MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
ai sensi del D.Lgs. 231/01

DI

QUID INFORMATICA S.p.A

APPROVATO DAL CONSIGLIO DI AMMINISTRAZIONE IL 29 LUGLIO 2020

AGGIORNAMENTO CON DELIBERA DEL CONSIGLIO DI AMMINISTRAZIONE DEL 26 OTTOBRE 2021

AGGIORNAMENTO CON DELIBERA DEL CONSIGLIO DI AMMINSISTRAZIONE DEL 5 APRILE 2022

AGGIORNAMENTO CON DELIBERA DEL CONSIGLIO DI AMMINSISTRAZIONE DEL 29 MARZO 2024

INDICE

Sommario

DEFINIZIONI

ATTIVITÀ SENSIBILE:	Attività aziendali nel cui ambito sussiste il rischio, anche potenziale, di commissione dei reati previsti dal Decreto.
AUTONOMIA FINANZIARIA:	Consiste nella possibilità di disporre di risorse finanziarie per il proprio settore di attività all'interno della Società.
CODICE ETICO:	Il Codice Etico è il documento che rappresenta la dichiarazione dei valori, l'insieme dei diritti, dei doveri e delle responsabilità che la Società assume nei confronti di chiunque si trovi a collaborare con essa o ad usufruire dei suoi servizi.
CONSULENTI:	Soggetti che, in ragione delle competenze professionali, prestano la propria opera intellettuale in favore o per conto della Società sulla base di un mandato o di altro rapporto di collaborazione professionale.
D.LGS. N. 231/2001 O DECRETO O DECRETO 231:	Decreto Legislativo 8 giugno 2001, n. 231 e successive modificazioni e integrazioni.
DIPENDENTI:	Soggetti aventi con la Società un rapporto di lavoro subordinato, parasubordinato o somministrati da agenzie per il lavoro.
INCARICATI DI UN PUBBLICO SERVIZIO	Ai sensi dell'art. 358 cod. pen. "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 quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".
LINEE GUIDA DI CONFINDUSTRIA:	Documento-guida di Confindustria (approvato il 7 marzo 2002 aggiornamento nel marzo 2014 e da ultimo a giugno 2021) per la costruzione dei modelli di organizzazione, gestione e controllo di cui al Decreto.
MODELLO:	Il Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001 predisposto dalla Società.
ORGANISMO DI VIGILANZA (ODV):	L'organismo interno di controllo, preposto alla vigilanza sul funzionamento e sull'osservanza del Modello, nonché al relativo aggiornamento, istituito ai sensi e per gli effetti dell'art. 6 del D.Lgs. 231/2001, conformemente alle previsioni emanate da Confindustria.

PARTNER:	Le controparti contrattuali con le quali la Società addivenga ad una qualche forma di collaborazione, contrattualmente regolata (associazione temporanea d'impresa, consorzio, agenzia, etc.), ove destinate a cooperare con la Società nell'ambito delle Attività sensibili.
PROCESSO "STRUMENTALE"	Processo in cui risiedono gli strumenti per la commissione del reato.
PUBBLICA AMMINISTRAZIONE (PA):	La Pubblica Amministrazione intesa in senso lato, e dunque: lo Stato (ivi inclusi enti governativi, territoriali, locali, settoriali, quali gli organi governativi, autorità regolamentari, Regioni, Province, Comuni, circoscrizioni) e/o tutti gli enti e soggetti pubblici (e nei casi determinati per legge i soggetti privati che comunque svolgono funzione pubblica quali, ad es., concessionari, organi di diritto pubblico, amministrazioni aggiudicatrici, società miste), che esercitano attività volte a provvedere al perseguimento di interessi pubblici. Si ricorda che tale definizione comprende anche la PA di Stati Esteri e dell'Unione Europea. In particolare, con riferimento ai Reati nei confronti della PA, ci si riferisce ai pubblici ufficiali e agli incaricati di un pubblico servizio.
REATI:	Le fattispecie di reato alle quali si applica la disciplina prevista dal Decreto sulla responsabilità amministrativa degli enti.
REGOLE FORMALIZZATE:	Le procedure, le disposizioni organizzative, le circolari e gli ordini di servizio con efficacia vincolante emanati all'interno della società.
SISTEMA DI CONTROLLO INTERNO:	L'insieme di regole, procedure e strutture organizzative che contribuisce a garantire il raggiungimento degli obiettivi di efficienza ed efficacia operativa, l'affidabilità delle informazioni finanziarie e gestionali, il rispetto delle leggi e dei regolamenti, nonché la salvaguardia del patrimonio sociale e dei terzi
SOCIETA':	QUID INFORMATICA S.P.A.
WHISTLEBLOWING:	Il "Whistleblowing" è un istituto di origine anglosassone, finalizzato a regolamentare e facilitare il processo di segnalazione di illeciti o di altre irregolarità di cui il soggetto segnalante (cd. "whistleblower") sia venuto a conoscenza e che prevede, per quest'ultimo, significative forme di tutela.

Tale materia è stata integrata nel Decreto 231 art. 6 dalla Legge 30 novembre 2017, n. 179, recante "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*".

PARTE GENERALE

SEZIONE PRIMA

1 Il Decreto Legislativo 231/2001

1.1 La Responsabilità amministrativa degli enti

In data 8 giugno 2001 è stato emanato – in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 – il Decreto Legislativo n. 231 (di seguito denominato anche il "Decreto" o "D.Lgs. 231/2001"), entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali cui l'Italia aveva già in precedenza aderito, ed in particolare:

- la Convenzione di Bruxelles del 26 luglio 1995 sulla 'tutela degli interessi finanziari delle Comunità Europee';
- la Convenzione anch'essa firmata a Bruxelles il 26 maggio 1997 sulla 'lotta alla corruzione di funzionari delle Comunità Europee o degli Stati membri';
- la Convenzione OCSE del 17 dicembre 1997 sulla 'lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali'.

Il Decreto ha introdotto nell'ordinamento giuridico *la responsabilità amministrativa degli enti per gli illeciti dipendenti da reato*. Le disposizioni in esso previste si applicano agli "*enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica" (di seguito anche solo "enti").*

Tale nuova forma di responsabilità, sebbene definita "amministrativa" dal legislatore, presenta tuttavia taluni caratteri propri della responsabilità penale, essendo ad esempio rimesso al giudice penale competente l'accertamento dei reati dai quali essa è fatta derivare ed essendo estese all'ente le garanzie del processo penale.

Il Decreto stabilisce che:

1. L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:
    a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;
    b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).
2. L'ente non risponde se le persone indicate nel punto 1 hanno agito nell'interesse esclusivo proprio o di terzi.

Oltre all'esistenza degli elementi oggettivi e soggettivi sopra descritti, il Decreto richiede anche l'accertamento della colpevolezza dell'ente, al fine di poterne affermare la responsabilità. Tale requisito è in definitiva riconducibile ad una "colpa di organizzazione", da intendersi quale mancata adozione, da parte dell'ente, di misure preventive adeguate a

prevenire la commissione dei reati elencati al successivo paragrafo, da parte dei soggetti individuati nel Decreto.

La responsabilità amministrativa dell'ente è quindi ulteriore e diversa da quella della persona fisica che ha materialmente commesso il reato e sono entrambe oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale. Peraltro, la responsabilità dell'ente permane anche nel caso in cui la persona fisica autrice del reato non sia identificata o non risulti punibile.

La responsabilità dell'impresa può ricorrere anche se il delitto presupposto si configura nella forma di tentativo (ai sensi dell'art. 26 del D.Lgs. 231/2001), vale a dire quando il soggetto agente compie atti idonei diretti in modo non equivoco a commettere il delitto e l'azione non si compie o l'evento non si verifica.

1.2 I reati previsti dal Decreto

I reati da cui può conseguire la responsabilità amministrativa per l'Ente sono espressamente indicati nel Decreto ed in successivi provvedimenti normativi che ne hanno allargato la portata. Si elencano di seguito le "famiglie di reato" attualmente ricomprese nell'ambito di applicazione del D.Lgs. 231/2001, i **cd. reati presupposto**:

1. **Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture** (Art. 24, D. Lgs. n. 231/2001) [articolo modificato dalla L. 161/2017 e dal D. Lgs. 75/2020 e dalla L. n 137/2023];
2. **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 e dal D. L. n. 105/2019];
3. **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];
4. **Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio** (Art. 25, D. Lgs. n. 231/2001) [articolo modificato dalla L. n. 190/2012 dalla L.3/19 e dal D.Lgs. n. 75/2020];
5. **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];
6. **Delitti contro l'industria e il commercio** (Art. 25-bis.1, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009];
7. **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. n. 69/2015, dal D. Lgs. 38/2017 e dal

D. Lgs. n. 19/2023];

8. **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];
9. **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];
10. **Delitti contro la personalità individuale** (Art. 25-quinquies, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 228/2003; modificato dalla L. n. 199/2016];
11. **Reati di abuso di mercato** (Art. 25-sexies, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 62/2005];
12. **Altre fattispecie in materia di abuso di mercato** (art. 187-quinquies TUF) [articolo modificato dal D.Lgs. 107/2018];
13. **Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro** (Art. 25-septies, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 123/2007 mod. L. 3/2018];
14. **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 e dal D. Lgs. n. 195/2021];
15. **Delitti in materia di strumenti di pagamento diversi dai contanti** (Art. 25 octies1, D. Lgs. n. 231/2001) [articolo aggiunto dal d. Lgs. 184/2021 e modificato dalla L. 137/2023];

    Altre fattispecie in materia di strumenti di pagamento diversi dai contanti (Art. 25 octies1 comma 2, D. Lgs. n. 231/2001) [articolo aggiunto dal d. Lgs. 184/2021];
16. **Delitti in materia di violazione del diritto d'autore** (Art. 25-novies, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009 e modificato dalla L. n. 93/2023];
17. **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];
18. **Reati ambientali** (Art. 25-undecies, D. Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 121/2011, modificato dalla L. n. 68/2015 e dal D.Lgs. 21/2018];
19. **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, modificato dalle L. n. 161/2017 e dal D.L. n. 20/2023];
20. **Razzismo e xenofobia** (Art. 25-terdecies, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 167/2017 e modificato dal D. Lgs. 21/2018];
21. **Reati transnazionali** (L. n. 146/2006);
22. **Reati relativi a frode in competizioni sportive esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati** (Art.25-

quaterdecies del D. Lgs. 231/2001) [articolo aggiunto dalla L. n. 39/2019];

23. **Reati tributari** (Art. 25 quinquiesdecies del D. Lgs. 231/2001) [L. 19 dicembre 2019, n. 157, di conversione del D.L. 26 ottobre 2019, n. 124 (c.d. decreto fiscale) e dal D.Lgs. n. 75/2020];
24. **Contrabbando** (Art. 25-sexiesdecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 75/2020]
25. **Delitti contro il patrimonio culturale** (Art. 25-septiesdecies, D. Lgs. 231/2001) [articolo aggiunto dalla L. n. 22/2022 modificazo dalla L. n. 6/2024];
26. **Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici** (Art. 25-duodevicies, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 22/2022];
27. **Delitti tentati** (Art. 26 D. Lgs n. 231/2001).

In Allegato A si fornisce il dettaglio delle singole "fattispecie di reato" incluse in ciascuna famiglia ([1]).

1.3 Le sanzioni previste dal Decreto

La competenza a conoscere degli illeciti amministrativi dell'ente appartiene al giudice penale. L'accertamento della responsabilità può comportare l'applicazione di sanzioni gravi e pregiudizievoli per la vita dell'ente stesso, quali:

a) sanzioni pecuniarie;
b) sanzioni interdittive;
c) confisca;
d) pubblicazione della sentenza.

In particolare le sanzioni interdittive, che si applicano in relazione ai reati per i quali sono espressamente previste, possono comportare importanti restrizioni all'esercizio dell'attività di impresa dell'ente, quali:

a) interdizione dall'esercizio dell'attività;
b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) divieto di contrattare con la Pubblica Amministrazione, salvo che per le prestazioni del pubblico servizio;
d) esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o revoca di quelli eventualmente già concessi;
e) divieto di pubblicizzare beni o servizi.

[1] Aggiornato alla data dell'8 febbraio 2024 (ultimo provvedimento inserito: L. n. 6/2024).

Tali misure possono essere applicate all'ente anche in via cautelare, e dunque prima dell'accertamento nel merito in ordine alla sussistenza del reato e dell'illecito amministrativo che da esso dipende, nell'ipotesi in cui si ravvisi l'esistenza di gravi indizi tali da far ritenere la responsabilità dell'ente, nonché il pericolo di reiterazione dell'illecito.

Nell'ipotesi in cui il giudice ravvisi l'esistenza dei presupposti per l'applicazione di una misura interdittiva a carico di un ente che svolga attività di interesse pubblico ovvero abbia un consistente numero di dipendenti, lo stesso potrà disporre che l'ente continui a operare sotto la guida di un commissario giudiziale.

1.4 Condizione esimente della Responsabilità amministrativa

L'art. 6 del D.Lgs. 231/2001 stabilisce che l'ente, nel caso di reati commessi da soggetti apicali, non risponda qualora dimostri che:

a) l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi;
b) il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di proporne l'aggiornamento sia stato affidato ad un Organismo dell'ente dotato di autonomi poteri di iniziativa e controllo (c.d. "Organismo di Vigilanza, nel seguito anche "Organismo" o "OdV");
c) le persone hanno commesso il reato eludendo fraudolentemente il suddetto Modello;
d) non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Nel caso in cui il reato sia stato commesso da soggetti sottoposti alla direzione o alla vigilanza del personale apicale, l'ente sarà ritenuto responsabile del reato solamente in ipotesi di carenza colpevole negli obblighi di direzione e vigilanza.

Pertanto, l'ente che, prima della commissione del reato, adotti e dia concreta attuazione ad un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi, è esente da responsabilità se risultano integrate le condizioni di cui all'art. 6 del Decreto.

In tal senso il Decreto fornisce specifiche indicazioni in merito alle esigenze cui i Modelli Organizzativi devono rispondere:

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

Tuttavia la mera adozione di un Modello Organizzativo non è di per sé sufficiente ad escludere detta responsabilità, essendo necessario che il modello sia effettivamente ed efficacemente attuato. In particolare ai fini di un efficace attuazione del Modello, il Decreto richiede:

- una verifica periodica e l'eventuale modifica dello stesso quando siano emerse significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione o nell'attività;
- la concreta applicazione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso.

L'Ente dovrà, dunque, dimostrare la sua estraneità ai fatti contestati al soggetto apicale provando la sussistenza dei sopra elencati requisiti tra loro concorrenti e, di riflesso, la circostanza che la commissione del reato non derivi da una propria "colpa organizzativa".

Nel caso, invece, di un reato commesso da soggetti sottoposti, l'Ente risponde se la commissione del reato è stata resa possibile dalla violazione degli obblighi di direzione o vigilanza alla cui osservanza la società stessa è tenuta (art. 7 comma 1).

In ogni caso, la violazione degli obblighi di direzione o vigilanza è esclusa se l'Ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire i reati della specie di quello verificatosi.

Al riguardo, si evidenzia che l'ipotesi di inversione dell'*onus probandi* (a carico dell'ente) espressa dalla dottrina e dalla giurisprudenza sulla base del contrasto di tale presunzione di responsabilità con i principi costituzionali di cui agli artt. 3, 24 e, soprattutto, 27 della nostra Carta Fondamentale, è stata negata da parte della Suprema Corte di Cassazione. La Corte, infatti, ha concluso che «nessuna inversione dell'onere della prova è, pertanto, ravvisabile nella disciplina che regola la responsabilità da reato dell'ente, gravando comunque sull'Accusa l'onere di dimostrare la commissione del reato da parte di persona che rivesta una delle qualità di cui all'art. 5 D.lgs. n. 231 e la carente regolamentazione interna dell'ente. Quest'ultimo ha ampia facoltà di fornire prova liberatoria» (cfr. Cass. n. 27735/2010 cit.).

1.5 I reati commessi all'estero

In forza dell'art. 4 del Decreto, l'ente può essere considerato responsabile, in Italia, per la commissione all'estero di taluni reati. In particolare, l'art. 4 del Decreto prevede che gli enti aventi la sede principale nel territorio dello Stato rispondono anche in relazione ai reati commessi all'estero nei casi e alle condizioni previsti dagli articoli da 7 a 10 del codice penale, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto. Pertanto, l'ente è perseguibile quando:

- in Italia ha la sede principale, cioè la sede effettiva ove si svolgono le attività amministrative e di direzione, eventualmente anche diversa da quella in cui si trova l'azienda o la sede legale (enti dotati di personalità giuridica), ovvero il luogo in cui viene svolta l'attività in modo continuativo (enti privi di personalità giuridica);

- nei confronti dell'ente non stia procedendo lo Stato del luogo in cui è stato commesso il fatto;
- la richiesta del Ministro della giustizia, cui sia eventualmente subordinata la punibilità, è riferita anche all'ente medesimo.

Tali regole riguardano i reati commessi interamente all'estero da soggetti apicali o sottoposti. Per le condotte criminose che siano avvenute anche solo in parte in Italia, si applica il principio di territorialità *ex* art. 6 del codice penale, in forza del quale "il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione".

1.6 Le nuove fattispecie di reato

Nell'attività di costante manutenzione del Modello, non va trascurata l'evoluzione dei "reati presupposto" via via implementati nel Decreto stesso che, dal 2001 ad oggi, ha assistito ad importanti mutamenti e integrazioni.

Le modifiche al Decreto intervenute nel corso del 2019 sono state introdotte dalla *Legge Anticorruzione* (Legge 9 gennaio 2019, n.3) e dalla *Legge* di ratifica ed esecuzione della Convenzione del Consiglio d'Europa *sulle manipolazioni sportive*, fatta a Magglingen il 18 settembre 2014 (Legge 3 maggio 2019, n.39).

Tra le modifiche più significative della Legge Anticorruzione si segnalano, in particolare: i) l'inasprimento delle sanzioni interdittive in caso di reato di concussione, induzione indebita a dare o promettere utilità o corruzione; ii) la procedibilità d'ufficio per i reati di corruzione tra privati e di istigazione alla corruzione tra privati.

La riforma dei reati tributari introdotta con la L. 19 dicembre 2019, n. 157, di conversione del D.L. 26 ottobre 2019, n. 124 (c.d. decreto fiscale), ha inserito nel Decreto l'art. 25 quinquiesdecies, che indica per quali reati tributari (previsti cioè nel novellato D. Lgs. 74/2000) commessi per interesse o vantaggio dell'ente, possa determinarsi la responsabilità amministrativa:

a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'art. 2, comma 1, d.lgs. 74/2000, la sanzione pecuniaria fino a cinquecento quote;

b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'art. 2, comma 2-bis, d.lgs. 74/2000, la sanzione pecuniaria fino a quattrocento quote;

c) per il delitto di dichiarazione fraudolenta mediante altri artifici previsto dall'art. 3, d.lgs. 74/2000, la sanzione pecuniaria fino a cinquecento quote;

d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti previsto dall'art. 8, d.lgs. 74/2000, comma 1, la sanzione pecuniaria fino a cinquecento quote;

e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti previsto dall'art. 8, comma 2-bis, d.lgs. 74/2000, la sanzione pecuniaria fino a quattrocento

quote;

f) per il delitto di occultamento o distruzione di documenti contabili previsto dall'art. 10, d.lgs. 74/2000, la sanzione pecuniaria fino a quattrocento quote;

g) per il delitto di sottrazione fraudolenta al pagamento di imposte previsto dall'art. 11, d.lgs. 74/2000, la sanzione pecuniaria fino a quattrocento quote.

In caso di profitto di rilevante entità la sanzione pecuniaria subisce un aumento di un terzo. Sono inoltre applicabili le sanzioni interdittive di cui all'art. 9, comma 2, d.lgs. 231/2001, lettere c) (divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio), lettera d) (esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi) e lettera e) (divieto di pubblicizzare beni o servizi). L'intervento normativo s'innesta nel contesto di una costante estensione della responsabilità amministrativa da reato dell'ente, determinata anche da un intervento europeo in tal senso (la direttiva UE 17/1371) e da un clima politico, in materia penale, estremamente rigorista nei confronti dei reati dei c.d. "grandi evasori".

Con riferimento a quanto sopra, il D.Lgs. n. 75/2020 (di attuazione della Direttiva PIF), ha apportato le seguenti modifiche al D.Lgs. 231/2001:

- all'art. 24 sono stati introdotti i reati di "Frode nelle pubbliche forniture" ex art. 356 c.p. e "Frode ai danni del Fondo europeo agricolo" ex art. 2 Legge n. 898/1986, per i quali è prevista la sanzione pecuniaria fino a 500 quote e le sanzioni interdittive di cui all'art. 9, comma 2, lett. c), d) ed e);
- all'art. 25 sono stati introdotti i gli artt. 314, comma 1, 316 e 323 c.p., rubricati: "Peculato", "Peculato mediante profitto dell'errore altrui" e "Abuso d'ufficio", per i quali è prevista la sanzione pecuniaria fino a 200 quote;
- l'art. 25-quinquiesdecies è stato arricchito mediante la previsione degli artt. 4, 5 e 10-quater del D.Lgs. n. 74/2000, rubricati rispettivamente "Dichiarazione infedele", per cui è prevista la sanzione pecuniaria fino a 300 quote, "Omessa dichiarazione" e "Indebita compensazione" per i quali è prevista la sanzione fino a 400 quote. Per tutti i reati sono previste anche le sanzioni interdittive di cui all'art. 9, comma 2, lett. c), d) ed e);
- è stato introdotto l'art. 25-sexiesdecies rubricato "Contrabbando", per il quale è prevista la sanzione pecuniaria fino a 200 quote, o fino a 400 se i diritti di confine superano i 100.000 euro, oltre le sanzioni interdittive di cui all'art. 9, comma 2, lett. c), d) ed e).

Nel corso del 2021, il D. Lgs. 8 novembre 2021, n. 184, oltre a modificare gli articoli 493 ter e 640 ter del codice penale e prevedere l'inserimento del nuovo articolo 493 quater c.p. rubricato "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti" ha introdotto il nuovo reato presupposto di cui all' art. 25-octies 1 "Delitti in materia di strumenti di pagamento diversi dai contanti".
In merito al Decreto attuativo della Direttiva Riciclaggio (D. Lgs. 8 novembre 2021, n. 195), si assiste ad un ampliamento dei reati presupposto dei delitti di ricettazione, riciclaggio,

autoriciclaggio ed impiego di beni o utilità di provenienza illecita di cui all' art 25-octies del D.Lgs. 231/2001, che comprende le contravvenzioni (punite con l'arresto superiore nel massimo ad 1 anno o nel minimo a 6 mesi) e, nel caso del riciclaggio e dell'autoriciclaggio, anche i delitti colposi.

Nel corso del 2022, la Legge n. 238/2021 rubricata "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea", ha introdotto alcune modifiche alle seguenti previsioni di reato richiamate dal D.Lgs. 231/2001:- art. 615-quater, art. 615-quinquies, art. 617-quater, art. 617 quinquies, art. 600-quater, art. 609-undecies, artt.184 e 185 D.Lgs. 58/1998. Sempre in argomento, la Legge 9 marzo 2022, n. 22 avente ad oggetto "Disposizioni in materia di reati contro il patrimonio culturale" ha inserito nel novero dell'elenco dei reati presupposto gli artt. 25 *septiesdecies* e 25 *duodevicies*.

Nel corso del 2023, fra i provvedimenti inseriti si annovera la Legge n. 137/2023 che ha convertito in Legge, con modificazioni il D.L. 10 agosto 2023 n. 105 (cd. Decreto Giustizia). La legge di conversione ha introdotto importanti modifiche al testo originario del Decreto Giustizia; sul versante penale, le principali novità hanno riguardato l'introduzione di nuovi delitti nel catalogo dei reati presupposto ex D. Lgs. 231/2001 oltre al potenziamento della tutela ambientale; inoltre, il 10 marzo 2023 è stato approvato il D. Lgs. n. 24, recante "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione". Il provvedimento è stato pubblicato in Gazzetta Ufficiale in data 15 marzo 2023 ed è entrato in vigore il 30 marzo 2023, in sostituzione appunto della Legge 30 novembre 2017, n. 179, anche detta Legge sul Whistleblowing.

SEZIONE SECONDA

2 Il Modello di Organizzazione, Gestione e Controllo di QUID INFORMATICA S.P.A.

2.1 Premessa

QUID INFORMATICA S.p.A. (di seguito anche "QUID" o la "Società") ha per oggetto la:

- progettazione, produzione e commercializzazione di macchine industriali e di relativi componenti, nonché gestione e realizzazione dei relativi servizi accessori di manutenzione e riparazione;
- progettazione, produzione e commercializzazione di prodotti e servizi informatici, concessione in licenza d'uso nonché fornitura dei relativi servizi di assistenza tecnica e operativa;
- assunzione di rappresentanza, per conto di società aventi sede legale in Italia o all'estero, di macchinari, pezzi di ricambio, di licenze d'uso e programmi per il settore informatico;
- progettazione, consulenza, commercializzazione e gestione di brevetti, modelli o utilità industriali e marchi;
- fornitura di servizi per l'"outsourcing" di sistemi informativi gestionali e tecnologici per le imprese;
- fornitura di "help desk" per sistemi informativi gestionali e tecnologici per le imprese;
- fornitura di servizi e programmi di contabilità aziendale che prevedano elaborazione elettronica dei dati, con esclusione delle relative attività di consulenza;
- assunzione di appalti pubblici e privati, per lo svolgimento delle attività di cui ai precedenti punti.

La Società, potrà, tra l'altro ed ai fini del paragrafo precedente:

- esercitare attività di direzione e coordinamento tecnico, gestionale e finanziario delle Società e/o enti direttamente o indirettamente partecipati, conformemente ai principi di corretta gestione societaria e imprenditoriale;
- acquistare e vendere partecipazioni ed interessenze in società ed enti aventi oggetto sociale affine, analogo o comunque connesso al proprio;
- rilasciare, nell'interesse delle società e/o enti direttamente o indirettamente partecipati, garanzie, reali e/o personali, tipiche e/o atipiche, ivi compresi contratti autonomi di garanzia e lettere di patronage;
- effettuare finanziamenti, sia a titolo gratuito, sia a titolo oneroso e svolgere attività di tesoreria accentrata a favore dei predetti enti e società;

- organizzare e gestire programmi di ricerca per l'innovazione tecnologica;
- effettuare ricerche di mercato, organizzazione e gestire banche dati;
- prestare servizi finanziari, amministrativi e commerciali a favore delle società e/o enti partecipanti.

La Società può inoltre compiere, sia in Italia sia all'estero, tutto quanto sia ritenuto necessario o utile, ad esclusivo giudizio dell'Organo Amministrativo, per il conseguimento dell'oggetto sociale.

E' in ogni caso escluso l'esercizio nei confronti del pubblico di qualunque attività dalla legge qualificata come "attività finanziaria" e, se non nei casi disciplinati dalla legge e nella piena osservanza di quanto ivi previsto, dall'attività professionale riservata e di quella che la legge riserva a particolari persone fisiche o giuridiche.

La Società adotta il modello di amministrazione e controllo tradizionale, che risulta adeguato a perseguire l'obiettivo di un appropriato bilanciamento dei poteri e una puntuale distinzione delle funzioni di gestione, demandata al Consiglio di Amministrazione, e di controllo, svolta dal Collegio Sindacale. La revisione legale dei conti è affidata ad una Società di revisione.

La Società è inoltre sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali, a tutela della propria posizione ed immagine, delle aspettative dei propri stakeholder e del lavoro dei propri dipendenti ed è consapevole dell'importanza di dotarsi di un sistema di controllo interno aggiornato ed idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri amministratori, dipendenti e partner.

A seguito della prima adozione del Modello nonché dei conseguenti aggiornamenti, la Società ha inteso ora provvedere ad una revisione del complessivo sistema di controllo interno in ottica 231 che, oltre a richiedere l'adozione di un nuovo Modello di Organizzazione, Gestione e Controllo e del Codice Etico, con un conseguente intervento sul sistema procedurale, volto alla formalizzazione di regole da applicare a processi e attività.

