabiliti dalla legge. Qualora il lavoratore straniero non consegna la copia della richiesta di rinnovo, l'ufficio personale deve informare tempestivamente il Datore di Lavoro per interrompere il rapporto di lavoro.

1. Al fine di poter effettuare una valutazione complessiva, la Società richiede ai soggetti coinvolti di rendicontare in merito all'attività svolta.

A tutti i soggetti sopra indicati è espressamente vietato:

- (i) porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da configurare la fattispecie di reato richiamata nella presente Parte Speciale;
- (ii) porre in essere, collaborare o dare causa alla realizzazione di comportamenti i quali, sebbene risultino tali da non costituire di per sé reato, possano potenzialmente diventarlo.

Tutti i Destinatari del Modello, se coinvolti nello svolgimento di attività nelle attività a rischio, devono:

- (a) verificare e garantire l'aggiornamento dello scadenziario relativo ai permessi di soggiorno dei lavoratori stranieri;
- (b) in attuazione degli adempimenti riferiti alla presente parte speciale, devono riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità o anomalie.

### **3.1 - Principi per la predisposizione delle procedure per la prevenzione dei delitti di cui alla presente sezione.**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste specifiche procedure, in forza delle quali:

- a) siano ricostruibili la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- b) i documenti riguardanti l'attività di selezione del personale e gestione del personale siano archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;
- d) la scelta di consulenti esterni avvenga sulla base di requisiti di professionalità, indipendenza e competenza e, in riferimento a essi, sia motivata la scelta come stabilito dal Codice Etico,
- e) si realizzi la formalizzazione del piano delle assunzioni in sede di definizione del budget annuale;
- f) la selezione avvenga in base ad un processo definito che prevede un colloquio con l'amministrazione del personale e uno con il responsabile della funzione competente;

g) l'ufficio del personale verifichi preventivamente in merito a alla esistenza del permesso di soggiorno di candidati stranieri e successivamente all'assunzione verifichi la durata dello stesso e garantisca l'aggiornamento dello scadenziario relativo ai permessi di soggiorno dei lavoratori stranieri.

**4.I – Elenco delle procedure per la prevenzione dei delitti di cui alla presente sezione.**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste le seguenti specifiche procedure:

- a) Codice Etico;
- b) Sign Off (H2 Acquisti non di materiali destinati alla rivendita);
- c) Sign Off (H5 Gestione del Personale).

L'Organismo di Vigilanza cura che le procedure di cui al presente paragrafo siano idonee al rispetto delle prescrizioni in esso contenute e adeguate alle finalità in precedenza indicate.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

L'Organismo di Vigilanza vigila che nelle società appartenenti al Gruppo siano adottati principi e procedure coerenti con i principi e le procedure fatti propri dalla Società.

**PARTE SPECIALE**  
**SEZIONE "L"**  
**REATI TRANSNAZIONALI**  
**(art. 10 L. 146/2006)**

L'articolo 10 della Legge n. 146/2006 ha esteso la responsabilità amministrativa degli enti anche ad alcune fattispecie di reato quando la loro commissione assume carattere transnazionale. Tra tali fattispecie di reato vengono anzitutto richiamati i reati di associazione per delinquere (art. 416 c.p.), associazioni di tipo mafioso anche straniere (art. 416-bis c.p.), associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater D.P.R. 23 gennaio 1973, n. 43) e associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9 ottobre 1990, n. 309). In questi casi si applicano, per una durata non inferiore ad un anno, le sanzioni interdittive dell'interdizione dall'esercizio dell'attività, la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi ed il divieto di pubblicizzare beni o servizi, nonché la sanzione pecuniaria da 400 fino a 1000 quote. La norma richiama inoltre le disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5, D. Lgs. 25 luglio 1998, n. 286), alle quali si applicano sia la sanzione pecuniaria da 200 fino a 1000 quote, sia le sanzioni interdittive dell'interdizione dall'esercizio dell'attività, la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi ed il divieto di pubblicizzare beni o servizi, per una durata non superiore a due anni. La norma, infine, fa riferimento ai reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.) e favoreggiamento personale (art. 378 c.p.) ai quali si applica una sanzione pecuniaria fino a 500 quote.