A tal fine, la Società ha avviato un progetto di analisi dei propri strumenti organizzativi, di gestione e di controllo, volto a verificare la corrispondenza dei principi comportamentali e dei protocolli già adottati alle finalità previste dal Decreto e ad implementare il Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/01. Attraverso l'adozione di un nuovo Modello, la Società intende perseguire i seguenti obiettivi:

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

***

2.2 Finalità del Modello

La Società si dota del presente Modello di organizzazione, gestione e controllo (di seguito anche "Modello 231" o "Modello") con l'obiettivo di prevenire la commissione dei reati riconducibili al Decreto da parte di esponenti della Società, apicali o sottoposti all'altrui direzione.

Il presente Modello ha lo scopo di costruire un sistema di controllo interno strutturato e organico, idoneo a prevenire la commissione dei reati previsti dal Decreto.

Come meglio precisato nel successivo paragrafo, nella predisposizione del presente documento la Società ha opportunamente tenuto presente, oltre alle prescrizioni del Decreto, anche alle Linee Guida predisposte da Confindustria.

La Società, in coerenza con l'impegno sempre profuso nella creazione e nel mantenimento di un sistema di governance caratterizzato da elevati standard etici e da un'efficiente gestione dell'attività aziendale, sin dagli anni immediatamente successivi all'entrata in vigore della normativa, ha svolto le necessarie attività di adeguamento al Decreto.

Sin dalla prima adozione, la Società ha desiderato perseguire i seguenti obiettivi:

- vietare comportamenti che possano integrare le fattispecie di reato di cui al Decreto;
- diffondere la consapevolezza che, dalla violazione del Decreto, delle prescrizioni contenute nel Modello e/o dei principi del Codice Etico possa derivare l'applicazione di misure sanzionatorie (pecuniarie e/o interdittive) anche a carico della Società;
- diffondere una cultura d'impresa improntata alla legalità, nella consapevolezza dell'espressa riprovazione da parte della Società di ogni comportamento contrario alla legge, ai regolamenti, alle disposizioni interne e, in particolare, alle disposizioni contenute nel presente Modello e nel Codice Etico;
- dare evidenza dell'esistenza di una struttura organizzativa efficace e coerente con il modello operativo adottato, con particolare riguardo alla chiara attribuzione dei poteri, alla formazione delle decisioni e alla loro trasparenza e motivazione, ai controlli, preventivi e successivi, sugli atti e le attività, nonché alla correttezza e veridicità dell'informativa interna ed esterna;
- consentire alla Società, grazie ad un sistema di presidi di controllo e ad una costante azione di monitoraggio sulla corretta attuazione di tale sistema, di prevenire e/o contrastare tempestivamente la commissione dei reati rilevanti ai sensi del Decreto.

La Società si è inoltre impegnata ad effettuare costantemente gli opportuni aggiornamenti al fine di:

- integrare i contenuti del Modello a seguito di interventi legislativi che introducono nuove categorie di reati-presupposto;
- accogliere gli orientamenti della giurisprudenza formati nel tempo in materia di responsabilità da reato degli enti;
- recepire l'evoluzione delle *best practice* e delle Linee Guida di riferimento;

- riflettere in modo adeguato l'evoluzione del business e degli assetti organizzativi della Società, così come definiti e formalizzati il 3 ottobre 2019.

2.3 Le Linee Guida di Confindustria

Come in precedenza evidenziato, nella stesura del presente Modello la Società si è ispirata alle Linee Guida emanate da Confindustria ed approvate dal Ministero della Giustizia. In particolare sono stati seguiti i seguenti principi fondamentali:

- individuazione delle aree di rischio, volta a verificare in quale area/settore aziendale sia possibile la realizzazione dei reati previsti dal Decreto;
- predisposizione di un sistema di controllo in grado di prevenire i rischi di realizzazione di tali reati attraverso l'adozione di appositi protocolli;
- individuazione delle componenti più rilevanti del sistema di controllo:
  - codice etico;
  - sistema organizzativo;
  - procedure;
  - poteri autorizzativi e di firma;
  - sistemi di controllo e gestione;
  - comunicazione al personale e sua formazione
- individuazione dei principi di controllo applicabili:
  - verificabilità, documentabilità, coerenza e congruenza di ogni operazione; applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo);
  - documentazione dei controlli;
  - previsione di un adeguato sistema sanzionatorio per la violazione delle norme interne e delle procedure previste dal Modello;
  - obblighi di informazione da e verso l'Organismo di Vigilanza.

Si riportano di seguito le principali modifiche e integrazioni della versione delle Linee guida risalente a marzo 2014, e in particolare della Parte generale riguardano: i) il nuovo capitolo sui lineamenti della responsabilità da reato e la sintesi dei reati presupposto; ii) il sistema disciplinare e i meccanismi sanzionatori; iii) l'Organismo di Vigilanza, con particolare riferimento alla sua composizione; iv) il fenomeno dei gruppi di imprese. La Parte speciale, dedicata all'approfondimento dei reati presupposto attraverso appositi *case study*, è stata oggetto di una profonda rivisitazione, volta non soltanto a trattare le nuove fattispecie di reato presupposto, ma anche a introdurre un metodo di analisi schematico e di più facile fruibilità.

La nuova versione delle Linee Guida (giugno 2021) adegua il precedente testo del 2014 alle novità legislative, giurisprudenziali e della prassi applicativa nel frattempo intervenute, mantenendo la distinzione tra le due Parti, generale e speciale.

Eventuali difformità che si dovessero riscontrare tra il Modello e il contenuto delle Linee Guida

non inficiano di per sé la validità del Modello stesso, in quanto questo descrive la specifica realtà di QUID INFORMATICA e quindi ben può discostarsi per specifiche esigenze di tutela e prevenzione dalle Linee Guida, che per loro natura hanno carattere generale.

Inoltre, la predisposizione del Modello è stata condotta sulla base degli aggiornamenti apportati al Decreto, dei principali casi giudiziari accertati, delle opinioni dottrinali, delle *best-practice* nonché delle principali normative, anche volontarie, che indicano principi guida e standard di controllo per un sistema di organizzazione interno.

2.4 Destinatari

Si considerano soggetti destinatari delle prescrizioni del Modello, ai sensi del Decreto e nell'ambito delle rispettive competenze, i componenti degli organi sociali, il management e i dipendenti di QUID INFORMATICA, nonché tutti coloro che operano nell'ambito delle Attività Sensibili in nome o per conto della Società (ad es. consulenti, revisori ecc.).

2.5 Struttura del Modello

La Società, in coerenza con i principi etici e di governance ai quali ha orientato le proprie regole di comportamento, ha adottato il presente Modello, articolato in:

- ***Parte Generale***, contenente una sintetica descrizione del quadro normativo, integrata dal dettaglio delle fattispecie di reato (Allegato A), la composizione e il funzionamento dell'Organismo di Vigilanza, i flussi informativi, le sanzioni applicabili in caso di violazioni delle regole e delle prescrizioni contenute nel Modello, le regole che disciplinano le modalità di diffusione ed aggiornamento del Modello;
- ***Parti Speciali***, contenenti una descrizione delle diverse fattispecie di reato-presupposto concretamente e potenzialmente rilevanti per la Società, in ragione delle sue caratteristiche peculiari, alle attività a rischio-reato, alle regole comportamentali e ai principi di controllo specifici.

Il Modello è completato dal **Codice Etico**, che ne costituisce parte integrante e che ha lo scopo di esprimere principi di "deontologia aziendale" sui quali la Società richiama l'osservanza da parte di tutti i Dipendenti, Organi Sociali, Consulenti e Partner, sin dalla prima adozione.

Sono infine da ritenersi parti integranti del Modello: i) l'Organigramma aziendale, ii) il Sistema di procure vigenti, iii) Procedure, circolari, comunicati e note organizzative, oltre ai iv) documenti relativi alla *data protection* e *privacy* (compliance GDPR), ed alla v) valutazione dei rischi (salute e sicurezza sul lavoro).

2.6 Presupposti del Modello

Nella predisposizione del Modello, la Società ha tenuto conto del proprio sistema di controllo interno, al fine di verificarne la capacità a prevenire le fattispecie di reato previste dal Decreto nelle attività identificate a rischio, nonché dei principi etico-sociali cui QUID INFORMATICA si attiene nello svolgimento delle proprie attività.

Più in generale, il sistema di controllo interno di QUID INFORMATICA è orientato a

garantire, con ragionevole certezza, il raggiungimento di obiettivi operativi, di informazione e di conformità e in particolare:

- l'*obiettivo operativo* riguarda l'efficacia e l'efficienza della Società nell'impiegare le risorse, nel proteggersi dalle perdite, nel salvaguardare il patrimonio aziendale. Il sistema di controllo è volto, inoltre, ad assicurare che il personale operi per il perseguimento degli obiettivi aziendali, senza anteporre altri interessi a quelli di QUID INFORMATICA.
- l'*obiettivo di informazione* si traduce nella predisposizione di rapporti tempestivi ed affidabili per il processo decisionale sia interno che esterno all'organizzazione aziendale;
- l'*obiettivo di conformità* garantisce, invece, che tutte le operazioni ed azioni siano condotte nel rispetto delle leggi e dei regolamenti, dei requisiti prudenziali e delle procedure aziendali interne.

Il sistema di controllo interno di QUID INFORMATICA si basa sui seguenti elementi:

- integrità e valori che ispirano l'agire quotidiano dell'intera azienda, esprimendo altresì lo stile del Board e del Management aziendale;
- sistema organizzativo formalizzato e chiaro nell'attribuzione dei poteri e delle responsabilità (incluso il concetto di *accountability*), in coerenza con il raggiungimento degli obiettivi assegnati;
- attenzione al sistema delle competenze del personale, alla luce degli obiettivi perseguiti;
- identificazione, valutazione e gestione dei rischi che potrebbero compromettere il raggiungimento degli obiettivi aziendali;
- definizione di procedure aziendali, parte del complessivo sistema normativo della Società, che esplicitano i controlli posti a presidio dei rischi e del raggiungimento degli obiettivi prefissati;
- sistemi informativi idonei a supportare i processi aziendali e il complessivo sistema di controllo interno (informatici, di reporting, ecc.);
- processi di comunicazione interna e formazione del personale;
- sistemi di monitoraggio a integrazione dei controlli di linea.

Tutti i Destinatari, nell'ambito delle funzioni svolte, sono responsabili della definizione e del corretto funzionamento del sistema di controllo attraverso i *controlli di linea*, costituiti dall'insieme delle attività di controllo che i singoli uffici svolgono sui loro processi.

2.7 Elementi fondamentali del Modello

Con riferimento alle esigenze individuate nel Decreto, gli elementi fondamentali sviluppati dalla Società nella definizione del Modello, possono essere così riassunti:

- mappatura delle attività sensibili, con esempi di possibili modalità di realizzazione dei reati e dei processi strumentali/ funzionali potenzialmente associabili alla commissione dei reati richiamati dal Decreto, da sottoporre, pertanto, ad analisi e monitoraggio periodico;
- previsione di specifici presidi di controllo relativi ai processi strumentali/ funzionali ritenuti a maggiore rischio potenziale di commissione di reato, diretti a regolamentare espressamente la formazione e l'attuazione delle decisioni della Società, al fine di fornire indicazioni specifiche sul sistema di controlli preventivi in relazione alle singole fattispecie di illecito da prevenire;
- identificazione dei principi etici e delle regole comportamentali volte alla prevenzione di condotte che possano integrare le fattispecie di reato previste, sancite nel Codice Etico adottato dalla Società e, più in dettaglio, nel presente Modello;
- nomina di un Organismo di Vigilanza al quale sono attribuiti specifici compiti di vigilanza sull'efficace attuazione ed effettiva applicazione del Modello ai sensi dell'art. 6, punto b), del Decreto;
- attuazione di un sistema sanzionatorio idoneo a garantire l'effettività del Modello, contenente le disposizioni disciplinari applicabili in caso di mancato rispetto delle misure indicate nel Modello medesimo;
- svolgimento di un'attività di informazione, sensibilizzazione, divulgazione e formazione sui contenuti del Modello, nonché sulle regole comportamentali valide a tutti i livelli aziendali;
- modalità per l'adozione e l'effettiva applicazione del Modello nonché per le necessarie modifiche o integrazioni dello stesso (cfr. sez. 8 "Aggiornamento del Modello).

2.8 Individuazione delle attività "a rischio"

L'art. 6, comma 2, lett. a) del Decreto prevede espressamente che il Modello individui le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati di cui al medesimo Decreto.

In aderenza al dettato normativo e tenuto conto degli orientamenti metodologici contenuti nelle Linee Guida di riferimento, sulla base del quadro aggiornato dei processi aziendali di QUID INFORMATICA vengono identificate in relazione alle singole fattispecie di reato previste dal Decreto 231 (attraverso un'analisi puntuale dei processi interessati) le *attività sensibili* rilevanti per la Società.

Tale analisi dei rischi è sottoposta periodicamente all'esame dell'OdV per la valutazione di eventuali esigenze di modifica e/o integrazione del Modello 231.

La mappatura degli ambiti operativi di potenziale esposizione della Società ai diversi rischi - reato 231, è accompagnata dalla rilevazione degli specifici elementi di controllo esistenti,

nonché dalla definizione di eventuali iniziative di integrazione e/o rafforzamento dei presidi in essere (alla luce degli esiti dell'apposita *gap analysis*).

In base alle indicazioni e alle risultanze della complessiva attività di analisi sopra delineata, le singole funzioni aziendali implementano – previa valutazione dei rischi individuati e definizione delle politiche di gestione degli stessi – strumenti normativi relativi alle attività a rischio, in coerenza con il sistema normativo dell'Azienda.

2.9 Principi e presidi generali di controllo interno

Per tutte le attività a rischio, valgono i seguenti principi generali:

- esplicita formalizzazione delle norme comportamentali;
- chiara, formale e conoscibile descrizione ed individuazione delle attività, dei compiti e dei poteri attribuiti a ciascuna Funzione e alle diverse qualifiche e ruoli professionali;
- precisa descrizione delle attività di controllo e loro tracciabilità;
- adeguata segregazione di ruoli operativi e ruoli di controllo;
- sistemi informativi integrati e orientati, oltre alla segregazione delle funzioni, anche alla protezione delle informazioni in essi contenute, con riferimento sia ai sistemi gestionali e contabili che ai sistemi utilizzati a supporto delle attività operative connesse al business.

In particolare, devono essere perseguiti i seguenti presidi organizzativo-gestionali di carattere generale.

Norme comportamentali

- Esistenza di un Codice Etico che descriva regole comportamentali di carattere generale a presidio delle attività svolte.

Definizioni di ruoli e responsabilità

- La regolamentazione interna deve declinare ruoli e responsabilità delle strutture organizzative a tutti i livelli, descrivendo in maniera omogenea le attività proprie di ciascuna struttura;
- Tale regolamentazione deve essere resa disponibile e conosciuta all'interno dell'organizzazione.

Protocolli e norme interne

- Le attività sensibili devono essere regolamentate, in modo coerente e congruo, attraverso gli strumenti normativi aziendali, così che in ogni momento si possano identificare le modalità operative di svolgimento delle attività, dei relativi controlli e le responsabilità di chi ha operato;
- Deve essere individuato e formalizzato un Responsabile per ciascuna attività sensibile, tipicamente coincidente con il responsabile della struttura organizzativa competente per la gestione dell'attività stessa.

Segregazione dei compiti

- All'interno di ogni processo aziendale sensibile, devono essere separate le funzioni o i soggetti incaricati della decisione e della sua attuazione rispetto a chi la registra e chi la controlla;
- Non deve esservi identità soggettiva tra coloro che assumono o attuano le decisioni, coloro che elaborano 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 autorizzativi e di firma

- Deve essere definito un sistema di deleghe all'interno del quale vi sia una chiara identificazione e una specifica assegnazione di poteri e limiti ai soggetti che operano impegnando la Società e manifestando la sua volontà;
- I poteri organizzativi e di firma (deleghe, procure e connessi limiti di spesa) devono essere coerenti con le responsabilità organizzative assegnate;
- Le procure devono essere coerenti con il sistema interno delle deleghe;
- Devono essere previsti meccanismi di pubblicità delle procure assegnate ai primi livelli verso gli interlocutori esterni;
- Devono essere previste modalità di revoca delle procure e delle deleghe assegnate.
- Il processo di attribuzione delle deleghe deve identificare, tra l'altro:
  - la posizione organizzativa che il delegato ricopre in ragione dello specifico ambito di operatività della delega;
  - l'accettazione espressa da parte del delegato o del subdelegato delle funzioni delegate e conseguente assunzione degli obblighi conferiti;
  - i limiti di spesa attribuiti al delegato.
- Le deleghe sono attribuite secondo i principi di:
  - autonomia decisionale e finanziaria del delegato;
  - idoneità tecnico-professionale del delegato;
  - disponibilità autonoma di risorse adeguate al compito e continuità delle prestazioni.

Attività di controllo e tracciabilità

- Nell'ambito degli strumenti normativi della Società devono essere formalizzati i controlli operativi e le loro caratteristiche (responsabilità, evidenza, periodicità);
- La documentazione afferente alle attività sensibili deve essere adeguatamente formalizzata e riportare la data di compilazione, presa visione del documento e la firma riconoscibile del compilatore/supervisore; la stessa deve essere archiviata in luogo idoneo alla conservazione, al fine di tutelare la riservatezza dei dati in essi contenuti e di evitare danni, deterioramenti e smarrimenti;
- Devono essere ricostruibili la formazione degli atti e i relativi livelli autorizzativi, lo sviluppo delle operazioni, materiali e di registrazione, con evidenza della loro

motivazione e della loro causale, a garanzia della trasparenza delle scelte effettuate;

- Il Responsabile dell'attività deve produrre e mantenere adeguati report di monitoraggio che contengano evidenza dei controlli effettuati e di eventuali anomalie;
- Deve essere prevista, laddove possibile, l'adozione di sistemi informatici che garantiscano la corretta e veritiera imputazione di ogni operazione, o di un suo segmento, al soggetto che ne è responsabile e ai soggetti che vi partecipano. Il sistema deve prevedere l'impossibilità di modifica (non tracciata) delle registrazioni;
- I documenti riguardanti l'attività della Società, ed in particolare i documenti o la documentazione informatica riguardanti attività sensibili, sono archiviati e conservati, a cura della funzione competente, con modalità tali da non permettere la modificazione successiva, se non con apposita evidenza;
- L'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate in base alle norme interne o ad un loro delegato, al Collegio Sindacale od organo equivalente o ad altri organi di controllo interno, alla Società di revisione e all'Organismo di Vigilanza.

Con riferimento ai principi specifici di controllo della Società, in ciascuna Parte Speciale del presente Modello sono riportati quelli effettivamente previsti dall'operatività aziendale di QUID INFORMATICA. Per i processi il cui svolgimento è totalmente o parzialmente esternalizzato sono formalizzati specifici *contratti di service* che prevedono:

- l'identificazione di un responsabile delle attività di controllo sulle attività esternalizzate;
- l'espletamento, da parte del suddetto responsabile, dei controlli e delle verifiche previste dal ruolo (verifica della corretta esecuzione contrattuale, verifica tecnico-operativa ed economica dei servizi e delle forniture, ecc.).

Inoltre, è altresì previsto l'inserimento, nei suddetti contratti, di clausole specifiche nell'ambito delle quali le società s'impegnano, nei confronti l'una dell'altra, al rispetto più rigoroso dei propri Modelli, con particolare riguardo ai processi dei Modelli che presentano rilevanza ai fini delle attività gestite mediante contratto di service e della sua esecuzione.

Con tali clausole, si impegnano altresì a darsi reciprocamente notizia di eventuali violazioni, che dovessero verificarsi e che possano avere attinenza con il contratto e/o la sua esecuzione e più in generale, ad astenersi, nell'espletamento delle attività oggetto del rapporto contrattuale, da comportamenti e condotte che possano integrare una qualsivoglia fattispecie di reato contemplata dal Decreto.

SEZIONE TERZA

3 Organismo di Vigilanza

3.1 Identificazione dell'Organismo di Vigilanza

L'art. 6, comma 1, del Decreto prevede che la funzione di vigilare e di curare l'aggiornamento del Modello sia affidata ad un Organismo di Vigilanza interno all'ente che, dotato di autonomi poteri di iniziativa e di controllo, eserciti in via continuativa i compiti ad esso rimessi, anche in ragione delle regole di funzionamento interno dell'Organismo medesimo, che potranno essere formalizzate in apposito regolamento interno.

L'Organismo di Vigilanza è nominato dal Consiglio di Amministrazione. I membri dell'Organismo di Vigilanza sono scelti tra soggetti qualificati, con competenze in ambito legale, amministrativo-contabile e/o di gestione d'impresa, provvisti dei requisiti di:

- *autonomia e indipendenza*: detto requisito è assicurato dalla composizione plurisoggettiva dell'Organismo di Vigilanza, dall'assenza di alcun riporto gerarchico all'interno dell'organizzazione e dalla facoltà di reporting all'amministratore;
- *professionalità*: requisito garantito dal bagaglio di conoscenze professionali, tecniche e pratiche, di cui dispongono i componenti dell'Organismo di Vigilanza;
- *continuità d'azione*: con riferimento a tale requisito, l'Organismo di Vigilanza è tenuto a vigilare costantemente, attraverso poteri di indagine, sul rispetto del Modello, a curarne l'attuazione e l'aggiornamento, rappresentando un riferimento costante per tutto il personale della Società.

In caso di nomina di componenti esterni, gli stessi non dovranno avere rapporti commerciali con la Società che possano configurare ipotesi di conflitto di interesse.

In ogni caso, i componenti dell'Organismo di Vigilanza sono - e saranno - scelti tra soggetti che non abbiano rapporti di parentela con i soci e con gli Amministratori.

In ossequio alle prescrizioni del Decreto, alle indicazioni espresse dalle Linee Guida di Confindustria, all'organizzazione della Società e agli orientamenti della giurisprudenza, il Consiglio di Amministrazione ha ritenuto di istituire in questa fase un Organismo di Vigilanza Monocratico, composto da un professionista esterno o in alternativa dal Presidente del Collegio Sindacale di QUID INFORMATICA.
In particolare, nel caso di nomina di un componente esterno alla compagine societaria sarà individuato in soggetto di comprovata esperienza e competenza, nelle tematiche di natura legale, di organizzazione aziendale, responsabilità amministrativa di impresa nonché in materia economica.

L'Organismo di Vigilanza si avvale del supporto della funzione di Internal Audit, ove prevista, o della funzione Controllo di Gestione, di eventuali consulenti esterni nonché di quelle altre funzioni aziendali della Società che di volta in volta si rendono utili per il perseguimento del proprio fine.

Nello svolgimento delle proprie funzioni, l'Organismo di Vigilanza riferisce esclusivamente al Consiglio di Amministrazione.

All'Organismo di Vigilanza sono attribuiti autonomi poteri di spesa che prevedono l'impiego di un budget annuo adeguato, approvato con delibera del Consiglio di Amministrazione, su proposta dell'Organismo di Vigilanza. L'Organismo di Vigilanza potrà impegnare risorse che eccedono i propri poteri di spesa, che devono essere autorizzate direttamente dal Consiglio di Amministrazione.

In ogni caso, alla scadenza del mandato, ciascun componente rimane in carica sino alla nomina del nuovo Organismo di Vigilanza da parte del Consiglio di Amministrazione.

Sono comunque fatti salvi i casi di dimissioni di un membro dell'OdV che hanno efficacia immediata.

3.2 Cause di ineleggibilità, decadenza e revoca dell'Organismo di Vigilanza

Costituiscono cause di *ineleggibilità e decadenza* dei componenti dell'OdV:

- aver ricoperto funzioni di amministratore esecutivo, nei tre esercizi precedenti alla nomina quale membro dell'Organismo di Vigilanza, in imprese sottoposte a fallimento, liquidazione coatta amministrativa o procedure equiparate;
- aver riportato una sentenza di condanna, anche non passata in giudicato, ovvero di applicazione della pena su richiesta (c.d. patteggiamento), in Italia o all'estero, in relazione a reati della stessa indole di quelli previsti dal Decreto.

E' altresì motivo di decadenza con effetto immediato il venir meno, nel corso del periodo di carica, dei requisiti che hanno determinato l'individuazione dei componenti stessi all'atto delle nomine in virtù della carica societaria o del ruolo organizzativo rivestito.

Costituiscono cause di *revoca* dei componenti dell'OdV:

- l'omessa o insufficiente vigilanza da parte dell'OdV risultante da una sentenza di condanna, anche non passata in giudicato, emessa nei confronti della Società ai sensi del Decreto 231 ovvero da sentenza di applicazione della pena su richiesta (c.d. patteggiamento);
- il grave inadempimento delle funzioni e/o doveri dell'Organismo di Vigilanza.

La revoca è disposta con delibera del Consiglio di Amministrazione e sentiti gli altri membri dell'OdV ed il Collegio Sindacale.

In caso di decadenza o revoca di uno dei componenti dell'OdV, il Consiglio di Amministrazione provvede tempestivamente alla sua sostituzione.

3.3 Poteri e funzioni dell'Organismo di Vigilanza

Il compito di vigilare sul funzionamento e l'osservanza del Modello Organizzativo è svolto dall'OdV anche attraverso l'esame di tutti i rapporti, ovvero da altre strutture aziendali con compiti di controllo, nella materia riguardante il Decreto, le quali provvedono a consegnarli accorpati durante le riunioni periodiche.

Inoltre, è facoltà dell'Organismo di vigilanza di modificare le tempistiche, le modalità ed il contenuto dei flussi informativi che le funzioni aziendali sono tenute ad inviare.

Il compito di curare l'aggiornamento del Modello Organizzativo, in relazione all'evolversi della struttura organizzativa e a necessità sopravvenute, è svolto dall'OdV mediante raccomandazioni / suggerimenti rappresentate alla Società, la quale provvede a sottoporle all'approvazione del Consiglio di Amministrazione.

Il Consiglio di Amministrazione mette a disposizione dell'OdV adeguate risorse aziendali in relazione ai compiti affidatigli e, nel predisporre il budget aziendale, approva – sulla base di quanto proposto dall'Organismo di Vigilanza stesso - una dotazione adeguata di risorse finanziarie della quale l'OdV potrà disporre per ogni esigenza necessaria al corretto svolgimento dei propri compiti.

In relazione alle attività sensibili, l'OdV presenta un Piano Generale di attività e per le verifiche periodiche, finalizzate a valutare l'effettiva applicazione, l'adeguatezza e la funzionalità degli strumenti normativi in termini di presidi atti a prevenire la commissione dei reati previsti dall'impianto normativo, si avvale del programma della funzione Internal Audit – ove prevista - richiedendo ex ante specifici approfondimenti o valutando le risultanze e richiedendo ex post eventuali chiarimenti e maggiori informazioni. Tale programma di verifiche è suscettibile di variazioni sulla base di eventuali richieste di intervento da parte dell'Organismo di Vigilanza ed a fronte di criticità emerse nel corso dell'attività di analisi dei flussi o delle segnalazioni. Resta ferma, in ogni caso, la facoltà di attivare, laddove ritenuto opportuno, verifiche a sorpresa.

Qualora lo ritenga opportuno, l'OdV, ai fini dell'attuazione e dell'aggiornamento del Modello, può avvalersi - nel rispetto delle procedure aziendali in materia di affidamento di incarichi professionali - anche di professionisti esterni, dandone preventiva informazione al Consiglio di Amministrazione.

In coerenza con l'attività di direzione e coordinamento nell'ambito della complessiva *Governance* 231, l'OdV di QUID INFORMATICA, nel rispetto dell'autonomia e della riservatezza delle informazioni e dei limiti imposti da disposizioni di legge, prevede:

- lo svolgimento di un monitoraggio sull'adozione del Modello 231, in ottica di rilevazione della complessiva coerenza dell'approccio delineato nei diversi documenti rispetto al Modello Organizzativo;
- l'attivazione di flussi informativi sistematici e strutturati, di contenuto generale verso l'OdV;
- il recepimento delle iniziative relative allo studio e all'approfondimento di tematiche afferenti al Decreto 231, la sua interpretazione e la sua applicazione all'interno della Società.

3.4 Reporting dell'Organismo di Vigilanza nei confronti degli Organi Societari

L'OdV riferisce in merito alle attività di propria competenza nei confronti del Consiglio di Amministrazione e del vertice societario e in particolare:

- ove necessario ed in occasione di eventi particolarmente rilevanti, direttamente nei confronti del Consiglio di Amministrazione e del management societario;
- su base annuale, nei confronti del Consiglio di Amministrazione e del Collegio Sindacale, contenente tra l'altro un report sull'attuazione del Modello. L'OdV può essere convocato in qualsiasi momento dal Consiglio di Amministrazione e dal Collegio Sindacale per riferire in merito al funzionamento e all'osservanza del Modello o a situazioni specifiche.

3.5 Flussi informativi nei confronti dell'Organismo di Vigilanza

Il Decreto enuncia (art. 6, comma, 2, lett. d.), tra le esigenze che il Modello deve soddisfare, l'istituzione di obblighi informativi nei confronti dell'Organismo di Vigilanza.

A tal fine è previsto che il personale dipendente informi tempestivamente l'OdV delle possibili violazioni e/o dei comportamenti non conformi a quanto stabilito dal Modello Organizzativo e dalle procedure aziendali, mediante un canale dedicato di comunicazione con l'Organismo di Vigilanza, consistente in:

- casella di posta elettronica: organismodivigilanza@quidinfo.it
- servizio postale: Quid Informatica S.p.A. Via Pratese 162, 50145 Firenze – c.a. Organismo di Vigilanza di Quid Informatica Spa.

Le segnalazioni dovranno pervenire in forma scritta. Nel caso in cui la segnalazione sia presentata tramite il servizio postale, per tutela di riservatezza, il nominativo del segnalante deve essere inserito in una busta chiusa all'interno della busta contenente la segnalazione. La segnalazione sarà costudita e protocollata in modalità tecniche tali da garantire la massima sicurezza.

La Società s'impegna a garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione per motivi collegati direttamente o indirettamente alla segnalazione. In ogni caso sarà assicurata la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

Sono previste sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate, in linea con il sistema sanzionatorio contenuto nella Sezione Quarta della presente Parte Generale, applicabile in caso di violazione delle disposizioni del presente Modello.

Oltre alle segnalazioni sopra indicate, devono essere obbligatoriamente e tempestivamente trasmesse all'Organismo di Vigilanza le informazioni concernenti:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, tributaria o da qualsiasi altra autorità, anche amministrativa, che vedano il coinvolgimento della Società o di soggetti apicali, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto, fatti salvi gli obblighi di riservatezza e segretezza legalmente imposti;
- richieste di informazioni o invio di prescrizioni, relazioni o lettere da parte di Autorità di

Vigilanza, ed ogni altra documentazione che scaturisce da attività di ispezione delle stesse svolte e rientranti negli ambiti di pertinenza del D.Lgs. 231/2001;

- comunicazioni all'Autorità Giudiziaria che riguardano potenziali o effettivi eventi illeciti che possono essere riferiti alle ipotesi di cui al D.Lgs. 231/2001;
- richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario, in particolare per i reati ricompresi nel Decreto;
- esiti delle attività di controllo svolte dai responsabili delle diverse funzioni aziendali dalle quali siano emersi fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto o del Modello;
- modifiche nel sistema delle deleghe e delle procure, modifiche statutarie o modifiche dell'organigramma aziendale;
- notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- segnalazione di infortuni gravi (incidenti mortali o con prognosi superiore a 40 giorni) occorsi a dipendenti, appaltatori e/o collaboratori presenti nei luoghi di lavoro della Società.

In aggiunta, i responsabili dei vari uffici/funzioni aziendali trasmettono all'Organismo le variazioni intervenute nei processi e nelle procedure, nonché gli interventi correttivi e migliorativi pianificati con conseguente stato di realizzazione.

Tutte le informazioni, la documentazione e le segnalazioni raccolte nell'espletamento dei compiti istituzionali devono essere archiviate e custodite, per almeno tre anni, dall'Organismo di Vigilanza, avendo cura di mantenere riservati i documenti e le informazioni acquisite, anche nel rispetto della normativa sulla privacy.

L'OdV riceve altresì, periodicamente, flussi informativi da parte delle varie strutture aziendali a fronte delle attività a rischio ritenute di maggiore rilievo, anche in coerenza delle procedure aziendali in essere.

Infine, annualmente l'OdV è destinatario della conferma da parte dei responsabili dei vari uffici/funzioni aziendali della coerenza, completezza e aggiornamento delle attività a rischio individuate, delle politiche di gestione degli stessi, nonché della effettiva attuazione delle procedure aziendali rilevanti ai fini del Decreto, in coerenza con il complessivo sistema normativo della Società.

SEZIONE QUARTA

4 Sistema sanzionatorio

4.1 Premessa

La definizione di un sistema sanzionatorio, applicabile in caso di violazione delle disposizioni del presente Modello, costituisce condizione necessaria per garantire l'efficace attuazione del Modello stesso, nonché presupposto imprescindibile per consentire alla Società di beneficiare dell'esimente dalla responsabilità amministrativa (*ex* art. 6, comma 2, lett. e) del Decreto).

L'applicazione delle sanzioni disciplinari prescinde dall'instaurazione e dagli esiti di un procedimento penale eventualmente avviato nei casi in cui la violazione integri un'ipotesi di reato rilevante ai sensi del D.Lgs. 231/2001.

Le sanzioni comminabili sono diversificate in ragione della natura del rapporto tra l'autore della violazione e la Società, nonché del rilievo e gravità della violazione commessa e del ruolo e responsabilità dell'autore. Più in particolare, le sanzioni comminabili sono diversificate tenuto conto del grado di imprudenza, imperizia, negligenza, colpa o dell'intenzionalità del comportamento relativo all'azione/omissione, tenuto altresì conto di eventuale recidiva, nonché dell'attività lavorativa svolta dall'interessato e della relativa posizione funzionale, unitamente a tutte le altre particolari circostanze che possono aver caratterizzato il fatto.

In generale, le violazioni possono essere ricondotte ai seguenti:

a) comportamenti che integrano una *mancata attuazione colposa delle prescrizioni* del Modello e/o del Codice Etico ivi comprese direttive, procedure o istruzioni aziendali;

b) comportamenti che integrano una *trasgressione dolosa delle prescrizioni* del Modello e/o del Codice Etico tale da compromettere il rapporto di fiducia tra l'autore e la Società in quanto preordinata in modo univoco a commettere un reato;

nonché classificate come segue:

- la violazione, anche con condotte omissive e in eventuale concorso con altri, delle previsioni del Modello o delle procedure stabilite per l'attuazione del medesimo e del Codice Etico;
- la redazione, eventualmente in concorso con altri, di documentazione alterata o non veritiera;
- l'agevolazione, mediante condotta omissiva, di violazioni del Modello e del Codice Etico e della redazione da parte di altri, di documentazione alterata o non veritiera;
- l'omessa redazione della documentazione prevista dal Modello o dalle procedure stabilite per l'attuazione dello stesso.

Il procedimento sanzionatorio è in ogni caso gestito dalla funzione e/o dagli organi societari competenti che riferiscono al riguardo all'OdV.

Di seguito si riportano le sanzioni divise per tipologia di rapporto tra il soggetto e la Società.

4.2 Sanzioni per i lavoratori dipendenti

In relazione al personale dipendente, la Società si attiene alle prescrizioni di cui all'art. 7 della Legge n. 300/1970 (Statuto dei lavoratori) ed alle previsioni contenute nei Contratti Collettivi Nazionali di Lavoro applicabili, sia con riguardo alle sanzioni comminabili che alle modalità di esercizio del potere disciplinare.

L'inosservanza - da parte del personale dipendente - delle disposizioni del Modello e/o del Codice Etico, nonché di tutta la documentazione che di essi forma parte, costituisce inadempimento alle obbligazioni derivanti dal rapporto di lavoro *ex* art. 2104 cod. civ. ed illecito disciplinare.

Più in particolare, l'adozione, da parte di un dipendente della Società, di un comportamento qualificabile, in base a quanto indicato al comma precedente, come illecito disciplinare, costituisce inoltre violazione dell'obbligo del lavoratore di eseguire con la massima diligenza i compiti allo stesso affidati, attenendosi alle direttive della Società, così come previsto dai vigenti CCNL applicabili.

Alla notizia di violazione del Modello, verrà promossa un'azione disciplinare finalizzata all'accertamento della violazione stessa. In particolare, nella fase di accertamento verrà previamente contestato al dipendente l'addebito e gli sarà, altresì, garantito un congruo termine di replica. Una volta accertata la violazione, sarà irrogata all'autore una sanzione disciplinare proporzionata alla gravità della violazione commessa.

Al personale non dirigente possono essere comminate le sanzioni previste dal CCNL applicabile, che - a titolo esemplificativo - possono essere le seguenti: rimprovero verbale, ammonizione scritta, multa, sospensione dal servizio, licenziamento con preavviso o per giusta causa.

4.3 Sanzioni nei confronti dei dirigenti

In caso di violazione, da parte di Dirigenti, delle procedure interne previste dal presente Modello o di adozione, nell'espletamento di attività a rischio, di un comportamento non conforme alle prescrizioni del Modello stesso, l'OdV ne informerà il Consiglio di Amministrazione e il Collegio Sindacale. Si provvederà ad applicare, nei confronti dei responsabili, le idonee misure in conformità a quanto previsto dai CCNL applicabili. Laddove la violazione sia tale da far venir meno il rapporto di fiducia, la sanzione è individuata nel licenziamento per giusta causa.

4.4 Misure nei confronti degli Amministratori e dei Sindaci

L'OdV informa il Consiglio di Amministrazione e il Collegio Sindacale delle segnalazioni aventi ad oggetto violazioni del Modello o del Codice Etico da parte degli Amministratori e dei Sindaci che non siano state ritenute manifestamente infondate affinché provvedano a investire della questione gli organi da essi presieduti. Il Consiglio di Amministrazione potrà proporre alla successiva assemblea la revoca del mandato per giusta causa. Si applicano gli articoli 2392 e 2407 del codice civile.

4.5 Misure nei confronti dei membri dell'OdV

In caso di violazioni del presente Modello da parte di uno o più componenti dell'OdV, gli altri

componenti dell'OdV ovvero uno qualsiasi tra i sindaci informano immediatamente il Consiglio di Amministrazione che, previa contestazione della violazione e preso atto delle argomentazioni difensive eventualmente addotte, assume gli opportuni provvedimenti tra cui, ad esempio, la revoca dell'incarico.

4.6 Misure nei confronti di Fornitori, Collaboratori, Partner e Consulenti

La violazione da parte di Collaboratori esterni alla Società, di Soci in Società ed enti partecipati dalla Società, di Fornitori di beni e servizi e Partner, delle norme previste dal Decreto e/o del Codice Etico può essere causa di risoluzione del contratto. Tale circostanza è esplicitamente contenuta in ciascun contratto in cui la Società sia parte.

La violazione va denunciata senza indugio al vertice societario da chi la rileva. Se i vertici societari ritengono che la denuncia sia fondata, ordinano l'immediata risoluzione del contratto e ne danno notizia all'OdV Essi danno ugualmente notizia all'OdV dei casi in cui essi non procedano a risolvere il contratto perché ritengono non fondata la denuncia o perché la risoluzione sarebbe di grave danno per la Società.

La risoluzione del contratto comporta l'accertamento dei danni che la Società abbia eventualmente subito e la conseguente azione di risarcimento.

SEZIONE QUINTA

5 La disciplina in materia di Whistleblowing

La disciplina della tutela del segnalante illeciti e irregolarità di cui è venuto a conoscenza nell'ambito di un rapporto di lavoro privato, nota come Whistleblowing, è stata inserita all'interno del D.Lgs. 231/2001 per opera della Legge 179/2017.
Tale disposto normativo, ha previsto nell'ambito delle società private, l'integrazione dell'articolo 6 del D.Lgs. 231/2001 con l'obbligo per la Società di prevedere dei canali che consentano la segnalazione di illeciti, garantendo la massima riservatezza in merito all'identità del segnalante, nonché l'individuazione di sanzioni specifiche per chi effettui segnalazioni che si rivelino prive di fondamento o per i casi in cui i soggetti deputati alla verifica delle segnalazioni violino gli obblighi di riservatezza del segnalante.
Il 10 marzo 2023 è stato approvato il D. Lgs. n. 24, recante "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione". Il provvedimento è stato pubblicato in Gazzetta Ufficiale in data 15 marzo 2023 ed è entrato in vigore il 30 marzo 2023, in sostituzione appunto della Legge 30 novembre 2017, n. 179, anche detta Legge sul Whistleblowing.
L'istituto del Whistleblowing, di origine anglosassone, nasce con l'obiettivo di prevedere un sistema di tutele nei confronti di coloro che segnalano irregolarità e/o illeciti di cui siano venuti a conoscenza in ambito lavorativo.
Con l'entrata in vigore del D. Lgs. 24/2023 è stato introdotto nell'ordinamento italiano un sistema integrato di regole che si rivolge sia al settore pubblico che a quello privato, con lo scopo di incentivare le segnalazioni di illeciti che pregiudichino l'interesse pubblico, ovvero l'integrità dell'ente.

Le suddette segnalazioni potranno avere ad oggetto non solo le condotte illecite rilevanti ai sensi del Decreto e le violazioni del Modello Organizzativo, ma anche tutte le violazioni del diritto nazionale (illeciti amministrativi, contabili e penali) e del diritto europeo.
L'ambito di applicazione della disciplina in commento è stato ampliato ed è ora caratterizzato da un regime di obblighi e tutele che differisce a seconda dell'oggetto della violazione, della natura pubblica o privata del soggetto di appartenenza del segnalante, c.d. Whistleblower, nonché delle dimensioni dell'ente e dell'applicabilità a quest'ultimo del Decreto.
Le tutele previste per i casi di segnalazione degli illeciti di cui sopra sono state rafforzate e operano sostanzialmente su due livelli, essendo state introdotte la procedura di segnalazione mediante canali esterni e la divulgazione pubblica, che si affiancano alla procedura di segnalazione mediante canali interni, già esistente.
Al fine di incentivare il ricorso alla procedura interna, agli enti privati è richiesta l'attivazione di un canale comunicativo interno, mediante il quale i whistleblowers possano presentare segnalazioni circostanziate di condotte illecite, che permetta una gestione tempestiva ed efficace delle segnalazioni e che garantisca, al contempo, la riservatezza del segnalante e della persona coinvolta o menzionata nella segnalazione, nonché del contenuto della segnalazione e della documentazione ad essa allegata. In caso di elusione del divieto di atti di ritorsione o discriminatori nei confronti del segnalante per motivi collegati direttamente o indirettamente alla segnalazione, ovvero in caso di abuso, l'ente deve comminare adeguate sanzioni, oltre a quanto disposto dal Sistema Sanzionatorio, nei confronti di chi violi le suddette misure di tutela del segnalante nonché nei confronti di chi effettua, con dolo o colpa grave, segnalazioni che si rivelano infondate.
Nell'ambito della gestione del canale di segnalazione interna, la persona o l'ufficio interno ovvero il soggetto esterno (di seguito anche "gestore delle segnalazioni"), all'uopo incaricato, in qualità di destinatario delle segnalazioni effettuate dai whistleblowers, spetta di vigilare sul corretto adempimento delle disposizioni normative in materia.
Al riguardo, il Gestore delle segnalazioni all'uopo incaricato:

- verifica l'adeguatezza dei canali informativi, predisposti in applicazione della disciplina sul Whistleblowing;
- vigila sul rispetto del divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante;
- gestisce il processo di analisi e valutazione delle segnalazioni;
- vigila sul corretto utilizzo dei canali informativi da parte dei segnalanti al fine di disincentivare il ricorso allo strumento comunicativo per segnalare fatti o circostanze che si rivelino infondati.

Il corretto funzionamento del sistema di Whistleblowing presuppone che i soggetti interessati ne siano adeguatamente informati e che questi siano messi in condizione di usufruire dei sistemi di segnalazione dei reati o delle irregolarità.
Pertanto, il Gestore delle segnalazioni ha il compito di sovraintendere alla formazione dei dipendenti e dei collaboratori della Società, di concerto con le altre funzioni aziendali responsabili in materia, informandoli su:

- le novità introdotte dalla normativa in materia;
- le sanzioni disciplinari previste a tutela dei segnalanti che integrano il sistema disciplinare già previsto nel Modello;

- il corretto uso dei canali informativi.

Il Decreto attribuisce, infine, un ruolo di controllo, anche sugli enti privati, all'Autorità Nazionale Anti Corruzione, che gestisce il canale esterno e interviene in caso di ritorsioni in funzione dei whistleblowers. La Società ha adottato la Policy Whistleblowing e attivato il nuovo canale di segnalazione interna, raggiungibile on-line al seguente indirizzo: https://gruppoquid.integrityline.com/ ("Canale"), scegliendo dall'apposito menù a tendina la Società del Gruppo per la quale si intende effettuare la segnalazione.

Il Canale è stato creato per consentire a chiunque di condividere in sicurezza ogni informazione che riguardi gravi illeciti relativi a violazioni di norme di legge e/o del sistema di controllo interno (es. Codice Etico, Modello Organizzativo ex D. Lgs. 231/2001, policy e procedure interne), che si sono verificate o è molto probabile che si verifichino nell'organizzazione. Il Segnalante dovrà avere fondato motivo di ritenere che le informazioni condivise siano vere (principio di buona fede) e che rientrino in una delle materie di cui al capoverso precedente.

Rimangono attivi i canali di segnalazione già presenti nel Modello verso l'OdV.

La Società garantisce la piena riservatezza dell'identità del segnalante e degli altri soggetti interessati dalla segnalazione, e qualsiasi informazione fornita sarà trattata con la massima diligenza. Non saranno accettate segnalazioni inviate in mala fede, così come non sarà tollerata nessuna misura ritrosiva verso il segnalante o persone a lui/lei vicine.

SEZIONE SESTA

6 Informazione e formazione del personale e diffusione del Modello

La conoscenza effettiva dei contenuti del Modello da parte delle risorse presenti in azienda e di tutti i soggetti che hanno rapporti con QUID INFORMATICA è condizione necessaria per assicurare l'efficacia e la corretta funzionalità del Modello stesso. A tal fine, l'adozione del Modello, nonché delle relative integrazioni e/o modifiche, è comunicata a tutte le risorse presenti in azienda al momento dell'approvazione da parte del Consiglio di Amministrazione. È inoltre previsto che tutte le risorse neoassunte ricevano, contestualmente all'assunzione, il Codice Etico e che a tutto al personale sia assicurato l'accesso alla sezione dedicata al Modello all'interno del portale aziendale.

Il personale, ad ogni livello, deve essere consapevole delle possibili ripercussioni dei propri comportamenti e delle proprie azioni rispetto alle regole prescritte dal Modello. È pertanto prevista la divulgazione delle regole di condotta del Modello mediante una specifica attività di formazione e di aggiornamento di dipendenti e collaboratori.

La partecipazione ai programmi di formazione sul Modello è obbligatoria ed il controllo sulla frequenza e sui contenuti del programma è demandato all'OdV, che svolge altresì un controllo circa la validità e la completezza dei piani formativi previsti ai fini di un'appropriata diffusione, di un'adeguata cultura dei controlli interni, dell'organigramma aziendale e di una chiara consapevolezza dei ruoli e responsabilità delle varie funzioni aziendali.

La formazione ha l'obiettivo di diffondere tra il personale la conoscenza dei reati, le fattispecie configurabili, i presidi specifici delle aree di competenza degli operatori, nonché richiamare l'attenzione sull'importanza di una corretta applicazione del Modello di

Organizzazione, Gestione e Controllo. I contenuti formativi sono aggiornati in relazione all'evoluzione della normativa esterna e del Modello; pertanto in caso di modifiche rilevanti si procederà ad una integrazione dei contenuti medesimi, assicurandone altresì la fruizione.

In ogni caso, l'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D.Lgs. 231/2001 e le prescrizioni del Modello adottato sarà differenziata nei contenuti e nelle modalità in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della Società.

Infine, la Società provvede alla divulgazione presso i clienti, i fornitori, i partner e i consulenti delle regole di condotta ivi contenute.

SEZIONE SETTIMA

7 Codice etico

Al fine di definire con chiarezza e trasparenza l'insieme dei valori ai quali si ispira per raggiungere i propri obiettivi, la Società adotta il Codice Etico la cui osservanza è imprescindibile per il corretto funzionamento, affidabilità, reputazione ed immagine, ed i cui principi costituiscono i fondamenti per il successo e lo sviluppo attuale e futuro della stessa.

Quid Informatica riconosce l'importanza della responsabilità etico-sociale nella conduzione delle attività aziendali e s'impegna al rispetto dei legittimi interessi dei propri stakeholder e della collettività in cui opera. Contestualmente richiede a tutti i dipendenti e a tutti coloro che cooperano all'esercizio delle attività d'impresa il rispetto delle regole aziendali e dei precetti stabiliti nel Codice.

Le regole contenute nel Codice Etico integrano i principi di comportamento che gli amministratori, i dirigenti, i dipendenti e tutti i collaboratori sono tenuti ad osservare, anche in conformità alle regole di diligenza cui sono obbligati per legge il mandatario ed ogni prestatore di lavoro.

SEZIONE OTTAVA

8 Aggiornamento del Modello

La verifica sull'aggiornamento e sull'efficace attuazione del Modello compete al Consiglio di Amministrazione, cui è pertanto attribuito il potere di apportare modifiche al Modello, che lo eserciterà mediante delibera con le modalità previste per la sua adozione.

L'attività di aggiornamento, intesa sia come integrazione sia come modifica, è volta a garantire l'adeguatezza e l'idoneità del Modello, valutate rispetto alla funzione preventiva di commissione dei reati previsti dal D.Lgs. 231/2001.

Compete, invece, all'Organismo di Vigilanza la concreta verifica circa la necessità od opportunità di procedere all'aggiornamento del Modello, facendosi promotore di tale esigenza nei confronti del Consiglio di Amministrazione. L'Organismo di Vigilanza, nell'ambito dei poteri ad esso conferiti conformemente agli art. 6, comma 1, lett. b) e art. 7, comma 4, lett. a) del Decreto, ha la responsabilità di formulare raccomandazioni/ suggerimenti in ordine all'aggiornamento e all'adeguamento del presente Modello.

In ogni caso il Modello deve essere tempestivamente modificato e integrato dal Consiglio di Amministrazione, anche su proposta e previa consultazione dell'Organismo di Vigilanza, quando siano intervenute:

- violazioni ed elusioni delle prescrizioni in esso contenute che ne abbiano evidenziato l'inefficacia o l'incoerenza ai fini della prevenzione dei reati;
- significative modificazioni all'assetto interno della Società e/o delle modalità di svolgimento delle attività di impresa;
- modifiche normative ed evoluzioni giurisprudenziali.

Le modifiche, gli aggiornamenti e le integrazioni del Modello devono essere sempre comunicati all'Organismo di Vigilanza.

PARTE SPECIALE

QUID INFORMATICA S.P.A.

1 Premessa

Le attività sensibili individuate

L'analisi svolta nel corso dei lavori di adozione del presente Modello ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie richiamate nel novero dei reati che fondano la responsabilità amministrativa degli enti a norma del D.Lgs 231/01.

Come anticipato nella Parte Generale del presente Modello (in particolare nel paragrafo 2.1), ed al quale si rimanda, la Società tra le attività svolte, quelle ritenute sensibili sono:

- Pagamenti;
- Gestione finanziaria e relativi flussi monetari e finanziari;
- Supporto amministrativo nella gestione delle partecipate;
- Gestione incassi e pagamenti;
- Acquisto di beni, servizi e consulenze;
- Gestione fornitori;
- Bilancio, contabilità e adempimenti fiscali;
- Rapporti con soci, sindaci e revisori;
- Partecipazione a gare;
- Iniziative di marketing/ commerciale;
- Comunicazione, ricerca e sviluppo, responsabilità sociale d'impresa;
- Assunzione e gestione del personale;
- Gestione delle attività relative ad omaggi e regalie;
- Gestione del sistema informativo aziendale;
- Gestione sistemi IT;
- Ispezione dell'autorità pubblica;
- Gestione della salute e sicurezza.

1.1 Il sistema dei controlli

Il sistema dei controlli adottato dalla Società con riferimento ai processi sensibili individuati prevede:

- *principi di controllo "generali"*, presenti in tutti i processi sensibili;
- *principi di controllo "specifici"*, applicati ai singoli processi sensibili;

Oltre ai principi di controllo sopra enunciati, QUID INFORMATICA prevede ulteriori presìdi di controllo che garantiscono un monitoraggio più stringente delle attività aziendali svolte.

QUID INFORMATICA, inoltre, prevede di istituire in futuro un Ufficio Affari Legali in grado di fornire supporto rispetto a tutte le attività svolte. Rispetto a tutti i processi sensibili sopra elencati, sarà previsto comunque il coinvolgimento di una struttura legale esterna e dell'Ufficio Affari Legali, quando sarà istituito, ogni qualvolta tale intervento sia necessario, opportuno o anche semplicemente utile.

1.2 Principi di controllo generali

La Parte Speciale prevede l'espresso obbligo, a carico dei destinatari, di rispettare i seguenti principi di controllo generali:

- osservanza di tutte le leggi e regolamenti, sia nazionali che di origine comunitaria;
- instaurazione e mantenimento dei rapporti con la Pubblica Amministrazione secondo

criteri di massima correttezza e trasparenza.

In conformità a tali principi:

- è fatto espresso divieto di effettuare o acconsentire ad elargizioni o promesse di denaro, beni o altre utilità di qualsiasi genere ad esponenti della Pubblica Amministrazione, incaricati di pubblico servizio o a soggetti terzi da questi indicati o che abbiano con questi rapporti diretti o indiretti di qualsiasi natura, al fine di ottenere favori indebiti o benefici in violazione di nome di legge;
- in particolare, non devono essere recepite eventuali segnalazioni provenienti da esponenti della Pubblica Amministrazione ai fini dell'assunzione di personale, o comunque dell'interessamento alla assunzione o collocazione di questo presso terzi;
- non devono essere recepite segnalazioni provenienti dalla Pubblica Amministrazione relative all'indicazione di consulenti, agenti o *partners* commerciali, affinché la Società se ne avvalga nello svolgimento della sua attività;
- non devono essere prese in considerazione richieste di sponsorizzazioni, contributi elettorali, di trattamenti privilegiati provenienti da esponenti, rappresentanti o funzionari della Pubblica Amministrazione, in particolare se formulate in occasione di specifici rapporti di affari, operazioni commerciali;
- è fatto espresso divieto di distribuire omaggi, regali o prestazioni di qualsiasi natura al di fuori di quanto previsto dalla prassi aziendale o da apposita procedura (vale a dire, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche promozionali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore indebiti o non dovuti nella conduzione di qualsiasi attività). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei paesi in cui l'elargizione di doni rappresenta una prassi diffusa) o a loro familiari o a soggetti da loro indicati, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore;
- è fatto espresso divieto di effettuare prestazioni in favore dei *partners,* agenti e collaboratori esterni che non trovino adeguata giustificazione nel contesto del rapporto professionale costituito con gli stessi;
- è fatto espresso divieto di scegliere collaboratori esterni, agenti o *partners* per ragioni diverse da quelle connesse alla necessità, professionalità ed economicità e riconoscere ad essi compensi che non trovino adeguata giustificazione nel contesto del rapporto in essere e nel valore effettivo della prestazione;
- è fatto espresso divieto di presentare dichiarazioni non veritiere o incomplete, o comunque indurre in errore, organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- è fatto espresso divieto di destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
- è fatto espresso divieto di ricevere denaro o altre utilità a vantaggio della Società da privati che possano trarre un vantaggio da decisioni o scelte assunte nell'ambito dell'attività di QUID INFORMATICA.