L'articolo 3 della Legge n. 146/2006 stabilisce che i reati appena menzionati, le cui condotte incriminatrici verranno approfondite di seguito, si considerano transnazionali qualora sia coinvolto un gruppo criminale organizzato, nonché: a) sia commesso in più di uno Stato; b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato; c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

**Associazione per delinquere (art. 416 c.p.)**

La norma punisce chi promuove, costituisce o organizza associazioni di tre o più persone con il fine di commettere più delitti.

**Associazioni di tipo mafioso anche straniere (art. 416-bis c.p.)**

La norma punisce chi fa parte di un'associazione di tipo mafioso formata da tre o più persone.

**Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater D.P.R. 23 gennaio 1973, n. 43)**

Tale fattispecie si configura quando tre o più persone si associano allo scopo di commettere più delitti tra quelli previsti dall'articolo 291-bis (contrabbando di tabacchi lavorati esteri).

**Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9**

**ottobre 1990, n. 309)**

La norma punisce l'associazione di tre o più persone finalizzata al traffico illecito di sostanze stupefacenti e c.d. precursori di droghe.

**Disposizioni contro le immigrazioni clandestine (Decreto Legislativo 25 luglio 1998, n. 286, art. 12 comma 3, 3-bis, 3-ter e 5)**

Per tale fattispecie si rimanda alla Parte Speciale Sezione "I".

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

Tale fattispecie si configura allorché taluno, con violenza, minaccia, con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere, davanti alla autorità giudiziaria, dichiarazioni utilizzabili in un procedimento penale, quando questa ha facoltà di non rispondere, salvo che il fatto costituisca più grave reato.

**Favoreggiamento personale (art. 378 c.p.)**

Tale fattispecie viene integrata quando un soggetto aiuta taluno a eludere le investigazioni dell'Autorità, comprese quelle svolte da organi della Corte penale internazionale, o a sottrarsi alle ricerche effettuate dai medesimi soggetti.

**1.L – Potenziali aree a rischio**

In considerazione delle attività svolte dalla Digital Bros le principali aree di rischio sono individuate nell'attività di gestione degli investimenti finanziari, gestione degli acquisti, attività di Marketing e gestione del personale.

**2.L – Principi di comportamento e controllo nelle principali aree a rischio**

Obiettivo della presente Parte Speciale è che i Destinatari si attengano – nella misura in cui gli stessi siano coinvolti nello svolgimento delle attività rientranti nelle aree a rischio e in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti di Digital Bros - a regole di condotta conformi a quanto prescritto nella stessa al fine di prevenire e impedire il verificarsi dei Reati Transnazionali.

Tutte le attività, nell'ambito delle categorie di operazioni a rischio devono essere svolte in conformità delle leggi, procedure e regolamenti vigenti, al Modello, al Codice di Autodisciplina ed ai valori e alle politiche e regole della Digital Bros. In particolare, è necessario che le operazioni vengano realizzate secondo principi di trasparenza e correttezza.

I seguenti principi si applicano nell'ambito della Digital Bros a tutti i Destinatari del presente Modello.

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 10 della L. n. 146/2006); sono altresì proibite le violazioni ai principi ed alle procedure aziendali.

È pertanto necessario:

- rispettare il Codice Etico;
- rispettare le procedure aziendali relative alle suddette attività a rischio;
- nel caso di valutazione di clienti/fornitori/partners, collaborare con le altre funzioni aziendali e, ove consentito dalla normativa vigente, scambiare le informazioni finalizzate alla completa ed adeguata conoscenza.