Ai fini dell'attuazione dei comportamenti di cui sopra:

- gli impegni con la Pubblica Amministrazione sono gestiti ed intrapresi solo da responsabili aziendali, agenti collaboratori o *partners* dotati di apposita e specifica procura;
- gli eventuali accordi contrattuali con gli agenti sono definiti per iscritto con l'evidenza di tutte le condizioni dell'accordo stesso e sono proposti, verificati ed approvati dai soggetti aziendali competenti nel rispetto del principio di separazione dei compiti;
- gli incarichi conferiti ai collaboratori esterni sono anch'essi redatti per iscritto, con l'indicazione del compenso pattuito e sono proposti, verificati ed approvati dai soggetti aziendali competenti nel rispetto del principio di separazione dei compiti espresso nella prassi aziendale e nelle procedure interne adottate;
- la liquidazione dei compensi è effettuata in modo trasparente, è documentata ed è sempre ricostruibile *ex post*;
- le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, contengono elementi assolutamente veritieri e sono complete, al fine di attestare la sussistenza di tutte le condizioni richieste per l'accesso al finanziamento e l'assenza di cause ostative; in caso di ottenimento degli stessi, è formalizzato ed archiviato un apposito rendiconto;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) curano la corretta attuazione degli adempimenti e riferiscono immediatamente all'OdV eventuali situazioni di irregolarità.

Per ciò che concerne, più nello specifico, l'ambito amministrativo-contabile e finanziario, QUID INFORMATICA impone ai Destinatari del Modello:

- di comportarsi in modo corretto, trasparente e conforme alle norme di legge, di regolamento, alle procedure esistenti, ai principi generalmente riconosciuti di tenuta della contabilità, in tutte le attività finalizzate alla redazione del bilancio, delle altre comunicazioni sociali, al fine di fornire ai soci, ai terzi, alle istituzioni e al pubblico un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
- di assicurare il corretto funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo sulla gestione, nonché la libera, consapevole e corretta formazione della volontà assembleare. A tal fine è fatto divieto di:
  - porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque costituiscano ostacolo allo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale;
  - determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà;
- di effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche, non

frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate. A tal fine, è fatto espresso divieto di:

- esporre nelle comunicazioni previste dalle leggi e dalla normativa di settore nei confronti delle Pubbliche Autorità dati non veritieri, ovvero occultare fatti rilevanti relativi alla sua situazione economica, patrimoniale e finanziaria, ovvero omettere informazioni rilevanti;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle dette funzioni di controllo, ad esempio nel corso di ispezioni.

1.3 Principi di controllo specifici

I principi di controllo di carattere specifico sono descritti nel prosieguo del documento in corrispondenza di ogni fattispecie di reato e processo sensibile. In termini indicativi, le aree di focalizzazione di tali controlli sono le seguenti:

- **regolamentazione del processo e segregazione dei compiti:** identificazione delle attività poste in essere dalle varie funzioni e ripartizione delle stesse tra chi esegue, chi autorizza e chi controlla, in modo tale che nessuno possa gestire in autonomia l'intero svolgimento di un processo;
- **esistenza di procedure/ linee guida/ prassi operative:** esistenza di disposizioni, procedure formalizzate o prassi operative idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili, nonché modalità di archiviazione della documentazione rilevante;
- **tracciabilità e verificabilità ex-post delle transazioni tramite adeguati supporti documentali/ informatici:** verificabilità ex post del processo di decisione, autorizzazione e svolgimento dell'attività sensibile, anche tramite apposite evidenze archiviate e, in ogni caso, dettagliata disciplina della possibilità di cancellare o distruggere le registrazioni effettuate;
- **esistenza di un sistema di deleghe coerente con le responsabilità organizzative assegnate:** formalizzazione di poteri di firma e di rappresentanza coerenti con le responsabilità organizzative e gestionali assegnate, chiaramente definiti e conosciuti all'interno della Società.

2 Fattispecie di reato-presupposto

In questa sezione della Parte Speciale, dopo una descrizione dei reati applicabili, sono identificate le attività sensibili e indicate le regole comportamentali e i principi di controllo specifici che tutti i Destinatari del presente Modello devono adottare ed applicare al fine di prevenire il verificarsi dei reati.

***

PARTE SPECIALE A – REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

(artt. 24 e 25 del D.Lgs. 231/2001)

La presente Parte Speciale "A" si riferisce ai reati realizzabili nell'ambito dei rapporti tra QUID INFORMATICA e la Pubblica Amministrazione e si applica alle tipologie di reati di corruzione, anche tra privati, ed altri reati nei rapporti con la Pubblica Amministrazione.

In particolare la presente Parte Speciale, dopo una descrizione dei reati applicabili, identifica le attività sensibili e indica le regole comportamentali e i principi di controllo specifici, che tutti i Destinatari del presente Modello devono adottare ed applicare al fine di prevenire il verificarsi dei reati.

A.1 Reati applicabili alla Società

I reati contro la Pubblica Amministrazione hanno come presupposto l'instaurazione di rapporti con soggetti pubblici e/o lo svolgimento di attività concretanti una pubblica funzione o un pubblico servizio.

Con riferimento ai reati di corruzione tra privati e istigazione alla corruzione tra privati, pur appartenendo alla categoria dei reati societari, sono stati inseriti all'interno della presente Parte Speciale al fine di garantire una maggiore uniformità nella trattazione dei fenomeni corruttivi che potrebbero manifestarsi nell'operativa aziendale.

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

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

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano, di altri enti pubblici o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi di pubblico interesse cui erano destinate. Tenuto conto che il momento di consumazione del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che non vengano destinati alle finalità per cui erano stati erogati.

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

Tale ipotesi di reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di

dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute – si ottengano, per sé o per altri e senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione europea. In questo caso, non rileva il corretto utilizzo delle erogazioni (come invece previsto dall'art. 316-bis), poiché il reato si concretizza nel momento stesso dell'ottenimento dei finanziamenti in modo indebito. Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie dell'art. 640-bis c.p., con riferimenti a quei casi in cui la condotta non integri gli estremi più gravi della truffa ai danni dello Stato.

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

L'ipotesi di reato di cui all'art. 318 c.p. si configura nel caso in cui un pubblico ufficiale, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altre utilità o ne accetta la promessa. Ai fini dell'applicazione del reato, ai pubblici ufficiali ed agli incaricati di pubblico servizio vanno equiparati membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri previsti dall'art. 322-bis, c.p.

Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p e art. 319-bis.)

L'ipotesi di reato di cui all'art. 319 c.p., si configura nel caso in cui il pubblico ufficiale, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri d'ufficio, riceve, per sé o per un terzo, denaro od altre utilità, o ne accetta la promessa.

La pena è aumentata se il fatto di cui all'articolo 319 c.p. ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene, nonché il pagamento o il rimborso di tributi. (319 bis).Ai fini dell'applicazione del reato, ai pubblici ufficiali ed agli incaricati di pubblico servizio vanno equiparati membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri previsti dall'art. 322-bis, c.p.

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

Tale ipotesi di reato si configura nel caso in cui i fatti indicati negli artt. 318 e 319 c.p. sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo. Il reato di corruzione in atti giudiziari può essere commesso nei confronti di giudici o membri del Collegio Arbitrale competenti a giudicare sul contenzioso/arbitrato nell'interesse dell'Ente (compresi gli ausiliari e i periti d'ufficio), e/o di rappresentanti della Pubblica Amministrazione, quando questa sia una parte nel contenzioso, al fine di ottenere illecitamente decisioni giudiziali e/o stragiudiziali favorevoli. Ai fini dell'applicazione del reato, ai pubblici ufficiali ed agli incaricati di pubblico servizio vanno equiparati membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di

Stati esteri previsti dall'art. 322-bis, c.p.

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

Tale ipotesi di reato si configura, salvo che il fatto costituisca più grave reato, nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induca taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altre utilità.

Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.)

Le disposizioni di cui agli artt. 318 e 319 c.p. si applicano anche all'incaricato di pubblico servizio. Ai fini dell'applicazione del reato, ai pubblici ufficiali ed agli incaricati di pubblico servizio vanno equiparati membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri previsti dall'art. 322-bis, c.p.

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

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

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

Tale ipotesi di reato si configura nei confronti di chiunque offra o prometta denaro o altre utilità non dovuti ad un pubblico ufficiale o incaricato di pubblico servizio per indurlo a compiere, omettere o ritardare un atto del suo ufficio, ovvero a compiere un atto contrario ai propri doveri, qualora l'offerta o la promessa non sia accettata. Questa fattispecie si realizza nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, un Pubblico Ufficiale o un incaricato di pubblico servizio rifiuti l'offerta illecitamente avanzatagli.

Ai fini dell'applicazione del reato, ai pubblici ufficiali ed agli incaricati di pubblico servizio vanno equiparati membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri previsti dall'art. 322-bis, c.p.

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

Questa fattispecie si realizza nel caso in cui chiunque, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio, 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, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri. Al contempo è punita la controparte responsabile della promessa o dazione di denaro o altra

utilità.

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

La fattispecie di cui all'art. 640 c.p. prevede un reato comune che può essere commesso da chiunque. Il fatto che costituisce reato consiste nel procurare a sé o ad altri un ingiusto profitto a danno di un altro soggetto, inducendo taluno in errore mediante artifici o raggiri. In particolare, nella fattispecie richiamata dall'art. 24 del D.Lgs. 231/2001 (i.e. art. 640 comma 2, n. 1 c.p.), rilevano i fatti commessi a danno dello Stato o di altro ente pubblico.

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

Tale ipotesi di reato si configura nel caso in cui la truffa (di cui all'art. 640 c.p.) sia posta in essere per conseguire indebitamente, contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

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

Tale ipotesi di reato si configura nel caso in cui, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, si procura un ingiusto profitto per sé o altri, con danno altrui.

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

Integra il reato la condotta di amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili, sindaci, liquidatori, nonché dei soggetti sottoposti alla direzione o vigilanza dei medesimi che, avendo accettato per sé o per altri denaro o altra utilità, o la relativa promessa, compiono od omettono un atto contrario agli obblighi inerenti al loro ufficio o agli obblighi di fedeltà, cagionando nocumento alla società.

Il comma 3 punisce anche la condotta del corruttore (c.d. reato di corruzione tra privati attiva), con le medesime pene previste per i corrotti. Solo tale reato, e non anche quello commesso dai corrotti, costituisce presupposto della responsabilità amministrativa degli enti, se commesso nell'interesse dell'ente al quale il corruttore appartiene e con nocumento per la società di appartenenza del soggetto corrotto.

Istigazione alla corruzione tra privati (art. 2635-bis)

Tale fattispecie di reato punisce chiunque offra o prometta 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, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo.

Peculato (limitatamente al primo comma – art. 314 c.p.)

Tale ipotesi di reato si perfezione quando un pubblico ufficiale o l'incaricato di un pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di danaro o di altra cosa mobile altrui, se ne appropria.

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

Tale reato si configura quando il pubblico ufficiale o l'incaricato di un pubblico servizio, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità.

Il reato in esame potrebbe verificarsi con condotte analoghe a quelle esposte per il Peculato (art. 314) ma giovandosi dell'errore altrui.

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

Tale fattispecie di reato si configura laddove, salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità (decreto semplificazioni - D.L. 16 luglio 2020, n. 76), ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto

Turbata libertà degli incanti (art. 353 c.p.)

Chiunque con violenza o minaccia o con doni promesse collusioni o altri mezzi fraudolenti impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche amministrazioni ovvero ne allontana gli offerenti è punito con la reclusione da sei mesi a cinque anni e con la multa da euro 103 a euro 1.032.

Se il colpevole è persona preposta dalla legge o dall'autorità agli incanti o alle licitazioni suddette la reclusione è da uno a cinque anni e la multa da euro 516 a euro 2.065.

Le pene stabilite in questo articolo si applicano anche nel caso di licitazioni private per conto di privati dirette da un pubblico ufficiale o da persona legalmente autorizzata ma sono ridotte alla metà.

Turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.)

Salvo che il fatto costituisca più grave reato chiunque con violenza o minaccia o con doni promesse collusioni o altri mezzi fraudolenti turba il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione è punito con la reclusione da sei mesi a cinque anni e con la multa da euro 103 a euro 1.032.

In relazione ai delitti introdotti nel novero dei reati-presupposto ex D.Lgs. 231/2001 ed in particolare all'art. 25 dal D.Lgs 75/2020, potrebbero divenire rilevanti anche sulla base del concorso nel reato (c.d. proprio) del pubblico funzionario, come altre fattispecie di reato contro la P.A. presenti nel D.Lgs. 231/2001 fra cui concussione e indebita induzione a dare o promettere utilità.

Inoltre, la responsabilità amministrativa degli enti è prevista anche quando i delitti di cui ai

commi da 1 a 3 dell'art. 25 del Decreto 231 sono stati commessi dalle persone indicate negli articoli 320 c.p. (persona incaricata di pubblico servizio) e 322-bis c.p. (membri della Corte penale internazionale o degli organi delle Comunità europee e funzionari delle Comunità europee e di Stati esteri).

A.2 Attività sensibili

I reati previsti dagli artt. 24 e 25 del D.Lgs. 231/2001 sono configurabili nell'ambito dei rapporti, sia in Italia sia all'estero, con la Pubblica Amministrazione e con tutti quei soggetti che possono essere qualificati pubblici ufficiali o incaricati di pubblico servizio.

In relazione ai reati previsti dagli artt. 24 e 25 del D. Lgs. 231/2001 sono state individuate le seguenti attività sensibili:

- Gestione del finanziamento conseguito in termini di modalità di utilizzo dello stesso, con riferimento alle modalità previste per la realizzazione del progetto e la veridicità di quanto dichiarato in fase di rendicontazione;
- Predisposizione, sottoscrizione e trasmissione della documentazione di richiesta di ottenimento di un finanziamento pubblico (ad es. finalizzati all'attuazione di piani formativi aziendali);
- Gestione dei rapporti con i Funzionari degli Enti competenti in materia di adempimenti societari presso il Tribunale, la CCIAA e l'Ufficio del Registro;
- Gestione dei rapporti con i Funzionari pubblici competenti nell'ambito delle attività di controllo, accertamento e ispezione sull'osservanza degli obblighi previsti dalla normativa ambientale;
- Gestione dei rapporti con gli Enti Pubblici (es. Regioni, Comuni) ai fini dell'espletamento degli adempimenti necessari all'organizzazione di eventi promozionali;
- Gestione dei flussi telematici con Enti Pubblici che implichino l'accesso ai siti/piattaforme istituzionali (ad es. INPS, Agenzia delle Entrate);
- Gestione dei rapporti con clienti pubblici anche attraverso la rete di agenti e i centri media, con particolare riferimento alla partecipazione a gare pubbliche bandite dalla PA, sia in modalità tradizionale che smaterializzata;
- Gestione dei rapporti con le autorità di controllo (ASL, Vigili del fuoco, Ispettorato del Lavoro) in materia di tutela della salute e sicurezza sul lavoro, in sede di verifiche ispettive.
- Gestione dei rapporti con i funzionari della Guardia di Finanza, l'Agenzia delle Entrate e gli altri Enti competenti in materia fiscale, tributaria e societaria, anche in occasione di verifiche, ispezioni e accertamenti;
- Gestione dei rapporti e delle informazioni dirette alle Autorità Amministrative Indipendenti e con le Autorità di Vigilanza anche in occasione di verifiche, ispezioni ed accertamenti;
- Gestione dei rapporti con Funzionari competenti (INPS, INAIL, ASL, Direzione Provinciale del Lavoro ecc.) per l'osservanza degli obblighi previsti dalla normativa di riferimento:
    - Predisposizione delle denunce relative a costituzione, modifica ed estinzione

del rapporto di lavoro;

- Elenchi del personale attivo, assunto e cessato presso l'INAIL;
- Controlli e verifiche circa il rispetto dei presupposti e delle condizioni previste dalla normativa vigente;
- Predisposizione ed esecuzione dei pagamenti verso lo Stato o altri Enti pubblici.

- Gestione delle posizioni creditorie e delle iniziative di recupero delle stesse (in relazione a ipotesi di stralci di credito, parziali o totali), nonché le transazioni commerciali remissive a fronte di disservizi e contestazioni;
- Selezione e assunzione del personale dipendente e dei collaboratori; Gestione di promozioni, avanzamenti di carriera, aumenti, assegnazione di "fringe benefits" a favore di dipendenti;
- Gestione dei rapporti con i Funzionari Pubblici in occasione di verifiche circa il rispetto dei presupposti e delle condizioni (esempio: piano formativo, durata, rispetto dei limiti d'età, ecc.) richieste dalla normativa vigente per le assunzioni agevolate e le assunzioni obbligatorie (categorie protette);
- Gestione dei flussi monetari e finanziari, con particolare riferimento a:
  - Apertura e/o chiusura e gestione dei c/c bancari e riconciliazioni bancarie;
  - Gestione degli incassi;
  - Gestione del credito: verifica dello stato dei crediti e del pagamento delle relative fatture;
  - Gestione dei pagamenti;
  - Gestione della piccola cassa;
  - Gestione rimborsi spese.
- Selezione, negoziazione, stipula ed esecuzione di contratti di acquisto, ivi compresi gli appalti di lavori, riferita a soggetti privati, con particolare riferimento al ricevimento di beni e attività finalizzate all'attestazione di avvenuta prestazione dei servizi e di autorizzazione al pagamento specialmente in relazione ad acquisti di natura immateriale, tra cui: consulenze e incarichi professionali; sponsorizzazioni; spese di rappresentanza; attività di sviluppo di software e servizi;
- Gestione dei rapporti con i giudici competenti, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito delle cause di varia natura o dei relativi ricorsi (civile, penale, amministrativo, giuslavoristico e tributario) con particolare riferimento alla nomina dei legali;

Con riferimento al reato di corruzione tra privati (art. 25-ter del D.Lgs. 231/2001 – artt. 2635 e 2365-bis c.c.), sono state individuate le seguenti attività sensibili:

- Selezione e assunzione del personale dipendente e dei collaboratori;
- Gestione dei flussi monetari e finanziari, con particolare riferimento a:
  - Apertura e/o chiusura e gestione dei c/c bancari e riconciliazioni bancarie
  - Gestione degli incassi

- Gestione del credito: verifica dello stato dei crediti e del pagamento delle relative fatture
- Gestione dei pagamenti
- Gestione della piccola cassa.

- Selezione, negoziazione, stipula ed esecuzione di contratti di acquisto, ivi compresi gli appalti di lavori, riferita a soggetti privati, con particolare riferimento al ricevimento di beni e attività finalizzate all'attestazione di avvenuta prestazione dei servizi e di autorizzazione al pagamento specialmente in relazione ad acquisti di natura immateriale, tra cui: consulenze e incarichi professionali; sponsorizzazioni; spese di rappresentanza; attività di sviluppo di software e servizi;
- Gestione dei rapporti con parti terze per la definizione di situazioni pre-contenziose o di contenziosi intrapresi nei confronti della Società;
- Iniziative di marketing e commerciale;
- Gestione dei rapporti con la rete distributiva (ad es. centri media);
- Gestione dei rapporti con clienti privati con particolare riferimento alle richieste di offerta pervenute da clienti privati per l'acquisto di prodotti e/o servizi.

A.3 Regole Comportamentali

Sono Destinatari dei seguenti divieti di carattere generale i componenti degli organi sociali, i dirigenti e i dipendenti di QUID INFORMATICA. In relazione ai consulenti, ai fornitori e ai partner devono essere previste nei relativi contratti apposite clausole contrattuali che rendano vincolanti le disposizioni del presente Modello agli stessi.

Ai Destinatari è fatto divieto di porre in essere o tentare di porre in essere, concorrere o dare causa a comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, anche per interposta persona, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del D.Lgs. 231/2001); sono altresì proibite le violazioni ai principi ed alle procedure aziendali indicate nella presente Parte Speciale.

Al fine di evitare il verificarsi dei suddetti reati previsti dal D. Lgs. 231/2001, a tutti i Destinatari, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti della Società, è fatto nello specifico divieto di:

- Tenere rapporti con la Pubblica Amministrazione, se non per ragioni d'ufficio e solo se deputati secondo l'organigramma della Società, le comunicazioni organizzative (che indicano anche le funzioni ed ambiti di responsabilità attribuiti), le job description di ciascuno o eventuali procure e deleghe;
- Dare seguito a qualunque richiesta di indebiti vantaggi o tentativi di concussione o induzione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza, dandone immediata segnalazione al proprio Responsabile; Promettere o versare, direttamente o per interposta persona, somme o beni in natura a qualsiasi soggetto (sia esso un dirigente, funzionario o dipendente della Pubblica Amministrazione o un soggetto privato) per promuovere o favorire gli interessi della Società anche a seguito di illecite pressioni o ricorrere a forme diverse di aiuti o contribuzioni che, sotto veste di sponsorizzazioni, incarichi, consulenze o pubblicità abbiano invece le stesse finalità sopra vietate;

- Accordare vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione italiana o straniera che possano determinare le stesse conseguenze previste al precedente punto;
- Assumere personale gradito a pubblici ufficiali, a meno che la selezione non abbia seguito un processo ispirato a criteri di valutazione oggettivi e rigorosamente meritocratici;
- Assegnare incarichi di fornitura a persone o società vicine o gradite a soggetti pubblici in assenza dei necessari requisiti di qualità, sicurezza e convenienza dell' operazione di acquisto;
- Distribuire omaggi e regali o accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione o di soggetti terzi al di fuori di quanto previsto dalla prassi aziendale (vale a dire, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale);
- Effettuare prestazioni in favore dei Consulenti, dei Partner e dei Fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- Riconoscere compensi in favore dei Consulenti, dei Partner e dei Fornitori che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere;
- Esibire documenti negligentemente incompleti e/o comunicare dati falsi o alterati ad Enti Pubblici;
- Tenere una condotta intenzionalmente ingannevole finalizzata ad indurre gli Enti Pubblici in errore, circa la documentazione presentata;
- Presentare dichiarazioni negligentemente non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- Destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
- Omettere informazioni dovute alla Pubblica Amministrazione, anche su induzione di suoi rappresentanti, al fine di orientarne a proprio favore le decisioni;
- Alterare, in qualsiasi modo e con qualsiasi mezzo, i processi e le risultanze delle attività di monitoraggio della qualità dei servizi di corrispondenza erogati dalla Società effettuate da organismi (di diritto pubblico o privato) in tal senso incaricati dalla Pubblica Amministrazione, da Autorità Indipendenti e di Vigilanza, ovvero svolte ai fini gestionali interni;
- Effettuare pagamenti in contanti, ad eccezione delle operazioni eseguite mediante la piccola cassa;
- Costringere o indurre terzi a promettere denaro o utilità, abusando della qualità di pubblico ufficiale o di incaricato di pubblico servizio;
- Ricevere omaggi, regali e vantaggi di qualsiasi natura, eccedenti le normali pratiche di cortesia, o comunque volti ad acquisire indebiti trattamenti di favore nella conduzione

di qualsiasi attività aziendale.

Inoltre i Destinatari del Modello sono tenuti a:

- Gestire in modo trasparente i rapporti nei confronti della Pubblica Amministrazione, dei Consulenti, dei Fornitori e dei Partner in generale;
- Effettuare gli adempimenti nei confronti della Pubblica Amministrazione e la predisposizione della relativa documentazione nel rispetto delle normative vigenti, nazionali o comunitarie, nonché delle convenzioni stipulate con soggetti e organi della P.A.;
- Conservare i verbali redatti in occasione delle ispezioni svolte dalla Pubblica Amministrazione.

A.4 Principi di controllo specifici

La Società ha adottato, oltre ai principi comportamentali sopra individuati, i seguenti principi di controllo specifici in relazione ai reati previsti dalla presente parte speciale, con particolare riferimento ai processi strumentali alla commissione del reato di seguito riportati:

Acquisto di beni, servizi e consulenze

- Segregazione dei compiti nelle fasi/attività del processo relative:
    - Alla richiesta della fornitura;
    - All'effettuazione dell'acquisto;
    - Alla certificazione dell'esecuzione dei servizi/consegna dei beni (rilascio benestare);
    - All'effettuazione del pagamento;
- Esistenza di criteri tecnico-economici per:
    - La selezione di potenziali fornitori (qualificazione ed inserimento nell'albo fornitori);
    - La validazione della fornitura e dei beni/servizi forniti;
    - La valutazione complessiva dei fornitori.
- Utilizzo di idonei dispositivi contrattuali adeguatamente formalizzati;
- Individuazione, da parte del singolo Ufficio, coerentemente con le proprie attività ed in accordo con la pianificazione di budget e delle sue revisioni, del fabbisogno di beni e servizi da acquisire;
- Ricezione delle RdA su un modulo standard debitamente compilato emesso dalle diverse Unità Aziendali;
- Valutazione, da parte delle Unità/ Direzioni, delle effettive esigenze di ricorrere all'acquisto e suggerimento all'Unità preposta all'acquisto del fornitore più conveniente per prezzo e qualità;
- Richiesta di emissione di un Ordine di Acquisto da parte dell'Unità richiedente all'unità preposta agli acquisti e alla persona autorizzata alla sottoscrizione di impegni formali nei confronti dei terzi;

- Rilevazione degli ordini emessi e dei costi sostenuti, in modo da verificare costantemente l'andamento delle spese rispetto ai budget ed alle prechiusure approvati;
- Selezione dei fornitori presenti nell'anagrafica aziendale da parte della Direzione Responsabile;
- Avvio del formale processo di valutazione per i nuovi fornitori, ai fini della classificazione di questi ultimi per l'inserimento in anagrafica, mediante compilazione di un apposito modulo standard;
- Richiesta, da parte della Direzione Responsabile, di preventivi diversi, che contengano le indicazioni necessarie per poter espletare un'adeguata attività di selezione tra le diverse offerte, sia dal punto di vista tecnico che economico, ad almeno 3 fornitori per ogni acquisto;
- Valutazione tecnica ed economica delle offerte da parte della direzione responsabile ed eventualmente in collaborazione con l'Ufficio richiedente, sulla base di criteri oggettivi e documentabili;
- Archiviazione di tutti i preventivi pervenuti per consentire la tracciabilità delle motivazioni delle scelte e delle responsabilità;
- Formalizzazione della Richiesta di Acquisto da parte del Responsabile dell'Ufficio richiedente e formale approvazione della stessa da parte della Direzione da cui tale soggetto dipende gerarchicamente;
- Formale autorizzazione delle Richieste di Acquisto per determinate categorie di spese, anche se previste a budget, da parte della Direzione responsabile;
- Formale autorizzazione per le spese non previste nei budget e nelle prechiusure da parte della Direzione responsabile, del Direttore Amministrativo e dell'Amministratore Delegato;
- Compilazione di un apposito modulo per la richiesta di approvazione delle spese ricomprese in determinate categorie e per le spese extra-budget e apposizione del visto dell'Ufficio Controllo di Gestione al suddetto modulo;
- Autorizzazione per i Direttori (RESPONSABILI DI FUNZIONE) ad assumere impegni nei confronti dei terzi nei limiti stabiliti dalle delibere del Consiglio di Amministrazione e dalle procure conferite;
- Motivazione, da parte dell'unità richiedente l'acquisto, e successiva approvazione da parte del Consiglio di Amministrazione, o della Direzione Amministrativa, di eventuali deroghe alle direttive aziendali che prevendono condizioni di pagamento non inferiori ai 90 giorni fine mese e che comportino condizioni più sfavorevoli per la Società;
- Emissione dell'Ordine di Acquisto nel sistema contabile attraverso il relativo modulo da parte dell'unità preposta alla gestione degli acquisti e formale invio del suddetto modulo al Direttore (se Procuratore) od al Procuratore al fine di ottenerne la legittimazione mediante la firma;
- Archiviazione dell'Ordine di Acquisto firmato e trasmissione del suddetto Ordine all'Ufficio Contabilità Fornitori ed al responsabile dell'unità richiedente;
- Preventiva sottoscrizione di un contratto di fornitura, per alcune tipologie di beni o

servizi con prestazioni predeterminate e continuative, con la verifica dell'Ufficio Legale e successiva approvazione e sottoscrizione da parte del Direttore responsabile in relazione ai poteri conferiti, in sostituzione dell'Ordine di Acquisto.

- Inserimento, nei contratti di fornitura, della clausola di presa visione del Codice Etico e del Modello Organizzativo ex D.Lgs. 231/01;
- Esistenza di livelli autorizzativi, in coerenza con il sistema delle procure aziendali, per l'approvazione delle varianti/integrazioni ai contratti di fornitura stipulati;
- Invio di copia del contratto di fornitura firmato all'Ufficio Legale, al Consiglio di Amministrazione e all'Unità richiedente l'acquisto;
- Verifica della conformità del bene ricevuto e/o del servizio prestato rispetto alle specifiche dell'ordine di acquisto e conseguente rilascio del benestare al pagamento degli importi fatturati;
- Tracciabilità delle singole fasi del processo (documentazioni a supporto, livello di formalizzazione e modalità tempistiche di archiviazione).

Gestione dei flussi monetari e finanziari

- Segregazione dei compiti nelle fasi/attività del processo relative:
    - alla richiesta dell'ordine di pagamento o di messa a disposizione;
    - all' effettuazione del pagamento;
    - al controllo/riconciliazione a consuntivo.
- Autorizzazione sia per la richiesta, che per l'ordine di pagamento o di messa a disposizione, articolati in funzione della natura dell'operazione (ordinaria/straordinaria) e dell'importo;
- Flusso informativo sistematico che garantisca il costante allineamento tra procure, deleghe operative e profili autorizzativi;
- Esistenza e diffusione di *specimen* di firma in relazione ai livelli autorizzativi definiti per la richiesta;
- Impiego delle risorse finanziarie mediante fissazione di soglie quantitative coerenti con le competenze gestionali e alle responsabilità organizzative affidate alle singole persone;
- Autorizzazione preventiva da parte dei soggetti dotati di idonei poteri circa l'apertura/ chiusura dei conti correnti.
- Tracciabilità degli atti e delle singole fasi del processo, con specifico riferimento ai documenti che hanno originato le operazioni di incasso e/o pagamento.

Formazione del bilancio e rapporti con gli organi di controllo

- Previsione di riunioni tra rappresentanti della Società di revisione, del Collegio Sindacale e dell'Organismo di Vigilanza.

Richiesta e gestione dei finanziamenti pubblici

- Verifica in termini di completezza e correttezza circa la documentazione da presentare all'ente pubblico finanziatore (relativamente sia alla documentazione di progetto che alla documentazione attestante i requisiti tecnici, economici e professionali dell'azienda che presenta il progetto);
- Verifiche incrociate di coerenza tra la funzione richiedente l'erogazione pubblica e la funzione designata a gestire le risorse per la realizzazione dell'iniziativa dichiarata;
- Monitoraggio sull'avanzamento del progetto realizzativo (a seguito dell'ottenimento del contributo pubblico) e sul relativo reporting alla Pubblica Amministrazione/Ente finanziatore, con evidenza e gestione delle eventuali anomalie;
- Controlli sull'effettivo impiego dei fondi erogati dagli organismi pubblici, in relazione agli obiettivi dichiarati.

Selezione, assunzione e gestione del personale dipendente e dei collaboratori

- Necessità di accertare la eventuale disponibilità di adeguate candidature interne prima di procedere ad assunzioni dal mercato esterno;
- Formale autorizzazione della richiesta di assunzione di un dipendente mediante apposizione di firma da parte dell'Unità Organizzativa Richiedente, delle Direzioni di competenza;
- Monitoraggio del mercato del lavoro da parte della Gestione del Personale mediante utilizzo di strumenti di selezione previsti dal budget di spesa assegnato;
- Tracciabilità delle fonti di reperimento dei CV (ad es. società di head-hunting, recruitment, inserzioni, candidature spontanee, etc.);
- Valutazione dell'inquadramento e della retribuzione del candidato in funzione del profilo professionale identificato e la coerenza con le politiche retributive aziendali;
- Predisposizione annuale da parte della Direzione del Personale, nel rispetto degli obiettivi strategici ed in stretta collaborazione con i Direttori delle Funzioni Aziendali e previa valutazione e autorizzazione del vertice aziendale, del budget degli organici e del relativo costo per ogni area di responsabilità;
- Ottenimento di approvazione preventiva da parte della Direzione di competenza, della Direzione del Personale e dell'Amministratore Delegato per l'attivazione del processo di ricerca e selezione qualora la posizione da ricoprire non fosse prevista nel budget aziendale;
- Compilazione, da parte dell'Unità Organizzativa Richiedente e dalla Gestione Personale, di apposita modulistica per l'indicazione delle attività e responsabilità della posizione e delle caratteristiche individuali che il candidato dovrà possedere;
- Distinte modalità di valutazione "attitudinale" e "tecnica" del candidato mediante colloqui ed in particolare, articolazione della fase di valutazione del processo di selezione nelle seguenti fasi:
    - colloquio effettuato dal Responsabile dell'Unità Organizzativa Richiedente con il supporto della Gestione del Personale, al fine di valutare le conoscenze tecnico-professionali e la coerenza con le competenze richieste dalla posizione da ricoprire;
    - Compilazione, nell'ambito del suddetto colloquio, di un questionario da parte

del candidato e degli esaminatori;

- Colloquio condotto dalla Gestione del Personale, per la valutazione delle caratteristiche attitudinali e motivazionali del candidato;
- Terzo colloquio, qualora i primi due colloqui abbiano dato esito positivo, effettuato dal Direttore di Funzione da cui dipende il Responsabile della Unità Organizzativa Richiedente, per la valutazione finale e per la definizione della retribuzione, dei tempi d'inserimento e delle esigenze formative;
- Per i Dirigenti, effettuazione di un colloquio anche con il Direttore del Personale.

- Predisposizione del modulo per la richiesta di assunzione del candidato selezionato da parte della Gestione Del Personale, debitamente autorizzato in base ai livelli autorizzativi esistenti, in coerenza con il sistema delle procure aziendali;
- Predisposizione da parte dell'Amministrazione del Personale dei documenti necessari all'assunzione, debitamente firmati in base ai livelli autorizzativi esistenti, in coerenza con il sistema delle procure aziendali;
- Formalizzazione di apposito modulo per la valutazione del neo assunto dopo il periodo di prova da parte del Responsabile dell'Unità Organizzativa Richiedente;
- Archiviazione della documentazione relativa al contratto di stage, sia in formato elettronico che cartaceo.

Rapporti e adempimenti con gli Enti Pubblici e le Autorità Amministrative Indipendenti

- Necessità che le seguenti fasi/attività del processo di gestione dei rapporti e degli adempimenti con gli Enti Pubblici e le Autorità Amministrative Indipendenti, non siano mai poste in essere dallo stesso soggetto:
  - predisposizione di dati/informazioni/documenti da fornire ai soggetti pubblici;
  - presentazione di dati/informazioni/documenti da fornire alla Pubblica Amministrazione.
- esistenza di direttive sulle modalità di condotta operativa da adottare nei contatti formali e informali intrattenuti con i diversi soggetti pubblici;
- formalizzazione degli eventuali rapporti con soggetti esterni (consulenti legali, terzi rappresentanti o altro) incaricati di svolgere attività di supporto di QUID INFORMATICA, prevedendo nei contratti una specifica clausola che li vincoli al rispetto dei principi etico-comportamentali adottati da QUID INFORMATICA;
- rendiconto dei rapporti formali con rappresentanti della Pubblica Amministrazione e tracciabilità degli atti e delle fonti documentali che ne stanno alla base.
- partecipazione agli incontri con i funzionari pubblici dai rappresentanti della Società; la documentazione richiesta e consegnata (evidenziando ad es. data, obiettivi, motivazioni, partecipanti), deve essere comunicata al responsabile archiviata e conservata;
- individuazione di Dipendenti o componenti degli Organi Sociali di competenza per la gestione dei rapporti con la Pubblica Amministrazione o con i soggetti privati, relativamente alle operazioni comprese nei procedimenti delle attività a rischio sulla base delle responsabilità organizzative assegnate;

- tracciabilità degli incontri svolti con il rappresentante della Pubblica Amministrazione attraverso la redazione di un elenco, con l'indicazione della data, dell'Ente, dell'interlocutore e dell'oggetto del rapporto;
- sottoscrizione delle comunicazioni dirette alla Pubblica Amministrazione nel rispetto dei poteri conferiti a soggetti della Società;
- approvazione da parte di adeguati livelli autorizzativi della documentazione da trasmettere in relazione alle richieste pervenute dalle Autorità;
- archiviazione e conservazione, a cura di ciascuna funzione, di tutta la documentazione prodotta nell'ambito della propria attività sensibile, ivi inclusa quella trasmessa alla Pubblica Amministrazione anche eventualmente in via telematica.

Gestione di omaggi, donazioni e sponsorizzazioni

- Previsione annuale degli importi destinati all'acquisto di omaggi nei piani di spesa ricompresi nei budget delle singole Società/Direzioni, indicati alle voci "Omaggi";
- Approvazione omaggi da destinarsi ai dipendenti da parte del Direttore Centrale Risorse Umane o dal Consiglio di Amministrazione;
- Effettuazione di spese per omaggi e liberalità nei limiti del piano di spesa di Budget/Prechiusura approvato, individuati prevalentemente per omaggi di costo unitario non superiore al limite di costo unitario (150,00 euro);
- Approvazione del Consiglio di Amministrazione per omaggi eccedenti i limiti di costo unitario e/o quelli fissati dai piani di spesa ricompresi nei budget delle singole Società/Direzioni ed effettuazione degli stessi solo da parte dei Direttori;
- Richiesta di beni a titolo di omaggio formulata per iscritto ed inviata alla funzione aziendale che si occupa dell'approvvigionamento, specificando quantità, nominativo del beneficiario del bene, l'azienda/Ente di appartenenza dello stesso e se si tratta di soggetto pubblico;
- Omaggi nei confronti della Pubblica Amministrazione consentiti soltanto se rientranti nell'esclusivo perimetro dei prodotti di QUID INFORMATICA e sempre preventivamente autorizzati in forma scritta dal Consiglio di Amministrazione;
- Formale autorizzazione di qualsiasi sponsorizzazione effettuata da parte dei Responsabili aziendali, i quali valutano tenuto conto dell'entità della spesa, della complessità e della finalità della sponsorizzazione di richiedere anche l'approvazione del Consiglio di Amministrazione;
- Approvazione del Consiglio di Amministrazione per erogazioni di denaro per liberalità ad enti per iniziative, quali ad esempio quelle a scopo culturale, sociale ed umanitario.

Gestione delle attività connesse alla comunicazione esterna

- Approvazione del Consiglio di Amministrazione del calendario che contiene la pianificazione degli eventi;
- Formale contrattualizzazione degli accordi presi con le terze parti per le attività

necessarie all'organizzazione degli eventi;

- Preventiva verifica circa l'affidabilità delle società a cui si intende esternalizzare le attività relative all'organizzazione dell'evento;
- Preventiva autorizzazione delle comunicazioni verso l'esterno da parte del Consiglio di Amministrazione della Società.

Rimborsi spese, anticipi e spese di rappresentanza

- Rimborso delle spese per le trasferte a mezzo di bonifico bancario, previlegiando in alternativa l'utilizzo di carte di credito aziendali/corporate rispetto alla corresponsione di anticipi in contanti;
- Indicazione in caso di spese di rappresentanza del numero di partecipanti, dei nominativi degli ospiti (o, in alternativa "fonte informativa" a discrezione dei giornalisti, per ragioni di confidenzialità) e delle società di appartenenza;
- Formalizzazione delle richieste di rimborso spese attraverso apposita modulistica contenente il giustificativo di spesa e la ricevuta della transazione effettuata con carta di credito;
- Compilazione di un form specifico in caso di acquisto del carburante per l'uso dell'autovettura aziendale;
- Presentazione alle Unità Amministrative preposte della motivazione della trasferta e delle fotocopie dei giustificativi;
- Verifica ed approvazione delle spese documentate da parte della Segreteria della Direzione di appartenenza;
- Firma del dipendente sulla stampa della Nota Spese prodotta dal Sistema;
- Formale approvazione delle note spese da parte del Direttore responsabile;
- Compilazione del modulo per l'autorizzazione all'uso dell'auto propria da parte del superiore gerarchico;
- Formale richiesta attraverso compilazione di apposita scheda per i rimborsi chilometrici in caso di uso dell'auto propria e del carburante in caso di uso di auto aziendale;
- Indicazione a Sistema delle spese di ristorazione in favore dei clienti, con specifica dei nomi delle persone e relative aziende clienti ospiti;
- Inserimento a Sistema delle richieste di anticipi in contante con la specifica della destinazione e della previsione di spesa;
- Autorizzazione dell'anticipo da parte del proprio Direttore responsabile e della Direzione Amministrativa;
- Indicazione dell'ammontare complessivo dell'anticipo in deduzione della nota spese con evidenza di quanto eventualmente restituito.

Gestione della commercializzazione di prodotti e/o servizi

- Segregazione dei compiti nelle fasi/attività del processo relative:

- alle trattative;
- alla gestione dei fornitori per le sub-forniture;
- all' esecuzione contrattuale;
- alla fatturazione.
- verifica di congruenza fra quanto contrattualizzato e quanto fatturato;

- Selezione ed utilizzo di subfornitori adeguatamente qualificati;
- Segnalazione di operazioni sospette di illecito o di violazione della normativa sull'antiriciclaggio all'autorità pubblica;
- Verifica di congruenza fra quanto autorizzato, quanto realizzato e quanto dichiarato alla Pubblica Amministrazione ai fini del pagamento dei corrispettivi previsti;
- Tracciabilità degli atti e delle fonti informative nelle singole fasi dei processi con specifico riferimento ad impiego di risorse e tempi;
- Direttive sulle modalità di condotta operativa da adottare nei contatti formali e informali intrattenuti con i diversi soggetti pubblici;
- Formalizzazione degli eventuali rapporti con soggetti esterni (consulenti, terzi rappresentanti o altro) incaricati di svolgere attività a supporto della società, prevedendo nei contratti una specifica clausola che li vincoli al rispetto dei principi etico - comportamentali adottati dalla società.

PARTE SPECIALE B – DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

Le disposizioni della Presente Parte Speciale hanno per Destinatari tutti i soggetti coinvolti, a qualunque titolo, nella gestione o nell'utilizzo dei sistemi informativi aziendali. In particolare i fornitori che prestano assistenza a QUID INFORMATICA nella gestione delle proprie dotazioni informatiche o che le forniscono hardware e software devono impegnarsi mediante apposita clausola contrattuale al rispetto del presente Modello.

La presente Parte Speciale "B" si applica alle tipologie di reati identificati dall'art. 24-bis del Decreto. La legge 18.3.2008 n. 48, entrata in vigore il 5.4.2008, ha introdotto nell' ordinamento italiano una serie di nuove fattispecie di reato che possono essere commesse attraverso un illecito utilizzo di documenti informatici e/o di sistemi informatici.

Tale legge ha altresì introdotto nel D.Lgs. 231/2001 il nuovo art. 24-bis, che estende alle società, ricorrendone i presupposti, la responsabilità amministrativa per i reati sopra indicati.

La natura informatica che qualifica questi reati può riguardare le modalità di realizzazione della condotta, il suo oggetto materiale, il bene giuridico tutelato o la natura dei mezzi di prova.

Preliminarmente, al fine di agevolare la lettura delle norme, vengono di seguito fornite le definizioni di documento informatico e sistema informatico:

- per documento informatico si intende "la rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti" secondo quanto previsto dal Codice dell' Amministrazione Digitale ex D.Lgs. 82/2005;
- per sistema informatico si intende, secondo la Convenzione di Budapest, "qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l'esecuzione di un programma per elaboratore, compie un' elaborazione automatica di dati".

B.1 Reati applicabili alla Società

Si descrivono brevemente di seguito le fattispecie di reato contemplate nel D.Lgs. 231/2001 all'art. 24 bis ritenute applicabili, anche se in via prudenziale, alla Società, in ragione delle attività svolte:

Falsità riguardanti un documento informatico (art. 491-bis c.p.)

Tale norma, di portata generale, estende le sanzioni previste per le falsità` degli atti pubblici e privati, alle falsità riguardanti, rispettivamente, un documento informatico pubblico o privato avente efficacia probatoria.

L'articolo stabilisce infatti che tutti i delitti relativi alla falsità in atti, 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.

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.

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

Il reato in questione contrasta in particolare il fenomeno dei c.d. “hackers”, e cioè di quei soggetti che si introducono nei sistemi informatici altrui, attraverso le reti telematiche, aggirando le protezioni elettroniche create dai proprietari di tali sistemi per tutelarsi dagli accessi indesiderati.

Tale reato si realizza quindi quando un soggetto abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza interne al medesimo, siano esse di tipo hardware o software.

La condotta illecita può concretizzarsi sia in un’attività di “introduzione” che di “permanenza” abusiva nel sistema informatico.

L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema stesso.

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

Detenzione, diffusione e installazione abusiva di apparecchiature, codici o altri mezzi atti all’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, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Questo delitto si integra sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi. La condotta è abusiva nel caso in cui i codici di accesso siano ottenuti a seguito della violazione di una norma, ovvero di una clausola contrattuale, che vieti detta condotta (ad esempio, policy Internet).

L'art. 615-quater, inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

La norma sanziona solo le condotte prodromiche e preparatorie all’accesso abusivo al sistema informatico o telematico.

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)

La norma in esame sanziona chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in essi contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici.

L'ipotesi tipica è quella di creazione dei c.d. "programmi virus", che diffondendosi e riproducendosi minano la funzionalità dei sistemi ove riescano ad introdursi.

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

La disposizione tutela sia la genuinità sia la riservatezza delle comunicazioni.

Tale ipotesi di reato e integrata dalla condotta di chi fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisce o interrompe tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione al pubblico. La locuzione "comunicazioni telematiche" si presta ad abbracciare qualunque forma e qualunque strumento di divulgazione, ivi compresa la stessa via telematica, e quindi anche la diffusione del testo della comunicazione via Internet o attraverso qualsiasi altra rete.

Il reato è aggravato, tra gli altri casi, se commesso da un soggetto che abusa della sua qualità di operatore del sistema informatico o telematico.

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

Tale ipotesi di reato si realizza quando qualcuno, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti 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.)

Tale fattispecie reato si realizza quando un soggetto "distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui". Il reato, ad esempio, si integra

nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità 635 ter c.p.

La norma in questione al primo comma punisce le condotte prodromiche e preparatorie al danneggiamento di informazioni, dati e programmi informatici di cui all'art. 635 bis c.p. riguardanti informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità.

La concreta realizzazione del danno, invece, integra un'autonoma ipotesi di reato, sanzionata nel comma 2 della norma in commento.

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

Tale reato di realizza quando un soggetto mediante le condotte di cui all'art. 635-bis (danneggiamento di dati, informazioni e programmi informatici), 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.

Danneggiamento di sistemi informatici o telematici di pubblica utilità `(635 quinquies c.p.)

La norma in questione punisce i fatti di danneggiamento previsti dall' art. 635 quater c.p. riguardanti i sistemi informatici o telematici di pubblica utilità. Il reato è aggravato, tra gli altri casi, se commesso da un soggetto che abusa della sua qualità` di operatore del sistema informatico o telematico.

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

Tale reato si configura quando il 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.

Questo reato può essere integrato da parte dei certificatori qualificati o meglio i soggetti che prestano servizi di certificazione di firma elettronica qualificata.

B.2 Attività sensibili

In relazione ai reati previsti dall'art. 24-bis del D. Lgs. 231/2001 applicabili alla Società sono state individuate le seguenti attività sensibili:

- Gestione delle modifiche architetturali ed applicative;
- Continuità del servizio;

- Sicurezza logica dei sistemi;
- Gestione del Service Desk e degli incidenti/problemi;
- Misure per la sicurezza delle reti di trasmissione;
- Gestione dell'ambiente fisico;
- Installazione di programmi e applicazioni non inclusi nella configurazione software standard;
- Download e installazione di programmi e/o applicazioni da siti web o altre fonti;
- Download e installazione di programmi e/o applicazioni coperti da copyright;
- Distruzione, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici di terze parti in genere e della Pubblica Amministrazione in particolare utilizzando le risorse aziendali;
- Violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato;

B 3 Regole Comportamentali

Conformemente a quanto previsto nelle procedure e nelle norme aziendali, ai Destinatari sopra individuati è fatto divieto di:

- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di:
    - acquisire senza l'autorizzazione del proprietario informazioni contenute nei suddetti sistemi informativi;
    - danneggiare, distruggere dati contenuti nei suddetti sistemi informativi;
    - utilizzare abusivamente codici d'accesso a sistemi informatici e telematici;
    - procedere alla diffusione degli stessi.
- porre in essere condotte miranti alla distruzione o all'alterazione dei documenti informatici aventi finalità probatoria in assenza di una specifica autorizzazione;
- utilizzare o installare programmi diversi da quelli autorizzati dall'Amministratore di Sistema di QUID;
- aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (Antivirus, Firewall, proxy, server,...);
- lasciare il proprio Personal Computer sbloccato e incustodito;
- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato.

Il personale della Funzione di Sistema di QUID INFORMATICA, anche mediante gli Outsourcers, deve attivarsi, in base al proprio ruolo e responsabilità, al fine di porre in essere quelle azioni necessarie per:

- assicurare che le attività svolte da parte di fornitori terzi in materia di:
    - networking;
    - gestione software applicativi;
    - gestione sistemi hardware;

  rispettino i principi e le regole aziendali al fine di tutelare la sicurezza dei dati ed il corretto accesso da parte dei soggetti ai sistemi applicativi ed informatici;

- verificare la sicurezza della rete e dei sistemi informativi aziendali;
- verificare che la sicurezza fisica dell'infrastruttura tecnologica di QUID INFORMATICA sia implementata nel rispetto delle regole interne ed in modo da consentire un monitoraggio delle attività di gestione e manutenzione sulla stessa;
- identificare le potenziali vulnerabilità nel sistema dei controlli IT;
- valutare la corretta implementazione tecnica del sistema "deleghe e poteri" aziendale a livello di sistemi informativi ed abilitazioni utente riconducibile ad una corretta segregazione dei compiti;
- vigilare sulla corretta applicazione di tutti gli accorgimenti ritenuti necessari al fine di fronteggiare, nello specifico, i delitti informatici e di trattamento dei dati, suggerendo ogni più opportuno adeguamento;
- porre in essere le azioni necessarie per monitorare il corretto utilizzo degli accessi (user - id, password) ai sistemi informativi di terze parti.

Tutti i Destinatari ed in particolare i responsabili delle diverse Funzioni di QUID INFORMATICA sono tenuti a rispettare e a far rispettare, per le attività di rispettiva competenza, le seguenti regole:

- gli strumenti aziendali devono essere utilizzati nel rispetto delle policy e procedure aziendali definite;
- le credenziali utente devono essere oggetto di verifica periodica al fine di prevenire eventuali erronee abilitazioni ai sistemi applicativi;
- non deve essere consentito l'accesso alle aree riservate (quali server rooms, locali tecnici, ecc.) alle persone che non dispongono di idonea autorizzazione, temporanea o permanente e, in ogni caso, nel rispetto della normativa (interna ed esterna) vigente in materia di tutela dei dati personali;
- la navigazione in internet e l'utilizzo della posta elettronica attraverso i sistemi informativi aziendali deve essere limitato alle sole attività lavorative;
- assicurare l'aggiornamento delle password dei singoli utenti;

Siano rispettate in ogni caso le misure tecniche e organizzative adottate da QUID INFORMATICA in adempimento alla normativa in materia di Data Protection (GDPR)

B.4 Principi di controllo e presidi organizzativo-procedurali specifici

La Società ha adottato, oltre ai principi comportamentali sopra individuati, i seguenti principi di controllo specifici in relazione ai reati previsti dalla presente parte speciale, con particolare riferimento al processo strumentale alla commissione del reato di seguito riportato:

Gestione dei sistemi informativi

- Definizione di ruoli ed allocazione di responsabilità alle diverse funzioni aziendali preposte alla sicurezza informatica;
- Sistema di gestione operativa della sicurezza informatica, sia in termini di prevenzione che di reazione, che prevede l'attuazione di adeguate misure per garantire la sicurezza dei dati e delle informazioni e dei dispositivi hardware/software presenti in Azienda;
- Sistema di monitoraggio della sicurezza delle informazioni e delle reti che prevede la tempestiva rilevazione, analisi e conseguente gestione di possibili attività illecite. Il sistema di monitoraggio ed analisi è strutturato su più livelli, al fine di garantire i

necessari requisiti di escalation e di separazione dei ruoli nella gestione delle diverse casistiche;

- Attività di formazione e sensibilizzazione dei dipendenti sui temi specifici della sicurezza informatica al fine di assicurare il corretto utilizzo delle risorse informatiche aziendali;
- Monitoraggio nel continuo delle minacce applicabili alle diverse risorse informatiche;
- Determinazione dei processi aziendali impattati da eventi di *change management*, incidenti di sicurezza e dalla diffusione di notizie su nuove vulnerabilità o minacce per sottoporli all'analisi dei rischi;
- Politica di controllo accessi alle risorse informatiche da parte degli amministratori di sistema ristretta alle sole esigenze di gestione ed esercizio del Servizio;
- Gestione e custodia dei file di tracciamento (applicativi e di sistema) secondo le modalità e i criteri di raccolta strettamente legati alle esigenze di natura legislativa e/o di sicurezza;
- Contromisure idonee a contrastare l'acquisizione e/o la diffusione di virus informatici;
- Verifica della sicurezza delle transazioni effettuando, tra l'altro, operazioni atte alla prevenzione di azioni di e al furto di identità, perpetrato per mezzo internet, ai danni dei clienti;

PARTE SPECIALE C – REATI DI CRIMINALITA' ORGANIZZATA

La presente Parte Speciale "C" si applica alle tipologie di reati identificati dall'art. 24-ter del Decreto.

C.1 Reati applicabili alla Società

La Legge 15 luglio 2009, n. 94 recante "Disposizioni in materia di sicurezza pubblica" ha introdotto nel Decreto 231 l'art. 24-ter, tra i possibili reati presupposto della responsabilità amministrativa degli enti, numerose fattispecie c.d. di "criminalità organizzata, anche se non connotate dal requisito della "transnazionalità".

A seguito delle attività di mappatura dei rischi, si è ritenuto di concludere che l'unica fattispecie che comporta astrattamente un rischio di realizzazione all'interno della Società è quella di cui all'art. 416 c.p (associazione per delinquere, di natura semplice – escluso sesto comma).

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

Con riferimento alle fattispecie di reati sopra considerata, la sanzione penale è ricollegata al solo fatto della promozione, costituzione, partecipazione ad una associazione criminosa formata da tre o più persone, indipendentemente dall'effettiva commissione (e distinta punizione) del reato che costituisce il fine dell'associazione. Ciò significa che la sola cosciente partecipazione ad una associazione criminosa da parte di un esponente o di un dipendente della società potrebbe determinare la responsabilità amministrativa della società stessa, sempre che la partecipazione o il concorso all'associazione risultasse strumentale al perseguimento anche dell'interesse o del vantaggio della Società medesima.

È tuttavia richiesto che il vincolo associativo si esplichi attraverso un minimo di organizzazione a carattere stabile nel tempo e la condivisione di un programma di realizzazione di una serie indeterminata di delitti. Non basta pertanto l'occasionale accordo per la commissione di uno o più delitti determinati.

C.2 Attività sensibili

La commissione, nell'interesse o a vantaggio della Società, dei reati di cui all'art 24-ter del Decreto appare difficilmente ravvisabile, in ragione delle oggettive finalità di QUID INFORMATICA.