**3.L - Principi per la predisposizione delle procedure per la prevenzione dei delitti di cui alla presente sezione.**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste specifiche procedure, in forza delle quali:

- siano ricostruibili la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- i documenti riguardanti l'attività di selezione del personale e gestione del personale siano archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;
- la scelta di consulenti esterni avvenga sulla base di requisiti di professionalità, indipendenza e competenza e, in riferimento a essi, sia motivata la scelta come stabilito dal Codice Etico,
- si realizzi la formalizzazione del piano delle assunzioni in sede di definizione del budget annuale;
- la selezione avvenga in base ad un processo definito che prevede un colloquio con l'amministrazione del personale e uno con il responsabile della funzione competente;
- l'ufficio del personale verifichi preventivamente in merito alla esistenza del permesso di soggiorno di candidati stranieri e successivamente all'assunzione verifichi la durata dello stesso e garantisca l'aggiornamento dello scadenziario relativo ai permessi di soggiorno dei lavoratori stranieri;
- siano ricostruibili la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- la scelta di consulenti esterni avvenga sulla base di requisiti di professionalità, indipendenza e competenza e, in riferimento a essi, sia motivata la scelta come stabilito dal Codice Etico;
- come previsto dal Codice Etico, i rapporti con i terzi (clienti, fornitori, collaboratori esterni, partner, consulenti, ecc.) dovranno essere improntati a lealtà, correttezza, trasparenza e tracciabilità, nel rispetto dello spirito di collaborazione; l'osservanza di tali principi dovrà altresì essere richiesta ai terzi, i quali dovranno essere portati a conoscenza del presente Codice Etico.

#### **4.L – Elenco delle procedure per la prevenzione dei delitti di cui alla presente sezione.**

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste le seguenti specifiche procedure:

- a) Codice Etico;
- b) Sign Off;
- c) Sign Off (H2 Acquisto non di materiali);
- d) Procedura in merito alla realizzazione di operazioni significative e in cui un amministratore risulti portatore di interesse;
- e) Policy Gruppo Digital Bros per l'utilizzo dei Sistemi ICT.

L'Organismo di Vigilanza cura che le procedure di cui al presente paragrafo siano idonee al rispetto delle prescrizioni in esso contenute e adeguate alle finalità in precedenza indicate.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

L'Organismo di Vigilanza vigila che nelle società appartenenti al Gruppo siano adottati principi e procedure coerenti con i principi e le procedure fatti propri dalla Società.

**PARTE SPECIALE**  
**SEZIONE “M”**  
**ALTRI REATI**

Come evidenziato nella parte generale, in relazione all’attività svolta da Digital Bros e dall’analisi delle risposte fornite in sede di intervista, è emerso che il rischio relativo alla commissione dei reati e/o delitti riportati nell’elenco in calce sia remoto e, pertanto, solo astrattamente e non concretamente ipotizzabile:

Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-bis, D.Lgs. n. 231/2001) [articolo aggiunto dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001; modificato dalla L. n. 99/2009; modificato dal D.Lgs. 125/2016]

Pratiche di mutilazione degli organi genitali femminili (Art. 583-bis c.p.) (Art. 25-quater.1, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 7/2006]

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria (Art. 25-decies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 116/2009]

Reati ambientali (Art. 25-undecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 121/2011, modificato dalla L. n. 68/2015]

Razzismo e xenofobia (Art. 25-terdecies)

Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25-quaterdecies)

ALLEGATI - MODELLO DI COMUNICAZIONE ALL'ORGANISMO DI VIGILANZA

Spettabile  
Organismo di Vigilanza  
c/o Digital Bros

SEGNALAZIONE DI NOTIZIE RILEVANTI  
AI SENSI DEL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

a) SEGNALANTE INTERNO

Il sottoscritto \_\_\_\_\_ nella sua qualifica di \_\_\_\_\_, interno n. \_\_\_\_\_

b) SEGNALANTE ESTERNO

Il sottoscritto \_\_\_\_\_, nato a \_\_\_\_\_, residente in \_\_\_\_\_, n. \_\_\_\_\_  
telefono \_\_\_\_\_, in qualità di \_\_\_\_\_

**SEGNALA**

INFORMATIVE SULLE CONDOTTE POTENZIALMENTE IN VIOLAZIONE DEL MODELLO

.....  
.....  
.....  
.....  
.....  
.....