Fermo restando quanto sopra, tenuto presente che i delitti associativi si caratterizzano per l'esistenza di un vincolo associativo tra i soggetti teso a commettere una serie indeterminata di delitti, in sede di analisi delle potenziali aree di rischio aziendali risulta opportuno, in via prudenziale, prendere altresì in considerazione fattispecie delittuose che, pur non essendo espressamente richiamate dal D.Lgs. 231/2001, appaiono teoricamente realizzabili mediante il predetto vincolo associativo.

Pertanto, in relazione ai reati previsti dall'art. 24-ter del D.Lgs. 231/2001 potenzialmente applicabili, la Società ha individuato unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita, la seguente attività sensibile:

- coinvolgimento in un'organizzazione per la quale potrebbero verificarsi i presupposti del vincolo associativo ex art. 416 c.p (associazione per delinquere),

In quanto considerata potenzialmente trasversale a tutti processi aziendali e che può ricomprendere tutte le attività rilevate in sede di analisi preliminare, tra le quali, a titolo esemplificativo e non esaustivo, si fa riferimento a:

- Appalti di beni, servizi, e consulenze;
- Processi di selezione, assunzione e gestione delle risorse umane;
- Gestione della fiscalità aziendale, con particolare riferimento alle seguenti attività:
    - Compilazione, tenuta e conservazione delle scritture contabili rilevanti ai fini fiscali e degli altri documenti di cui è obbligatoria la conservazione;
    - Predisposizione delle dichiarazioni fiscali;
- Liquidazione delle imposte;
- Partecipazione a Gare

C.3 Regole Comportamentali

Per la sua natura particolare, caratterizzata da una carenza di tipicità della fattispecie, il reato di "associazione per delinquere" è astrattamente configurabile oltre che in alcuni ambiti puramente interni, anche e soprattutto negli ambiti di attività di QUID INFORMATICA caratterizzati da un contatto frequente o continuativo con terze parti, laddove uno o più soggetti interni alla Società, approfittando delle proprie mansioni, possano associarsi con soggetti esterni al fine di commettere in forma organizzata più delitti nell'interesse o a vantaggio di QUID INFORMATICA.

Più in particolare, si è ritenuto di considerare la possibilità teorica che taluni specifici reati, già considerati in altre Parti Speciali (cui si rimanda), possano essere commessi anche in forma "associativa". Potrebbe quindi configurarsi l'ipotesi di associazione per delinquere finalizzata alla commissione di uno dei seguenti reati:

- Corruzione;
- Indebita percezione di contributi pubblici anche federali;
- False comunicazioni sociali;
- Abuso di informazioni privilegiate / manipolazione di mercato;
- Ricettazione / riciclaggio / autoriciclaggio / impegno di beni, denaro o altre utilità di provenienza illecita;
- Frode in competizioni sportive ed esercizio abusivo di attività di giuoco o scommessa;

Al fine di evitare il verificarsi dei suddetti reati previsti dall'art. 24-ter del D.Lgs. 231/2001, a tutti i Destinatari del presente Modello, è fatto divieto di:

- Stringere accordi in qualsiasi forma, anche orale, per concordare con terze persone una o più azioni che riguardano il lavoro svolto per QUID INFORMATICA al di fuori delle finalità statutarie della Società, delle delibere degli organi sociali, dei contratti stipulati dalla società, delle proprie deleghe, dei propri poteri e della propria job description;

- Intrattenere rapporti, negoziare, stipulare e porre in esecuzione contratti o atti con persone indicate nelle Liste di Riferimento (c.d. black list) o facenti parte di organizzazioni presenti nelle stesse;
- Assumere persone indicate nelle Liste di Riferimento (c.d. black list) o facenti parte in organizzazioni presenti nelle stesse.

Inoltre, i Destinatari sono tenuti a:

- Determinare in maniera formale i criteri di selezione di fornitori di appalti e partner per la stipula di contratti e per la realizzazione di investimenti, nonché i criteri di valutazione delle offerte;
- Verificare l'attendibilità commerciale e professionale dei prestatori di appalti e partner;
- Tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge, nonché delle procedure aziendali interne, in tutte le attività finalizzate;
- Osservare rigorosamente, anche nei rapporti con i terzi, tutte le norme poste dalla legge a tutela della veridicità dell'informativa contabile, contro il riciclaggio e in materia fiscale;
- fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società.

C.4 Principi di controllo specifici

Oltre ai principi comportamentali sopra individuati valgono, in via prioritaria, i principi di controllo già previsti da QUID INFORMATICA in relazione ad altre tipologie di reato 231 disciplinate nelle seguenti parti speciali del presente Modello Organizzativo:

- Reati di corruzione, anche tra privati, ed altri reati nei rapporti con la Pubblica Amministrazione;
- Reati Societari;
- Reati di Ricettazione, Riciclaggio ed Impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio.

Valgono in ogni caso, in relazione a tutti i processi aziendali, i seguenti principi di controllo:

- Verifica e valutazione *ex ante* della selezione delle controparti circa:
  - la professionalità e l'onorabilità dei partner e dei fornitori;
  - la tracciabilità e la trasparenza degli accordi/ RTI con altre imprese per la realizzazione di investimenti o accordi commerciali;
- Sottoscrizione da parte dei partner o dei fornitori di specifica dichiarazione sul rispetto dei contenuti del Modello e delle Linee Guida adottate dalla Società;
- Tracciabilità degli atti e delle fonti informative nelle singole fasi del processo.

PARTE SPECIALE D – REATI DI FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO E DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

La presente Parte Speciale "D" si applica alle tipologie di reati identificati dagli artt. 25 bis e 25-bis 1 del Decreto.

D.1 Reati applicabili alla Società

La Legge 23 novembre 2001, n. 406 ha inserito nel Decreto 231 l'art. 25 bis, che estende la responsabilità amministrativa degli enti per i reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento.

Inoltre, la Legge 23 luglio 2009, n. 99 recante "Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia" ha inserito nel Decreto 231 l'art. 25 bis.1, che estende la responsabilità amministrativa degli enti per i delitti contro l'industria e il commercio.

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

Spendita di monete falsificate ricevute in buona fede (Art. 457 c.p.)

Il reato si configura qualora un soggetto spenda o metta altrimenti in circolazione monete contraffatte o alterate, da lui ricevute in buona fede.

Detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p).

La norma estende ai valori di bollo la disposizione dell'art. 457 c.p. prevista per le monete.

Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)

La norma condanna chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, contraffà o altera marchi o segni distintivi, nazionali o esteri di prodotti industriali, ovvero chiunque, senza essere concorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati. Condanna, inoltre, chiunque contraffà 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.

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

Questa fattispecie punisce chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio.

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

La norma condanna chiunque nell'esercizio di un'attività commerciale, industriale o comunque produttiva, compie atti di concorrenza con violenza o minaccia.

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

Questa fattispecie si realizza quando un soggetto 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

Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)

La norma condanna 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.

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

Il reato consiste di due distinte fattispecie. La prima, perseguibile a querela, punisce chiunque, potendo conoscere dell' esistenza di brevetti o di registrazioni altrui, fabbrica o utilizza ai fini della produzione industriale oggetti o altri beni, usurpando un titolo di proprietà industriale o in violazione dello stesso. La seconda fattispecie concerne la condotta di chi, al fine di trarne profitto, introduce in Italia, detiene per la vendita, pone in vendita o mette comunque in circolazione beni fabbricati in violazione dei titoli di proprietà` industriale.

D.2 Attività sensibili

In relazione ai reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento e ai delitti contro l'industria e il commercio sono state individuate le seguenti attività sensibili:

- sviluppo di nuovi prodotti al fine di sfruttarli commercialmente;
- iniziative di marketing e commerciale;
- comunicazione, ricerca e sviluppo, e responsabilità sociale di impresa.
- incassi e pagamenti in contanti (piccola cassa) e rimborsi spese.

D.3 Regole Comportamentali

Al fine di evitare il verificarsi dei suddetti reati previsti dal D.Lgs. 231/2001, a tutti i Destinatari, è fatto divieto di:

- ogni azione in violazione della normativa vigente in materia di ritiro dalla circolazione e trasmissione alla Banca d'Italia delle banconote denominate in euro sospette di falsità;
- utilizzare segni distintivi di soggetti terzi (ivi inclusi gli enti di certificazione) che non siano stati forniti (ad esempio scaricati da internet) e comunque senza l'autorizzazione di questi ultimi in base ad un contratto stipulato da QUID INFORMATICA;

- consegnare prodotti che possano indurre in inganno il destinatario circa l'origine, la provenienza, la composizione (materiale) degli stessi;
- compilare documenti di trasporto e consegna in maniera tale che il destinatario possa essere indotto in errore circa la qualità o la quantità dei prodotti consegnati;
- diffondere notizie e apprezzamenti sui prodotti e sull'attività di un imprenditore che siano anche solo potenzialmente idonei a determinarne il discredito;
- lo svolgimento di qualsiasi attività che possa essere considerata una forma di concorrenza non pienamente corretta e trasparente;
- la realizzazione di qualsiasi forma di attività intimidatoria o vessatoria nei confronti di imprese.

Inoltre, i destinatari del Modello sono tenuti a:

- verificare la presenza di eventuali diritti o brevetti esistenti sui prodotti commercializzati o distribuiti anche per conto terzi.

D.4 Principi di controllo specifici

La Società ha adottato, oltre ai principi comportamentali sopra individuati, i seguenti principi di controllo specifici in relazione ai potenziali reati in materia di reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento e delitti contro l'industria e il commercio, con particolare riferimento ai processi di seguito riportati:

Gestione della commercializzazione di prodotti e/o servizi

- Segregazione dei compiti nelle fasi/attività del processo relative:
  - alle trattative;
  - alla gestione dei fornitori per le sub-forniture;
  - all'esecuzione contrattuale;
  - alla fatturazione;
  - verifica di congruenza fra quanto contrattualizzato e quanto fatturato;
- Selezione ed utilizzo di sub-fornitori adeguatamente qualificati;
- Segnalazione di operazioni sospette di illecito o di violazione della normativa sull'antiriciclaggio all'autorità pubblica;
- Verifica di congruenza fra quanto autorizzato, quanto realizzato e quanto dichiarato alla Pubblica Amministrazione ai fini del pagamento dei corrispettivi previsti;
- Tracciabilità degli atti e delle fonti informative nelle singole fasi dei processi con specifico riferimento ad impiego di risorse e tempi;
- Direttive sulle modalità di condotta operativa da adottare nei contatti formali ed informali intrattenuti con i diversi soggetti pubblici;
- Formalizzazione degli eventuali rapporti con soggetti esterni (consulenti, terzi rappresentanti o altro) incaricati di svolgere attività a supporto della società, prevedendo nei contratti una specifica clausola che li vincoli al rispetto dei principi etico - comportamentali adottati dalla società;

- Tracciabilità e verificabilità ex-post delle transazioni tramite adeguati supporti documentali/informatici;
- Controfirma di accettazione dell'ordine;
- Invio di richiesta di chiarimenti al funzionario responsabile in caso di dubbio sulla provenienza/ regolarità/ completezza dell'ordinativo;
- Specifica sulla fattura, per clienti qualificati come enti locali territoriali, degli estremi della delibera che autorizza la firma del contratto.

Gestione dei contenuti dei prodotti/ servizi offerti

- Verifica di eventuali diritti o brevetti esistenti sul prodotto commercializzato o distribuito;
- Flussi documentali tra le funzioni aziendali competenti al fine di verificare la conformità del processo alle prescrizioni di legge;
- Verifica della corrispondenza delle dichiarazioni/certificazioni presentate con la documentazione di supporto;
- Flussi documentali tra le funzioni aziendali competenti per i vari processi o sotto processi e gli organi/enti deputati al rilascio di autorizzazioni e/o certificazioni attestanti la conformità alle prescrizioni di legge;
- Svolgimento di un controllo di liceità di testi o immagini contenuti nei propri prodotti;
- Tracciabilità delle singole attività (documentazione a supporto, verbalizzazione delle decisioni, intestazione/formalizzazione dei documenti e modalità/tempistiche di archiviazione);
- Archiviazione puntuale e precisa di tutta la documentazione rilevante a cura dell'Ufficio Competente;

PARTE SPECIALE E – REATI SOCIETARI

La presente Parte Speciale "E" si applica alle tipologie di reati identificati dall'art. 25-ter del d.lgs. 231/2001

E.1 Reati applicabili alla Società

L'art. 3 del D.Lgs. 11 aprile 2002, n. 61, in vigore dal 16 aprile 2002, nell'ambito della riforma del diritto societario ha introdotto nel Decreto 231 l'art. 25-ter che estende il regime di responsabilità amministrativa degli enti ai reati societari.

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

False comunicazioni sociali (art. 2621 c.c.)

I reati previsti dall'art. 2621 c.c. possono essere commessi esclusivamente dagli amministratori, dai direttori generali, dai dirigenti preposti alla redazione dei documenti contabili societari, dai sindaci o dai liquidatori della Società e si realizza quando questi, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazione ovvero omettono informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione.

La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Fatti di lieve entità (art. 2621-bis c.c.)

Tale norma punisce le medesime condotte previste dall'articolo 2621 c.c. con una sanzione penale inferiore quando i fatti sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta.

Falsità nelle relazioni o nelle comunicazioni della Società di revisione (art. 2624, commi 1 e 2, c.c.)

Tale ipotesi di reato consiste in false attestazioni od occultamento di informazioni, nelle relazioni od in altre comunicazioni della Società di revisione, concernenti la situazione economica, patrimoniale o finanziaria della società sottoposta a revisione, secondo modalità idonee a indurre in errore i destinatari delle comunicazioni stesse.

Ancorché l'art. 2624 c.c. sia stato abrogato dall'art. 37 del D.Lgs. 39/2010, si ritiene di prendere comunque il relativo reato in considerazione ai fini del presente Modello.

Impedito controllo (art. 2625, comma 2, c.c.)

Il reato di cui all'art. 2625, comma 2 del codice civile, si verifica nell'ipotesi in cui gli

amministratori impediscano od ostacolino, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali, procurando un danno ai soci. Il reato è punito a querela della persona offesa e la pena è aggravata se il reato è commesso in relazione a società quotate ovvero in relazione ad emittenti con strumenti finanziari diffusi tra il pubblico in misura rilevante.

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. In altri termini, la suddetta fattispecie di reato punisce una riduzione del capitale, con conseguente mancata ufficializzazione della riduzione del capitale reale tramite l'abbassamento del capitale nominale, il cui valore, pertanto, risulta superiore a quello del capitale reale. La condotta incriminata deve essere tenuta nei confronti dei soci e per integrare la fattispecie non occorre che tutti i soci siano liberati dall'obbligo di conferimento ma è sufficiente che lo sia un singolo socio o più soci.

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

Tale reato si concretizza qualora siano ripartiti utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero siano ripartite riserve, anche non costituite con utili, che non possono per legge essere distribuite.

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

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, al di 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.

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 fusioni con altre società o scissioni, che cagionino danno ai creditori.

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

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

caso di trasformazione.

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.

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.)

Il reato in questione si realizza nel caso in cui, col fine specifico di ostacolare l'esercizio delle funzioni delle autorità pubbliche di vigilanza, si espongano in occasione di comunicazioni ad esse dovute in forza di legge, fatti materiali non rispondenti al vero, ancorché oggetto di valutazione, ovvero si occultino, totalmente o parzialmente, con mezzi fraudolenti, fatti che si era tenuti a comunicare, circa la situazione patrimoniale, economica o finanziaria della società, anche qualora le informazioni riguardino beni posseduti o amministrati dalla società per conto terzi. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto terzi.

Con riferimento al reato di corruzione tra privati, si evidenzia che tale reato, pur essendo previsto nel codice civile unitamente ai citati reati societari, è stato inserito all'interno della Parte Speciale "A" al fine di garantire una maggiore uniformità nella trattazione dei fenomeni corruttivi che potrebbero manifestarsi nell'operatività aziendale.

False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D.Lgs. 19/2023) [aggiunto dal D.Lgs. n. 19/2023]

Chiunque, al fine di far apparire adempiute le condizioni per il rilascio del certificato preliminare di cui all'articolo 29, forma documenti in tutto o in parte falsi, altera documenti veri, rende dichiarazioni false oppure omette informazioni rilevanti, è punito con la reclusione da sei mesi a tre anni.

In caso di condanna ad una pena non inferiore a mesi otto di reclusione segue l'applicazione della pena accessoria di cui all'articolo 32-bis del codice penale.

E.2 Attività sensibili

Le attività che la Società ha individuato come sensibili, nell'ambito dei reati societari, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

In relazione ai reati societari sono state individuate le seguenti attività sensibili:

- Gestione della contabilità generale, con particolare riferimento alle attività di:
  - Rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi ed economici;
  - Corretta tenuta dei rapporti amministrativi con i terzi (e.g. clienti, fornitori) e relativa

gestione contabile delle partite di debito /credito;

- Gestione amministrativa e contabile dei cespiti;
- Gestione amministrativa e contabile del magazzino;
- Accertamenti di tutti gli altri fatti amministrativi in corso d'anno (e.g. costi del personale, penalità contrattuali, finanziamenti attivi e passivi e relativi interessi, ecc.);
- Acquisto di beni, servizi e consulenze;
- Iniziative di marketing e commerciale;

- Collaborazione e supporto all'Organo Amministrativo per la predisposizione di situazioni patrimoniali funzionali alla realizzazione di:
  - Operazioni straordinarie;
  - Operazioni di aumento/riduzione del capitale sociale;
  - Altre operazioni su azioni o quote sociali o della società.
- Raccolta, aggregazione e valutazione dei dati contabili necessari per la predisposizione della bozza di Bilancio Civilistico della Società, nonchè delle relazioni allegate ai prospetti economico-patrimoniali di bilancio da sottoporre alle delibere del Consiglio di Amministrazione;
- Gestione dei rapporti con gli Organi di Controllo relativamente alle verifiche sulla gestione amministrativa/contabile e sul Bilancio d'Esercizio e con i Soci nelle attività di verifica della gestione aziendale;
- Tenuta delle scritture contabili e dei Libri Sociali;
- Collaborazione e supporto all'Organo Amministrativo nello svolgimento delle attività di ripartizione degli utili di esercizio, delle riserve e restituzione dei conferimenti;
- Gestione di tesoreria;
- Collaborazione e supporto all'Organo Amministrativo per l'effettuazione delle operazioni di incremento/riduzione del capitale sociale o di altre operazioni su azioni della Società;
- Rapporti con soci, sindaci e revisori;
- Predisposizione della documentazione che sarà oggetto di discussione e delibera in Assemblea e gestione dei rapporti con tale Organo Sociale;

E.3 Regole Comportamentali

Al fine di evitare il verificarsi dei suddetti reati previsti dal D. Lgs. 231/2001, a tutti i Destinatari, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti della Società, è fatto divieto di:

- rappresentare o trasmettere per l'elaborazione e la predisposizione dei bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale o finanziaria della società;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;

- attivarsi affinché i fatti di gestione siano rappresentati correttamente e tempestivamente nella contabilità;
- garantire la tempestività, l'accuratezza e il rispetto del principio di competenza nell'effettuazione delle registrazioni contabili;
- assicurarsi che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima e coerente con la documentazione di supporto in modo da consentire la ricostruzione accurata dell'operazione;
- indicare elementi attivi per un ammontare superiore/inferiore a quello effettivo o elementi passivi fittizi (es. costi fittiziamente sostenuti e/o ricavi indicati in misura superiore/inferiore a quella reale) facendo leva su una falsa rappresentazione nelle scritture contabili obbligatorie e avvalendosi di mezzi idonei ad ostacolarne l'accertamento;
- indicare elementi passivi fittizi avvalendosi di fatture o altri documenti aventi rilievo probatorio analogo alle fatture, per operazioni inesistenti;
- applicare adeguate procedure di controllo in caso di sopravvenienze attive apparentemente non giustificate o in caso di registrazioni di incassi (e pagamenti) di cui non si riscontri una contropartita di credito (o debito) corrispondente;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte del Collegio sindacale o della Società di revisione;
- tenere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità Pubbliche di Vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

In particolare, agli amministratori è fatto divieto di:

- determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- procedere a formazione o aumenti fittizi del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di costituzione di nuove società o di aumento del capitale sociale;

- omettere di comunicare agli altri amministratori e al Collegio Sindacale, l'eventuale presenza di interessi, per conto proprio o di terzi, che abbiano in una operazione della Società, precisandone la natura, i termini, l'origine e la portata.

Inoltre, i Destinatari del Modello sono tenuti a:

- Rispettare puntualmente le regole aziendali in merito alla chiarezza ed alla completezza dei dati e delle notizie che ciascuna funzione deve fornire, ai criteri contabili per l'elaborazione dei dati e alle tempistiche per la loro consegna alle funzioni responsabili;
- Rispettare i criteri e le modalità previste dalle regole aziendali per l'elaborazione dei dati del bilancio civilistico e consolidato;
- Osservare scrupolosamente le regole e le procedure previste dalla Legge e dalle normative di settore per la valutazione e la selezione della Società di revisione;

E.4 Principi di controllo specifici

La Società ha adottato, oltre ai principi comportamentali sopra individuati, i seguenti principi di controllo specifici in relazione ai reati societari, con particolare riferimento ai processi strumentali alla commissione del reato di seguito riportati:

Formazione del bilancio e rapporti con gli organi di controllo

- attività di revisione legale dei conti svolta da parte di una Società di revisione;
- previsione di riunioni tra rappresentanti della Società di revisione, del Collegio Sindacale e dell'OdV;
- vigilanza, da parte del Collegio Sindacale, sull'effettivo mantenimento dell'indipendenza da parte della Società di revisione;
- istruzioni rivolte alle Funzioni, con cui si stabilisce quali dati e notizie debbano essere forniti ad Amministrazione e Bilancio in relazione alle chiusure annuali e infra-annuali (per i relativi documenti contabili societari), quali modalità e relativa tempistica, anche attraverso la formale definizione e verifica di un calendario delle operazioni di bilancio;
- monitoraggio dell'evoluzione della normativa di riferimento, al fine di garantire l'adeguamento alle novità normative in materia contabile;
- identificazione dei soggetti deputati alla gestione della contabilità generale e alla predisposizione ed approvazione del Bilancio e delle comunicazioni sociali;
- verifiche, supportate da evidenze formali, atte ad accertare la completezza delle informazioni presenti in fattura al fine di procedere al pagamento;
- segregazione delle funzioni tra chi provvede all'esecuzione dei pagamenti e chi provvede alla verifica di coerenza del benestare al pagamento;
- tracciabilità, attraverso i sistemi informativi aziendali, di tutte le fatture e verifica dell'esistenza di un benestare (fattura firmata, e-mail, comunicazione interna o altro) al fine di rendere la fattura pagabile;

- esistenza di un sistema di archiviazione delle registrazioni contabili;
- dall'archiviazione puntuale e precisa di tutta la documentazione relativa alle diverse fasi presso la segreteria del Consiglio di Amministrazione;
- trascrizione, pubblicazione e archiviazione del verbale di Assemblea ai sensi di legge.

Rapporti e adempimenti con gli Enti Pubblici e le Autorità Amministrative Indipendenti

- necessità che le seguenti fasi/attività del processo di gestione dei rapporti e degli adempimenti con gli Enti Pubblici e le Autorità Amministrative Indipendenti, non siano mai poste in essere dallo stesso soggetto:
  - predisposizione di dati/informazioni/documenti da fornire ai soggetti pubblici;
  - presentazione di dati/informazioni/documenti da fornire alla Pubblica Amministrazione;
- esistenza di direttive sulle modalità di condotta operativa da adottare nei contatti formali e informali intrattenuti con i diversi soggetti pubblici;
- formalizzazione degli eventuali rapporti con soggetti esterni (consulenti legali, terzi rappresentanti o altro) incaricati di svolgere attività di supporto, prevedendo nei contratti una specifica clausola che li vincoli al rispetto dei principi etico-comportamentali adottati da QUID INFORMATICA;
- rendiconto dei rapporti formali con rappresentanti della Pubblica Amministrazione e tracciabilità degli atti e delle fonti documentali che ne stanno alla base.
- partecipazione agli incontri con i funzionari pubblici dei rappresentanti della Società; la documentazione richiesta e consegnata (evidenziando ad es. data, obiettivi, motivazioni, partecipanti), deve essere comunicata al responsabile archiviata e conservata;
- tracciabilità degli incontri svolti con il rappresentante della Pubblica Amministrazione attraverso la redazione di un elenco, con l'indicazione della data, dell'Ente, dell'interlocutore e dell'oggetto del rapporto;
- sottoscrizione delle comunicazioni dirette alla Pubblica Amministrazione nel rispetto dei poteri conferiti a soggetti della Società;
- approvazione da parte di adeguati livelli autorizzativi della documentazione da trasmettere in relazione alle richieste pervenute dalle Autorità;
- archiviazione e conservazione, a cura di ciascuna funzione, di tutta la documentazione prodotta nell'ambito della propria attività sensibile, ivi inclusa quella trasmessa alla Pubblica Amministrazione anche eventualmente in via telematica.

PARTE SPECIALE F – DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE

La presente Parte Speciale "F" si applica alle tipologie di reati identificati dall'art. 25-quinquies del Decreto.

F.1 Reati applicabili alla Società

L'ambito legislativo riguardante i delitti contro la personalità individuale è stato introdotto con la Legge 11 agosto 2003, n. 228 – che ha aggiunto l'art. 25-quinquies che richiama specifici articoli contenuti nella sezione I, capo III, titolo XII, libro II del codice penale, nonché modificato dalla L. n. 199/2016.

Con riguardo a tali reati, la Società ha valutato irrilevante il rischio di loro commissione, salvo che per il reato previsto e punito dall'art. 603-bis c.p. il cui rischio di commissione appare comunque remoto, atteso che la Società, nei confronti dei lavoratori, applica le previsioni e le tutele specificatamente previste dal Contratto Collettivo Nazionale di Lavoro. A scopo prudenziale, si considera a rischio l'ambito degli appalti di servizi e lavori (in relazione alla teorica estensione della responsabilità nei confronti del committente in presenza di contratti di appalto).

Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)

Il reato 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 primo punto, sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.

Costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni:

- 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.

Costituiscono aggravante specifica e comportano l'aumento della pena:

- il fatto che il numero di lavoratori reclutati sia superiore a tre;
- il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa;
- l'aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

F.2 Attività sensibili

In particolare, sono state individuate, tenuto conto del contesto operativo della Società e delle sue finalità istituzionali, le seguenti attività sensibili:

- Gestione dei sistemi IT;
- Comunicazione, ricerca e sviluppo, responsabilità sociale di impresa;
- Acquisizione e gestione di materiale utilizzato per personalizzare la gamma di prodotti/servizi (a titolo esemplificativo, immagini e video);
- Appalti di servizi e lavori (in relazione alla teorica estensione della responsabilità nei confronti del committente in presenza di contratti di appalto).

F.3 Regole Comportamentali

Al fine di evitare il verificarsi dei suddetti reati previsti dal D. Lgs. 231/2001, a tutti i Destinatari, è fatto divieto di:

- diffondere immagini, documenti o altro materiale pornografico riguardante i minori;
- porre in essere, promuovere, collaborare, o dare causa a comportamenti tali da integrare le fattispecie rientranti tra i reati contro la personalità individuale;
- conferire incarichi ad appaltatori e/o subappaltatori che non rispettino la normativa giuslavorista vigente.

Inoltre, i Destinatari del Modello sono tenuti a:

- considerare sempre prevalente la tutela dei diritti delle persone e dei lavoratori rispetto a qualsiasi considerazione economica;
- assicurare massima tracciabilità e trasparenza nella gestione dei rapporti con società che svolgono attività in appalto.

F.4 Principi di controllo specifici

La Società ha adottato, oltre ai principi comportamentali sopra individuati, i seguenti principi di controllo specifici, con particolare riferimento ai processi di seguito riportati:

Gestione dei contenuti dei prodotti/servizi offerti

- Strumenti informatici che impediscano l’accesso e/o la ricezione di materiale relativo alla pornografia minorile

- Svolgimento di un controllo di liceità di immagini contenute nei prodotti/servizi da parte di uno studio legale esterno;
- tracciabilità delle singole attività (documentazione a supporto, verbalizzazione delle decisioni, intestazione/formalizzazione dei documenti e modalità/tempistiche di archiviazione).

Acquisto di beni, servizi e consulenze

- adeguate clausole nei contratti di appalto a tutela dei lavoratori e della mano d'opera impiegata nell'appalto;
- attività di verifica dei requisiti dei fornitori in relazione al processo di qualificazione dei fornitori di beni e servizi secondo le vigenti procedure in ambito acquisti.

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

La presente Parte Speciale "G" si applica alle tipologie di reati identificati dall'art. 25-septies del Decreto.

Le norme antinfortunistiche e di tutela dell'igiene e della salute sul lavoro hanno come destinatari alcuni specifici soggetti e cioè il datore di lavoro, i dirigenti, i preposti ed i lavoratori; alcune specifiche disposizioni riguardano il responsabile del servizio di prevenzione e protezione ed il rappresentante per la sicurezza; in tema di cantieri temporanei mobili alcune specifiche disposizioni riguardano ancora il committente, il responsabile dei lavori ed i coordinatori per la sicurezza.

I reati di omicidio e di lesioni colpose commessi in violazione delle norme antinfortunistiche e di tutela dell'igiene e della salute sul lavoro interessano, a diverso titolo secondo le attribuzioni, i compiti e/o le responsabilità assegnate, principalmente i soggetti in questione.

G.1 Reati applicabili alla Società

La Legge 03 agosto 2007, n. 123 recante "Misure in tema di tutela della salute e della sicurezza sul lavoro e delega al Governo per il riassetto e la riforma della normativa in materia" ha inserito nel Decreto 231 l'art. 25-septies che prevede l'estensione della responsabilità amministrativa dell'ente ai delitti in materia di violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

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

Omicidio colposo (art. 589 c.p.)

Il reato si configura nel caso in cui si cagioni per colpa la morte di una persona.

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

Il reato si configura nel caso in cui si cagionino per colpa ad una persona lesioni gravi o gravissime, a seguito della violazione delle norme per la prevenzione degli infortuni sul lavoro.

Le lesioni si considerano gravi nel caso in cui: a) dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni; b) il fatto produce l'indebolimento permanente di un senso o di un organo (art. 583, comma 1, c.p.).

Le lesioni si considerano gravissime se dal fatto deriva: a) una malattia certamente o probabilmente insanabile; b) la perdita di un senso; c) la perdita di un arto o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella; d) la deformazione, ovvero lo sfregio permanente del viso 8art. 583, comma 2, c.p.).

Ai fini della integrazione dei suddetti reati, non è richiesto l'elemento soggettivo del dolo, ovvero la coscienza e la volontà di cagionare l'evento lesivo, ma la mera negligenza,

impudenza o imperizia del soggetto agente, ovvero l'inosservanza da parte di quest'ultimo di leggi, regolamenti, ordini o discipline (art. 43 c.p.).

G.2 Attività sensibili

In relazione ai reati e alle condotte criminose sopra esplicitate, l'attività considerata sensibile è l'espletamento e gestione degli adempimenti in materia di tutela della sicurezza e salute sul lavoro ai sensi del D. Lgs. 81/08 (Testo Unico Sicurezza), anche con riferimento all'articolo 26 (Obblighi connessi ai contratti di appalto d'opera o di somministrazione) in relazione ai rapporti di appalto continuativi, relativi ad esempio a manutenzioni, installazioni di impianti, di macchinari, attrezzature e all'ampliamento di impianti della Società.

Le principali attività sensibili individuate sono:

- Acquisto di beni, servizi e consulenze;

- gestione degli adempimenti in materia di salute e sicurezza degli impianti e dei luoghi di lavoro;

A tal fine è stato predisposto il documento di valutazione dei rischi che ha analizzato ogni ipotetico rischio che i lavoratori potrebbero dover affrontare; tale documento deve essere soggetto a modifiche, qualora le esperienze maturate suggeriscano la necessità di implementare il livello di sicurezza in ambito aziendale.

QUID INFORMATICA si adopera al fine di promuovere l'attività di informazione e formazione dei lavoratori che viene svolta puntualmente per dare attuazione, nel modo più ampio e completo possibile, al rispetto della legislazione in materia di salute e sicurezza sul lavoro; viene prestata, inoltre, particolare attenzione affinché ogni lavoratore sia provvisto ed utilizzi i dispositivi di protezione individuale previsti dalla legislazione.

Viene, ancora, seguita con particolare attenzione l'attività che è stata appaltata a soggetti – aziende esterne -, questi devono essere scelti in ragione della loro comprovata capacità e devono essere sensibilizzati ad operare mediante la puntuale osservanza delle norme che disciplinano la materia oggetto del presente capitolo.

G.3 Regole Comportamentali

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

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

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-septies del d.lgs. 231/2001);
- violare i principi previsti nella presente parte speciale.

Si precisa che in materia di salute e sicurezza sul lavoro, la Società si è dotata di una struttura organizzativa conforme a quella prevista dalla normativa prevenzionistica vigente, nell'ottica di eliminare, ovvero, laddove ciò non sia possibile, ridurre – e quindi gestire – i rischi lavorativi per i lavoratori; sono stati, inoltre, definiti i compiti e le responsabilità in

materia di salute e sicurezza sul lavoro a partire dal Datore di Lavoro fino al singolo Lavoratore.

Per i principi generali di comportamento si rimanda, pertanto, al Documento Generale di Valutazione Rischi predisposto ai sensi del D. Lgs. 81/08 ed adottato da QUID INFORMATICA, nonché a tutte le procedure interne in tema di sicurezza sul lavoro implementate dall'Organizzazione.

G.4 Principi di controllo specifici

La Società ha adottato, oltre ai principi comportamentali sopra individuati, principi di controllo specifici in relazione ai reati previsti dalla presente parte speciale, con particolare riferimento al processo "Adempimenti in materia di salute e sicurezza ex D. Lgs 81/08", individuato come quello nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato.

Relativamente a tale processo strumentale/funzionale individuato, di seguito sono riportati i principi specifici di controllo minimali a cui si deve ispirare l'operatività degli stessi:

- Monitorare l'adeguatezza del Documento di Valutazione dei Rischi rispetto alle caratteristiche dei luoghi di lavoro, risorse umane ed organizzazione;
- Effettuare la formazione prevista dalla normativa vigente per tutti i soggetti coinvolti nel processo (lavoratori, preposti, dirigenti ecc.);
- Manutenere macchine ed impianti secondo le indicazioni e tempistiche fornite dai fabbricanti e/o dalla normativa vigente e registrare gli esiti di tali attività;
- Verificare periodicamente l'efficacia dei Piani e Procedure di Emergenza e registrare gli esiti di tale attività;
- Monitorare lo stato di salute dei lavoratori come previsto dai Protocolli Sanitari e registrare gli esiti di tali attività.

PARTE SPECIALE H – REATI DI RICICLAGGIO, RICETTAZIONE, IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA NONCHÉ AUTORICICLAGGIO

La presente Parte Speciale "H" si applica alla tipologia di reati identificati dall'art. 25-octies del Decreto.

H.1 Reati applicabili alla Società

Il Decreto Legislativo 21 novembre 2007, n. 231 relativo all'attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, nonché della direttiva 2006/70/CE che ne reca misure di esecuzione, ha introdotto nel Decreto 231 l'art.25-octies che estende l'ambito della responsabilità amministrativa degli enti in relazione ai reati di riciclaggio (art. 648-bis c.p.), ricettazione (art. 648 c.p.) e impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.). Inoltre, l'art. 3 della Legge n. 186/2014 ha introdotto il reato di autoriciclaggio all'art. 648-ter.1 c.p., prevedendo altresì il suo inserimento all'interno dell'art. 25-octies del D. Lgs. 231/2001.
Il D.Lgs. 8 novembre 2021, n. 195, ha apportato modifiche ai seguenti articoli del codice penale, a decorrere dal 15 dicembre 2021: (i) articolo 648; articolo 648-bis; articolo 648-ter; articolo 648-ter.1 ed ha esteso la punibilità dei reati sopramenzionati ai proventi derivati anche da delitti colposi e contravvenzioni (queste ultime punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi)

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

Ricettazione (art. 648 c.p.)

Commette il reato di ricettazione chiunque, fuori dai casi di concorso nel reato, acquista, riceve od occulta, denaro o cose provenienti da un qualsiasi delitto al fine di procurare a se od ad altri un profitto, o comunque si intromette nel farle acquistare, ricevere od occultarle.

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

Fuori dei casi di concorso nel reato, commette il delitto di riciclaggio chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da un delitto ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione delittuosa della loro provenienza.

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

Tale norma dispone inoltre che, al di fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 (ricettazione) e 648-bis (riciclaggio), commette il delitto di impiego di denaro, beni o altre utilità di provenienza illecita chiunque "impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto".

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

Il reato consiste nel fatto di chi, avendo commesso direttamente o concorso con altri a commettere un delitto, 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. In tal senso, non sarà punibile nell'ipotesi in cui i beni siano destinati alla mera utilizzazione o al godimento personale.

H.2 Attività sensibili

Le attività che la Società ha individuato come sensibili, nell'ambito dei reati di riciclaggio, ricettazione, impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Relativamente alla tipologia di reato di autoriciclaggio, l'analisi delle attività sensibili si è focalizzata sulla condotta propria della fattispecie di reato applicabile e, in via prudenziale, su alcune attività sensibili che sono indentificate in dottrina come potenziali reati fonte nell'ambito delle organizzazioni di impresa (es. reati tributari).

Premesso quanto precede, in relazione ai reati di riciclaggio, ricettazione, impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio sono state individuate le seguenti attività sensibili:

- Attività di selezione del fornitore e stipula dei contratti di acquisto di beni:
    - acquisto di beni, servizi e consulenze;
    - rapporti con intermediari e agenti;
- Gestione dei flussi monetari e finanziari, con particolare riferimento a:
    - apertura e/o chiusura e gestione dei c/c bancari e riconciliazioni bancarie;
    - gestione del credito: verifica dello stato dei crediti e del pagamento delle relative fatture;
    - gestione dei pagamenti;
    - gestione della piccola cassa;
    - gestione dei flussi finanziari con le associate;
    - gestione investimenti;
    - sponsorizzazioni;
    - omaggi e donazioni.
- Pagamenti e incassi.
    - Tesoreria
    - Camera di compensazione
- Gestione della fiscalità aziendale, con particolare riferimento alle seguenti attività:
    - compilazione, tenuta e conservazione delle scritture contabili rilevanti ai fini

fiscali e degli altri documenti di cui è obbligatoria la conservazione;

- predisposizione delle dichiarazioni fiscali;
- liquidazione delle imposte;

H.3 Regole Comportamentali

Al fine di prevenire il verificarsi dei suddetti reati previsti dal D.Lgs. 231/2001, a tutti i Destinatari, è fatto divieto di:

- Effettuare qualunque tipo di pagamento nell'interesse della Società in mancanza di adeguata documentazione di supporto;
- Ricevere o accettare la promessa di pagamento in contanti, in alcun modo, in alcuna circostanza, o compiere operazioni che presentino il rischio di essere implicati in vicende relative a riciclaggio di denaro proveniente da attività criminali;
- Utilizzare strumenti anonimi per il compimento di azioni o di operazioni di trasferimento di importi rilevanti;
- Utilizzare contante o altro strumento finanziario al portatore (fermo restando eventuali eccezioni dettate da esigenze operative/ gestionali oggettivamente riscontrabili, sempre per importi limitati e comunque rientranti nei limiti di legge), per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie, nonché il divieto di utilizzo di conti correnti o libretti di risparmio in forma anonima o con intestazione fittizia;
- Effettuare versamenti su conti correnti cifrati o presso istituti di credito privi di insediamenti fisici;
- Emettere fatture o rilasciare documenti per operazioni inesistenti al fine di consentire a terzi di commettere un'evasione fiscale;
- Indicare elementi passivi fittizi avvalendosi di fatture o altri documenti aventi rilievo probatorio analogo alle fatture per operazioni inesistenti.

Inoltre i Destinatari sono tenuti a:

- Valutare, secondo i dettami di cui alla normativa vigente in materia di pubblici appalti, l'affidabilità dei fornitori;
- Valutare l'affidabilità dei clienti con modalità che consentano di verificarne la correttezza professionale;
- Garantire l'attuazione del principio di segregazione dei ruoli in relazione alle attività di gestione della contabilità aziendale e nella successiva trasposizione nelle dichiarazioni tributarie, anche attraverso la predisposizione di specifiche procedure;
- Custodire in modo corretto ed ordinato le scritture contabili e gli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali, approntando difese fisiche e/o informatiche che impediscano eventuali atti di distruzione e/o occultamento;
- Rispettare i termini e le modalità previsti dalla normativa applicabile per la predisposizione delle dichiarazioni annuali e per i conseguenti versamenti relativi alle

imposte sui redditi e sul valore aggiunto.

H.4 Principi di controllo specifici

La Società ha adottato, oltre ai principi comportamentali sopra individuati, i seguenti principi di controllo specifici in relazione ai potenziali reati previsti dalla presente Parte speciale, con particolare riferimento ai processi strumentali alla commissione del reato quali il processo di acquisto di beni, servizi e consulenze, il processo di gestione dei flussi monetari e finanziari ed il processo di formazione del bilancio e rapporti con gli organi di controllo.

Acquisto di beni, servizi e prestazioni professionali

- Necessità che le seguenti fasi/attività del processo di acquisti di beni e servizi non siano mai poste in essere dallo stesso soggetto:

  - richiesta della fornitura;
  - effettuazione dell'acquisto;
  - certificazione dell'esecuzione dei servizi/consegna dei beni (rilascio benestare);
  - effettuazione del pagamento;

- Esistenza di criteri tecnico-economici per:

  - la selezione di potenziali fornitori (qualificazione ed inserimento nell'albo fornitori);
  - la validazione della fornitura e dei beni/servizi forniti;
  - valutazione complessiva dei fornitori;

- Espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte sulla base di criteri oggettivi e documentabili;
- Esistenza di livelli di approvazione per la formulazione delle richieste di acquisto e per la certificazione della fornitura/erogazione;
- Esistenza di livelli autorizzativi, in coerenza con il sistema delle procure aziendali, per la stipulazione di contratti e l'approvazione delle relative varianti/integrazioni;
- Necessità che le seguenti fasi/attività del processo di acquisti di consulenze non siano mai poste in essere dallo stesso soggetto:
  - richiesta della consulenza/prestazione;
  - autorizzazione;
  - definizione contrattuale;
  - certificazione dell'esecuzione dei servizi (rilascio benestare);
  - effettuazione del pagamento;
- Esistenza di requisiti professionali, economici ed organizzativi a garanzia degli standard qualitativi richiesti (Albo Fornitori) e di meccanismi di valutazione complessiva del servizio reso;
- Esistenza di livelli di approvazione per la formulazione delle richieste di prestazione e per la certificazione/validazione del servizio reso;

- Esistenza di livelli di approvazione delle richieste;
- Esistenza di livelli autorizzativi (in coerenza con il sistema di procure aziendale) per la stipulazione di contratti e l'approvazione delle relative varianti/integrazioni;
- Tracciabilità delle singole fasi del processo (documentazione a supporto, livello di formalizzazione e modalità/tempistiche di archiviazione), per consentire la ricostruzione delle responsabilità, della motivazione delle scelte e delle fonti informative;
- Firma della RdA da parte dell'Ufficio richiedente al fine di comprovare l'esistenza dei livelli di approvazione, invio di copia della RdA all'Ufficio Acquisti e successiva archiviazione della stessa da parte dell'Ufficio Richiedente, in forma cartacea e/o digitale;
- Certificazione dell'esecuzione dei servizi/consegna dei beni da parte del fornitore mediante la firma dell'Ufficio Richiedente sul documento di riferimento (Documento di Trasporto o Rapporto di servizio) e successiva archiviazione dello stesso da parte dell'Ufficio Acquisti.

Gestione dei flussi monetari e finanziari

- Necessità che le seguenti fasi/attività del processo non siano mai poste in essere dallo stesso soggetto:
    - richiesta dell'ordine di pagamento o di messa a disposizione;
    - effettuazione del pagamento;
    - controllo/riconciliazione a consuntivo;
- Esistenza di livelli autorizzativi sia per la richiesta, che per l'ordine di pagamento o di messa a disposizione, articolati in funzione della natura dell'operazione (ordinaria/straordinaria) e dell'importo;
- Esistenza di un flusso informativo sistematico che garantisca il costante allineamento tra procure, deleghe operative e profili autorizzativi;
- Esistenza e diffusione di *specimen* di firma in relazione ai livelli autorizzativi definiti per la richiesta;
- Effettuazione di periodica attività di riconciliazione, sia dei conti *intercompany*, sia dei conti intrattenuti con banche;
- Tracciabilità degli atti e delle singole fasi del processo, con specifico riferimento ai documenti che hanno originato le operazioni di incasso e/o pagamento.
- Effettuazione dei pagamenti relativi all'acquisto di beni solo a seguito di verifica del ricevimento dei beni stessi e la verifica delle relative fatture.

Formazione del bilancio e rapporti con gli organi di controllo

- Attività di revisione legale dei conti svolta da parte di una Società di revisione;
- Previsione di riunioni tra rappresentanti della Società di revisione, del Collegio Sindacale e dell'OdV;

- Istruzioni rivolte alle Funzioni, con cui si stabilisce quali dati e notizie debbano essere forniti ad Amministrazione e Bilancio in relazione alle chiusure annuali e infra-annuali (per i relativi documenti contabili societari), con quali modalità e la relativa tempistica;
- Monitoraggio dell'evoluzione della normativa di riferimento, al fine di garantire l'adeguamento alle novità normative in materia contabile, e comunicazione delle suddette novità alla Società;
- Rispetto di compiti, ruoli e responsabilità definiti dall'organigramma e nel rispetto delle procure e deleghe in essere;
- Rispetto di un iter approvativo di tutte le registrazioni di contabilità generale da parte dei responsabili;
- Identificazione dei soggetti deputati alla gestione della contabilità generale e alla predisposizione ed approvazione del Bilancio e delle comunicazioni sociali;
- Verifiche, supportate da evidenze formali, atte ad accertare la completezza delle informazioni presenti in fattura al fine di procedere al pagamento;
- Segregazione delle funzioni tra chi provvede all'esecuzione dei pagamenti e chi provvede alla verifica di coerenza del benestare al pagamento;
- Tracciabilità, attraverso i sistemi informativi aziendali, di tutte le fatture e verifica dell'esistenza di un benestare (fattura firmata, e-mail, comunicazione interna o altro) al fine di rendere la fattura pagabile;
- Formale definizione e verifica di un calendario delle operazioni di bilancio;
- Esistenza di un sistema di archiviazione delle registrazioni contabili;
- Custodia delle scritture contabili e degli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali, con l'adozione di difese fisiche e/o informatiche che impediscano eventuali atti di distruzione e/o occultamento.

Operazioni societarie ordinarie e straordinarie

- conservare la documentazione a supporto delle operazioni finanziarie e societarie, adottando tutte le misure di sicurezza necessarie;
- deliberare eventuali operazioni societarie straordinarie nel rispetto di tutte le procedure interne e di legge, e solo a fronte di adeguate analisi e valorizzazioni;
- assicurare il rispetto dei poteri delegati, nonchè adeguate procedure di autorizzazione e controllo da parte delle strutture preposte, per la gestione di eventuali operazioni straordinarie o operazioni societarie / sul capitale di società controllate (diluizione o liquidazione di società, delibere di ricapitalizzazione, etc);
- segnalare eventuali indicatori di anomalia.

H5 Indicatori di anomalia

QUID INFORMATICA richiede alle Funzioni e agli esponenti aziendali di segnalare prontamente eventuali situazioni di potenziale anomalia che dovessero ravvisare in talune operazioni negoziali con controparti (esterne o correlate) o in transazioni finanziarie.

Se non adeguatamente motivate e giustificate, tali situazioni sono da considerarsi preclusive del perfezionamento di un rapporto finanziario/commerciale con QUID INFORMATICA, in linea con i divieti sopra esposti.

A titolo indicativo e non esaustivo, sono considerati “indicatori di anomalia”, i seguenti:

- Indicatori di anomalia relativi a comportamenti della controparte:
    - la controparte si mostra riluttante a fornire informazioni circa l’identità dei propri rappresentanti, le proprie sedi, o sugli intestatari o la localizzazione dei conti bancari che intende utilizzare per l’operazione con QUID INFORMATICA;
    - emerge che la controparte abbia fornito informazioni significativamente difformi da quelle desumibili da fonti pubbliche e indipendenti;
    - la controparte cambia frequentemente - o richiede di modificare - la ragione sociale e/o le proprie coordinate bancarie.
- Indicatori di anomalia connessi al rapporto commerciale o alle operazioni finanziarie:
    - operazioni che paiono notevolmente svantaggiose per la controparte o non allineate ai prezzi di mercato, oppure in nessun modo giustificate;
    - richieste dalla controparte di perfezionare l’operazione (o il pagamento) intestandola ad un soggetto terzo, se non per giustificate e comprovate ragioni (es. vincoli a favore di terzi);
    - pagamento di compensi ad amministratori a titolo di consulenza;
    - pagamenti effettuati per attività svolte da controparti italiane o dell’Unione Europea, ma accreditate su conti correnti di società in paesi ”non collaborativi;
    - incassi di significativo ammontare o reiterati nel tempo, da parti correlate o da terzi, apparentemente non giustificati da alcun titolo negoziale con QUID INFORMATICA;
    - sponsorizzazioni o donazioni per importi sensibili a Fondazioni o Onlus non meglio individuate;
    - stipula di rapporti contrattuali con vincoli o pegni a favore di terzi che non presentano alcun collegamento con la controparte.

PARTE SPECIALE I – REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

La presente Parte Speciale "I" si applica alle tipologie di reati identificati dall'art. 25-novies del Decreto.

In particolare la Parte Speciale, dopo una descrizione dei reati applicabili, identifica le attività sensibili, indica le regole comportamentali, i principi di controllo specifici che tutti i Destinatari del presente Modello devono adottare ed applicare al fine di prevenire il verificarsi dei reati sopra specificati.

I.1 Reati applicabili alla Società

La Legge 23 luglio 2009, n. 99 recante "Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia" ha inserito nel Decreto 231 l'art. 25-novies che prevede l'estensione della responsabilità amministrativa dell'ente ai delitti in materia di violazione del diritto d'autore.

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

Divulgazione tramite reti telematiche di un'opera dell'ingegno protetta (art. 171, comma 1, lett. a-bis e comma 3. Legge sul Diritto d'Autore)

In relazione alla fattispecie delittuosa di cui all'art. 171 della Legge sul Diritto d'Autore, il Decreto ha preso in considerazione esclusivamente due fattispecie, ovvero:

- la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa;
- la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno 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 o alla reputazione dell'autore.

Se dunque nella prima ipotesi ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere lese le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete, nella seconda ipotesi il bene giuridico protetto non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera, ma il suo onore e la sua reputazione.

Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, 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 un programma per elaboratori (art. 171-bis, Legge 633/1941)

Punisce chi 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); ovvero chi, 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.

Tale norma è posta a tutela penale del software e delle banche dati. Con il termine "software", si intendono i programmi per elaboratore, in qualsiasi forma espressi, purché originali, quale risultato della creazione intellettuale dell'autore; mentre con "banche dati", si intendono le raccolte di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo.

Art. 171-ter, Legge 633/1941

È punita (art. 171-ter comma 1):

- L'abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di 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 (lett. a);
- L'abusiva riproduzione, trasmissione o diffusione in pubblico, con qualsiasi procedimento, di 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 (lett. b);
- Pur non avendo concorso alla duplicazione o riproduzione, l'introduzione nel territorio dello Stato, la detenzione per la vendita o la distribuzione, o la distribuzione, la messa in commercio, la concessione in noleggio o la cessione a qualsiasi titolo, la proiezione in pubblico, la trasmissione a mezzo della televisione con qualsiasi procedimento, la trasmissione a mezzo radio, l'ascolto in pubblico delle duplicazioni o riproduzioni abusive di cui alle lettere a) e b) (lett. c);
- La detenzione per la vendita o la distribuzione, la messa in commercio, la vendita, il noleggio, la cessione a qualsiasi titolo, la proiezione in pubblico, la trasmissione a mezzo della radio o della televisione con qualsiasi procedimento, di videocassette, musicassette, di qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, o altro supporto per il quale è prescritta, ai sensi della legge, l'apposizione di contrassegno da parte della SIAE, privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato (lett. d);
- In assenza di accordo con il legittimo distributore, la ritrasmissione o diffusione con qualsiasi mezzo di un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato (lett. e);

- L'Introduzione nel territorio dello Stato, la detenzione per la vendita o la distribuzione, la distribuzione, la vendita, la concessione in noleggio, la cessione a qualsiasi titolo, la promozione commerciale, l'installazione di dispositivi o elementi di decodificazione speciale che consentono l'accesso a un servizio criptato senza il pagamento del canone dovuto (lett. f);
- La fabbricazione, l'importazione, la distribuzione, la vendita, il noleggio, la cessione a qualsiasi titolo, la pubblicizzazione per la vendita o il noleggio, o la detenzione per scopi commerciali, di attrezzature, prodotti o componenti ovvero la prestazione di servizi aventi la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di protezione ovvero progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di tali misure (lett. f-bis);
- L'abusiva rimozione o alterazione di informazioni elettroniche sul regime dei diritti di cui all'articolo 102-quinquies, ovvero la distribuzione, importazione a fini di distribuzione, diffusione per radio o per televisione, comunicazione o messa a disposizione del pubblico di opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse (lett. h);
- abusivamente, anche con le modalità indicate al comma 1 dell'articolo 85-bis del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, esegue la fissazione su supporto digitale, audio, video o audiovideo, in tutto o in parte, di un'opera cinematografica, audiovisiva o editoriale ovvero effettua la riproduzione, l'esecuzione o la comunicazione al pubblico della fissazione abusivamente eseguita (lett. h-bis).

È punita (art. 171-ter comma 2):

- La riproduzione, la duplicazione, la trasmissione o la diffusione abusiva, la vendita o comunque la messa in commercio, la cessione a qualsiasi titolo o l'importazione abusiva di oltre 50 copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi (lett. a);
- La comunicazione al pubblico, attraverso l'immissione a fini di lucro in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera o parte di un'opera dell'ingegno protetta dal diritto d'autore, in violazione del diritto esclusivo di comunicazione al pubblico spettante all'autore (lett. a-bis);
- La realizzazione delle condotte previste dall'art. 171-ter, co. 1, Legge 633/1941, da parte di chiunque eserciti in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, ovvero importazione di opere tutelate dal diritto d'autore e da diritti connessi (lett. b);
- La promozione od organizzazione delle attività illecite di cui all'art.171-ter, comma 1, Legge 633/1941 (lett. c).

Art. 171-septies, Legge 633/1941

E' punita (art. 171-septies):

- L'Immissione in commercio o importazione di supporti non soggetti all'obbligo del c.d.

"bollino SIAE" (i.e. supporti contenenti programmi per elaboratore di cui all'articolo 181-bis, terzo comma, l. 633/1941) e mancata comunicazione alla SIAE dei dati necessari per procedere all'identificazione di tali supporti;

- La falsa attestazione alla SIAE da parte della Società dell'assolvimento degli obblighi derivanti dalla normativa sul diritto d'autore e diritti connessi, ai fini dell'ottenimento del contrassegno.

I.2 Attività sensibili

Le attività che la Società ha individuato come sensibili, nell'ambito dei reati in materia di violazione del diritto d'autore unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

In relazione ai reati in materia di violazione del diritto d'autore sono state individuate le seguenti attività sensibili:

- Riproduzione e diffusione, anche mediante il sito istituzionale, di opere tutelate dal diritto di autore e dai diritti connessi;
- Acquisizione e gestione di materiale coperto da diritto d'autore utilizzato per personalizzare la gamma di prodotti offerti al cliente;
- Uso di software soggetti a licenze nell'ambito dei sistemi informativi aziendali;
- Condivisione di contenuti non protetti da password oppure, a seconda della criticità canale trasmissivo non crittografato;
- Supporti informatici non crittografati e non custoditi in archivi chiusi a chiave o, a seconda del grado di criticità, in armadi blindati;
- Acquisto di beni, servizi e consulenze;
- Iniziative di marketing e commerciale;
- Comunicazione, ricerca e sviluppo, responsabilità sociale di impresa;
- Assunzione del personale;
- Acquisizione e gestione di materiale coperto da diritto d'autore per la predisposizione e la diffusione al pubblico di brochure e presentazioni per la promozione delle offerte commerciali e dei prodotti della Società.

I.3 Regole Comportamentali

Al fine di evitare il verificarsi dei suddetti reati previsti dal D.Lgs. 231/2001, a tutti i Destinatari, è fatto divieto di:

- Utilizzare illecitamente materiale tutelato dall'altrui diritto d'autore;
- Utilizzare software privi delle necessarie autorizzazioni/licenze nell'ambito dei sistemi informativi aziendali;
- Duplicare e/o diffondere in qualsiasi forma programmi e file se non nelle forme e per gli scopi di servizio per i quali sono stati assegnati e nei termini (vincoli d'uso) delle licenze ottenute;

- Riprodurre o diffondere, in qualunque forma e senza diritto, l'opera intellettuale altrui, in mancanza di accordi contrattuali formalizzati per iscritto con i relativi titolari per lo sfruttamento economico o in violazione dei termini e delle condizioni previste in detti accordi;
- Installare e utilizzare sistemi di *file sharing* non autorizzati;
- Utilizzare file multimediali sul proprio computer ottenuti in violazione della normativa sul diritto d'autore;
- Con particolare riguardo alla gestione del sito internet aziendale, diffondere immagini, documenti o altro materiale tutelati dalla normativa in materia di diritto d'autore.

Inoltre, i destinatari del Modello sono tenuti a:

- Assicurare il rispetto delle norme interne, comunitarie e internazionali poste a tutela della proprietà intellettuale;
- Utilizzare i software installati sulla postazione lavorativa (personal computer) o reperibili sulla rete aziendale, conformemente ai brevetti e/o ai termini delle licenze (vincoli d'uso) e per esclusive finalità lavorative;
- Promuovere il corretto uso di tutte le opere dell'ingegno, compresi i programmi per elaboratore e le banche di dati;
- Curare diligentemente gli adempimenti di carattere amministrativo connessi all'utilizzo di opere protette dal diritto d'autore, nell'ambito della gestione del sistema IT aziendale e nell'uso del web.

I.4 Principi di controllo specifici

La Società ha adottato, oltre ai principi comportamentali sopra individuati, i seguenti principi di controllo specifici in relazione ai reati previsti dalla presente parte speciale, con particolare riferimento ai processi strumentali alla commissione del reato di seguito riportati:

Gestione delle attività connesse alla comunicazione esterna

- Chiara identificazione dei soggetti aziendali deputati ad approvare i contenuti dei messaggi pubblicitari e di comunicazione;
- Formalizzazione all'interno di contratti standard con le controparti di clausole che garantiscono la Società sull'avvenuto rispetto delle obbligazioni di legge tra cui anche la normativa in tema di proprietà intellettuale;
- Chiara identificazione del soggetto deputato all'approvazione dei contenuti da pubblicare;
- Formale identificazione del soggetto deputato ad approvare e diffondere le comunicazioni verso l'esterno.

Gestione dei contenuti dei prodotti/servizi offerti

- Flussi documentali tra le funzioni aziendali competenti per i vari processi o sotto

processi e gli organi/enti deputati al rilascio di autorizzazioni e/o certificazioni attestanti la conformità alle prescrizioni di legge;

- Chiara identificazione dei soggetti aziendali deputati ad approvare i contenuti dei messaggi pubblicitari;
- Regolamentazione della fornitura di contributi fotografici tramite specifici contratti siglati con il detentore dei diritti e riportanti specifiche clausole sulla tutela del diritto d'autore;
- Verifica di eventuali diritti esistenti sul prodotto commercializzato o distribuito;
- Flussi documentali tra le funzioni aziendali competenti al fine di verificare la conformità del processo alle prescrizioni di legge;
- Verifica della corrispondenza delle dichiarazioni/certificazioni presentate con la documentazione di supporto;
- Svolgimento di un controllo di liceità di testi o immagini contenuti nei prodotti offerti ai clienti da parte di uno studio legale esterno;
- Tracciabilità delle singole attività (documentazione a supporto, verbalizzazione delle decisioni, intestazione/formalizzazione dei documenti e modalità/tempistiche di archiviazione).

Gestione dei sistemi informativi

- Regolamentazione degli acquisti di hardware e software tramite specifici contratti siglati con il produttore principale o con fornitori autorizzati dal produttore stesso e riportanti specifiche clausole sulla tutela del diritto d'autore;
- Accesso alle applicazioni, da parte del personale IT, garantito attraverso strumenti di autorizzazione;
- Formalizzazione da parte delle funzioni preposte all'attività di gestione dei sistemi delle banche dati dei requisiti di autenticazione ai sistemi per l'accesso ai dati e per l'assegnazione dell'accesso remoto agli stessi da parte di soggetti terzi quali consulenti e fornitori;
- Verifiche periodiche degli accessi effettuati dagli utenti, in qualsiasi modalità, ai dati, ai sistemi ed alla rete;
- Tracciabilità tramite le applicazioni delle modifiche ai dati ed ai sistemi compiute dagli utenti;
- Controllo tramite meccanismi, anche automatici, del rispetto dei divieti di installazione dell'utilizzo non autorizzato di sistemi di file sharing e software applicativi non autorizzati ed in assenza di licenza d'uso.

PARTE SPECIALE L – REATI DI "INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA"

La presente Parte Speciale "L" si applica alla tipologia di reato identificato dall'art. 25-decies del Decreto e segnatamente l'art. 377-bis c.p.

L.1 Reati applicabili alla Società

La Legge 3 agosto 2009, n.116 recante "Ratifica ed esecuzione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione" adottata dall'Assemblea Generale dell'ONU il 31 ottobre 2003 ha introdotto la responsabilità amministrativa degli enti per il reato di cui all'art. 377-bis c.p. "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria" (art. 25-decies del Decreto 231).

Il reato che è stato considerato potenzialmente realizzabile è il seguente:

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 377-bis c.p.)

L'art. 377-bis c.p. punisce il fatto di chi, mediante violenza o minaccia o con l'offerta o la promessa di danaro o altre utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci colui che è chiamato a rendere dichiarazioni utilizzabili in un procedimento penale, quando tale soggetto ha la facoltà di non rispondere.

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

L.2 Attività sensibili

L'attività che la Società ha individuato come sensibile, nell'ambito del reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

In relazione al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria è stata individuata la seguente attività sensibile:

- Gestione dei procedimenti penali che vedano coinvolta la Società suoi amministratori/dipendenti.

L.3 Regole Comportamentali

Al fine di evitare il verificarsi del suddetto reato previsto dal D.Lgs. 231/2001, a tutti i Destinatari, è fatto divieto di:

- Indurre un soggetto a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria nel corso di un procedimento penale, attraverso minaccia o violenza (coazione fisica o morale) al fine di occultare/omettere fatti che possano arrecare un danno alla Società;

- Ricorrere alla forza fisica, a minacce o all'intimidazione oppure promettere, offrire o concedere un'indebita utilità per indurre colui il quale può avvalersi della facoltà di non rispondere nel procedimento penale, a non rendere dichiarazioni o a rendere false dichiarazioni all'Autorità Giudiziaria, con l'intento di ottenere una pronuncia favorevole o determinare il conseguimento di altro genere di vantaggio per la Società;
- Riconoscere forme di liberalità o altre utilità a dipendenti o terzi che siano persone sottoposte alle indagini preliminari e imputati nel processo penale per indurli a omettere dichiarazioni o a falsare le stesse.

Inoltre, i destinatari del Modello sono tenuti a:

- Prestare una fattiva collaborazione e rendere dichiarazioni veritiere ed esaustivamente rappresentative dei fatti nei rapporti con l'Autorità Giudiziaria;
- Esprimere liberamente la propria rappresentazione dei fatti o ad esercitare la facoltà di non rispondere riconosciuta dalla legge e a mantenere il massimo riserbo relativamente alle dichiarazioni rilasciate ed al loro oggetto, ove le medesime siano coperte da segreto investigativo;
- Avvertire tempestivamente il loro diretto Responsabile di ogni atto di citazione a testimoniare e di ogni procedimento penale che li veda coinvolti, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata o comunque ad essa attinente.

L.4 Principi di controllo specifici

In relazione a tale tipologia di reato, considerate le peculiarità connesse alla sua ipotetica realizzazione, con particolare riferimento al processo strumentale alla commissione del reato quale la gestione dei rapporti e degli adempimenti con gli Enti Pubblici e le Autorità Amministrative Indipendenti, valgono essenzialmente i presidi di carattere generale individuati nel Modello e le regole di condotta sopra delineate, che disciplinano, complessivamente, gli aspetti etico-comportamentali che devono essere osservati dai destinatari del Modello Organizzativo.

PARTE SPECIALE M – REATI IN MATERIA AMBIENTALE

La presente Parte Speciale "M" si applica alle tipologie di reati identificati dall'art. 25-undecies del Decreto.

M.1 Reati applicabili alla Società

Il Decreto Legislativo 7 luglio 2011, n.121 recante Attuazione della direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della direttiva 2009/123/CE che modifica la direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni" ha inserito nel Decreto 231 l'art. 25-undecies che prevede l'estensione della responsabilità amministrativa dell'ente ai reati in materia ambientale, da ultimo modificato dalla Legge 137/2023 che ha inasprito la disciplina sanzionatoria prevista dal codice penale per gli art. 452-bis e 452-quater.

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

Attività di gestione dei rifiuti non autorizzate (con riferimento all'art. 256, commi 1, 3 e 5, D. Lgs. 152/2006)

Tale reato si configura qualora:

- Si effettui una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214, 215 e 216 del Codice Ambiente;
- Si realizzi o gestisca una discarica non autorizzata, da intendersi anche come il superamento dei limiti di tenuta e scarico dei rifiuti nel deposito temporaneo (limite temporale e/o volumetrico);
- Si effettuino attività non consentite di miscelazione di rifiuti.

M.2 Attività sensibili

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte speciale "M" del Modello, le attività ritenute più specificamente a rischio sono:

- Gestione dei rapporti con i soggetti pubblici (es. Regione, Ministero dell'Ambiente) nell'ambito delle attività legate all'ottenimento o al rinnovo di provvedimenti amministrativi quali autorizzazioni, licenze e permessi per la gestione dei rifiuti o nell'ambito di visite ispettive volte alla verifica della conformità alle prescrizioni previste dalla legislazione vigente in materia di gestione dei rifiuti;
- Gestione delle attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti.

M.3 Regole Comportamentali

Al fine di evitare il verificarsi dei suddetti reati previsti dal D.Lgs. 231/2001, a tutti i Destinatari, è fatto divieto di:

- Conferire l'attività di gestione dei rifiuti a soggetti non dotati di un'apposita autorizzazione per il loro smaltimento e recupero;
- Miscelare categorie diverse di rifiuti pericolosi (oppure rifiuti pericolosi con quelli non pericolosi);
- Impedire l'accesso agli insediamenti da parte del soggetto incaricato del controllo.

M.4 Principi di controllo specifici

La Società ha adottato, oltre ai principi comportamentali sopra individuati, principi di controllo specifici in relazione ai reati previsti dalla presente parte speciale, con particolare riferimento al processo "Gestione degli adempimenti in materia ambientale", individuato come quello nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato.

Relativamente a tale processo strumentale/funzionale individuato, di seguito sono riportati i principi specifici di controllo minimali a cui si deve ispirare l'operatività degli stessi:

- Etichettare i contenitori dei rifiuti per evitare miscelazioni degli stessi;
- Misure idonee ad impedire che vengano smaltiti, anche involontariamente, rifiuti pericolosi (ad es. toner) con quelli non pericolosi.

PARTE SPECIALE N – REATI DI "IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE"

La presente Parte Speciale "N" si applica alle tipologie di reati identificati dall'art. 25-duodecies del Decreto.

N.1 Reati applicabili alla Società

Il delitto di "impiego di cittadini di paesi terzi il cui soggiorno è irregolare" è stato introdotto nel novero dei c.d. "Reati Presupposto" del Decreto 231, all'art. 25-duodecies, dal D.Lgs. 16 luglio 2012, n. 109, il quale, entrato in vigore il 9 agosto 2012, disciplina l'attuazione della Direttiva 2009/52/CE.

Tale reato si configura qualora il soggetto che riveste la qualifica di datore di lavoro occupi alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, o sia stato revocato o annullato, laddove ricorrano le specifiche circostanze aggravanti previste dall'art. 22, comma 12-bis, del D.Lgs. 25 luglio 1998 n. 286, quali:

a) se i lavoratori occupanti 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 c.p.

In particolare le condizioni lavorative di cui al punto c) che precede riguardano l'esposizione dei lavoratori a situazioni di grave pericolo con riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

N.2 Attività sensibili

In relazione al reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare è stata individuata la seguente attività sensibile:

- Selezione e assunzione del personale dipendente e dei collaboratori (in relazione all'eventuale assunzione di lavoratori stranieri extracomunitari);
- Appalti di servizi e lavori (in relazione alla teorica estensione della responsabilità nei confronti del committente in presenza di contratti di appalto).

N.3 Regole Comportamentali

Al fine di evitare il verificarsi del suddetto reato previsto dal D.Lgs. 231/2001, a tutti i Destinatari, è fatto divieto di:

- Assumere lavoratori stranieri privi di permesso di soggiorno;
- Assumere o impiegare lavoratori il cui permesso sia scaduto – e per il quale non sia richiesto il rinnovo – revocato o annullato;
- Omettere carenze o irregolarità nella documentazione ricevuta dai potenziali candidati;
- Conferire incarichi ad appaltatori e/o subappaltatori che si avvalgano di dipendenti

stranieri privi di permesso di soggiorno regolare;

- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti i quali, sebbene risultino tali da non costituire di per sé reato, possano potenzialmente diventarlo.

Inoltre, i Destinatari del Modello sono tenuti a:

- Considerare sempre prevalente la tutela dei diritti delle persone e dei lavoratori rispetto a qualsiasi considerazione economica;
- Assicurare massima tracciabilità e trasparenza nella gestione dei rapporti con società che svolgono attività in appalto.

N.4 Principi di controllo specifici

La Società ha adottato, oltre ai principi comportamentali sopra individuati, i seguenti principi di controllo specifici in relazione al potenziale reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, con particolare riferimento ai processi strumentali alla commissione del reato quali il processo di selezione, assunzione e gestione del personale dipendente e dei collaboratori e il processo di acquisto di beni, servizi e consulenze.

Selezione, assunzione e gestione del personale dipendente e dei collaboratori

- Controlli previsti in fase di selezione e assunzione del personale, con particolare riguardo alla verifica del permesso di soggiorno valido e successiva attività di monitoraggio, in capo alle competenti funzioni, circa il permanere della situazione di regolarità dei permessi di soggiorno per tutta la durata del rapporto lavorativo.

Acquisto di beni, servizi e consulenze

- Clausole contrattuali che impegnino i fornitori a rispettare la normativa vigente in materia di assunzioni di personale extracomunitario.

PARTE SPECIALE O – RAZZISMO E XENOFOBIA

La presente Parte Speciale "O" si applica alle tipologie di reati di Razzismo e Xenofobia indicati nell'art. 25-terdecies del D. Lgs.231/2001.

O.1 Reati applicabili alla Società

Il delitto Proroga e istigazione a delinquere per motivi di discriminazione razziale, etica e religiosa (art. 604-bis c.p.) è stato aggiunto dal D.Lgs. n. 21/2018.

Il reato che è stato considerato potenzialmente realizzabile dalla Società è il seguente:

Il delitto Proroga e istigazione a delinquere per motivi di discriminazione razziale, etica e religiosa (art. 604-bis c.p.)

Salvo che il fatto costituisca più grave reato, è punito:
a) con la reclusione fino ad un anno e sei mesi o con la multa fino a 6.000 euro chi propaganda idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi;
b) con la reclusione da sei mesi a quattro anni chi, in qualsiasi modo, istiga a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi.

È vietata ogni organizzazione, associazione, movimento o gruppo avente tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi. Chi partecipa a tali organizzazioni, associazioni, movimenti o gruppi, o presta assistenza alla loro attività, è punito, per il solo fatto della partecipazione o dell'assistenza, con la reclusione da sei mesi a quattro anni. Coloro che promuovono o dirigono tali organizzazioni, associazioni, movimenti o gruppi sono puniti, per ciò solo, con la reclusione da uno a sei anni.

Si applica la pena della reclusione da due a sei anni se la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia della Shoa o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale.

O.2 Attività sensibili

In relazione al reato previsto dall' art. 25-terdecies del D.lgs. 231/2001 è stata individuata la seguente attività sensibile:

- Acquisizione e gestione di materiale utilizzato per personalizzare la gamma di prodotti offerti al cliente.

O.3 Regole Comportamentali

Al fine di evitare il verificarsi del suddetto reato previsto dal D.lgs. 231/2001, a tutti i Destinatari, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti della Società, è fatto divieto di:

- Approvare contenuti pubblicitari che istighino o incitino, in modo che derivi concreto pericolo di diffusione, al razzismo e/o alla xenofobia;

- Diffondere immagini, documenti o altro materiale che promuova l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia, della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6,7 e 8 dello Statuto della Corte penale internazionale, ratificato ai sensi della legge 12 luglio 1999, n. 232.

O.4 Principi di controllo specifici

La Società ha adottato, oltre ai principi comportamentali sopra individuati, i seguenti principi di controllo specifici in relazione al reato previsto dalla presente parte speciale, con particolare riferimento al processo strumentale alla commissione del reato di seguito riportato:

Gestione dei contenuti dei prodotti/servizi offerti

- Individuazione di ruoli e responsabilità dell'attività di verifica formalizzata di quanto acquistato dal punto di vista editoriale e la tracciabilità di tale verifica;
- Pluralità di controlli in merito ai contenuti editoriali delle testate nazionali pubblicate;
- chiara identificazione dei soggetti aziendali deputati ad approvare i contenuti delle testate giornalistiche e dei messaggi pubblicitari;
- Inserimento nei contratti stipulati con i collaboratori/giornalisti freelance di specifica informativa sulle norme comportamentali adottate dalla Società relativamente al Modello Organizzativo e al relativo Codice Etico, nonché sulle conseguenze che comportamenti contrari alle previsioni del Codice Etico, ai principi comportamentali che ispirano la Società e alle normative vigenti, possono avere con riguardo ai rapporti contrattuali.

PARTE SPECIALE P – REATI TRIBUTARI

La presente Parte Speciale "P" si applica alle tipologie di reati indicati nell'art. 25-quinquiesdecies del D. Lgs.231/2001.

P.1 Reati applicabili alla Società

La riforma dei reati tributari introdotta con la L. 19 dicembre 2019, n. 157, di conversione del D.L. 26 ottobre 2019, n. 124 (c.d. decreto fiscale), ha inserito l'art. 25 quinquiesdecies al D. Lgs. 231/2001, che indica per quali reati tributari (previsti cioè nel novellato D. Lgs. 74/2000) commessi per interesse o vantaggio dell'ente, possa determinarsi la responsabilità amministrativa:

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, art. 2 D. Lgs. n. 74/2000);
- dichiarazione fraudolenta mediante altri artifici, ex art. 3 del D. Lgs n. 74/2000;
- emissione di fatture o altri documenti per operazioni inesistenti, ex art. 8 del D. Lgs. n. 74/2000;
- occultamento o distruzione di documenti contabili, ex art. 10 del D. Lgs. n. 74/2000;
- sottrazione fraudolenta al pagamento di imposte, ex art. 11 del D. Lgs. 74/2000.

E le seguenti sanzioni pecuniarie:

- per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'art. 2, comma 1, d.lgs. 74/2000, la sanzione pecuniaria fino a cinquecento quote;
- per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'art. 2, comma 2-bis, d.lgs. 74/2000, la sanzione pecuniaria fino a quattrocento quote;
- per il delitto di dichiarazione fraudolenta mediante altri artifici previsto dall'art. 3, d.lgs. 74/2000, la sanzione pecuniaria fino a cinquecento quote
- per il delitto di emissione di fatture o altri documenti per operazioni inesistenti previsto dall'art. 8, d.lgs. 74/2000, comma 1, la sanzione pecuniaria fino a cinquecento quote;
- per il delitto di emissione di fatture o altri documenti per operazioni inesistenti previsto dall'art. 8, comma 2-bis, d.lgs. 74/2000, la sanzione pecuniaria fino a quattrocento quote;
- per il delitto di occultamento o distruzione di documenti contabili previsto dall'art. 10, d.lgs. 74/2000, la sanzione pecuniaria fino a quattrocento quote;
- per il delitto di sottrazione fraudolenta al pagamento di imposte previsto dall'art. 11, d.lgs. 74/2000, la sanzione pecuniaria fino a quattrocento quote.

In caso di profitto di rilevante entità la sanzione pecuniaria subisce un aumento di un terzo. Sono inoltre applicabili le sanzioni interdittive di cui all'art. 9, comma 2, d.lgs. 231/2001, lettere c) (divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio), lettera d) (esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi) e lettera e) (divieto di

pubblicizzare beni o servizi). L'intervento normativo si innesta nel contesto di una costante estensione della responsabilità amministrativa da reato dell'ente, determinata anche da un intervento europeo in tal senso (la direttiva UE 2017/1371) e da un clima politico, in materia penale, estremamente rigorista nei confronti dei reati dei c.d. "grandi evasori".

Con riferimento a quanto sopra, il D.Lgs. n. 75/2020 che attua la direttiva UE 2017/1371 (meglio nota come direttiva PIF) che armonizza nell'eurozona la normativa relativa alla lotta contro le frodi che ledono gli interessi finanziari dell'Unione europea. In particolare, dopo il comma 1 dell'art. 25 quinquiesdecies è inserito il seguente: *" 1-bis. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, si applicano all'ente le seguenti sanzioni pecuniarie: a) per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote; b) per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote; c) per il delitto di indebita* compensazione *previsto dall'articolo 10-quater, la sanzione pecuniaria fino a quattrocento quote;"*

L'ambito della punibilità dei reati tributari costituisce, accanto alle modifiche al codice penale, il fulcro della direttiva PIF. E uno dei pilastri del cambio di passo introdotti dal D. Lgs. n. 75/2020, è, di certo la punibilità del "tentativo di reato", escluso, sino all'avvento della riforma, nel nostro ordinamento dal comma 1 dell'art. 6 del D. Lgs. 74/2000, che prevede, al contrario, la comminazione delle pene esclusivamente nel caso di illecito consumato. In altre parole, viene operata un'estensione tale da superare il limite del tentativo, precedentemente previsto con riferimento ai reati tributari finanche a livello normativo, e inteso come confine invalicabile per la responsabilità penale-tributaria.

P.2 Attività sensibili

In relazione al reato previsto dall' art. 25-quinquiesdecies del D.lgs. 231/2001 sono state individuate le seguenti attività sensibili:

- Gestione dei flussi monetari e finanziari, con particolare riferimento a:
  - Apertura e/o chiusura e gestione dei c/c bancari e riconciliazioni bancarie;
  - Gestione degli incassi;
  - Gestione del credito: verifica dello stato dei crediti e delle relative fatture;
  - Gestione dei pagamenti;
  - Gestione della cassa;
- Selezione, negoziazione, stipula ed esecuzione di contratti di acquisto, ivi compresi gli appalti di lavori, riferita a soggetti privati, con particolare riferimento al ricevimento di beni e attività finalizzate all'attestazione di avvenuta prestazione dei servizi e di autorizzazione al pagamento specialmente in relazione ad acquisti di natura immateriale, tra cui: consulenze e incarichi professionali; spese di rappresentanza; attività di sviluppo e di software e servizi;
- Gestione della contabilità generale, con particolare riferimento alle attività di:
  - Rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi ed economici;
  - Corretta tenuta dei rapporti amministrativi con i terzi (e.g. clienti, fornitori) e relativa gestione contabile delle partite di debito /credito;

- Gestione amministrativa e contabile dei cespiti;
- Accertamenti di tutti gli altri fatti amministrativi in corso d'anno (e.g. costi del personale, penalità contrattuali, finanziamenti attivi e passivi e relativi interessi, ecc.);
- Acquisto di beni, servizi e consulenze;
- Gestione dei flussi finanziari con le associate;

- Collaborazione e supporto all'Organo Amministrativo per la predisposizione di situazioni patrimoniali funzionali alla realizzazione di:
  - Operazioni straordinarie;
  - Operazioni di aumento/riduzione del capitale sociale;
  - Altre operazioni su azioni o quote sociali o della società.
- Raccolta, aggregazione e valutazione dei dati contabili necessari per la predisposizione della bozza di Bilancio della Società, nonché delle relazioni allegate ai prospetti economico-patrimoniali di bilancio da sottoporre alla delibera del Consiglio di Amministrazione;
- Gestione dei rapporti con gli Organi di Controllo relativamente alle verifiche sulla gestione amministrativa/contabile e sul Bilancio d'Esercizio e con i Soci nelle attività di verifica della gestione aziendale;
- Tenuta delle scritture contabili e dei Libri Sociali;
- Collaborazione e supporto all'Organo Amministrativo nello svolgimento delle attività di ripartizione degli utili di esercizio, delle riserve e restituzione dei conferimenti;
- Collaborazione e supporto all'Organo Amministrativo per l'effettuazione delle operazioni di incremento/riduzione del capitale sociale o di altre operazioni su azioni della Società;
- Rapporti con soci, sindaci e revisori, ove nominati;
- Predisposizione della documentazione che sarà oggetto di discussione e delibera in Assemblea e gestione dei rapporti con tale Organo Sociale;
- Gestione dei rapporti e delle informazioni dirette alle Autorità Amministrative Indipendenti, anche in occasione di verifiche, ispezioni ed accertamenti.

P.3 Regole Comportamentali

Al fine di evitare il verificarsi dei suddetti reati previsti dal D. Lgs. 231/2001, a tutti i Destinatari, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti della Società, è fatto divieto di:

- rappresentare o trasmettere per l'elaborazione e la predisposizione dei bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale o finanziaria della società;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- indicare elementi attivi per un ammontare superiore/inferiore a quello effettivo o elementi passivi fittizi (es. costi fittiziamente sostenuti e/o ricavi indicati in misura superiore/inferiore a quella reale) facendo leva su una falsa rappresentazione nelle scritture contabili obbligatorie e avvalendosi di mezzi idonei ad ostacolarne l'accertamento;
- indicare elementi passivi fittizi avvalendosi di fatture o altri documenti aventi rilievo

probatorio analogo alle fatture, per operazioni inesistenti;

- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte del Collegio sindacale o della Società di revisione;
- tenere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità Pubbliche di Vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

P.4 Principi di controllo specifici

Formazione del bilancio e rapporti con gli organi di controllo

- attività di revisione legale dei conti svolta da parte di una Società di revisione;
- previsione di riunioni tra rappresentanti della Società di revisione, del Collegio Sindacale e dell'OdV;
- identificazione dei soggetti deputati alla gestione della contabilità generale e alla predisposizione ed approvazione del Bilancio e delle comunicazioni sociali;
- vigilanza, da parte del Collegio Sindacale, sull'effettivo mantenimento dell'indipendenza da parte della Società di revisione e la comunicazione all'OdV dei criteri di scelta della Società di revisione;
- ricezione di apposite lettere di attestazione della veridicità dei dati contenuti nei bilanci delle società controllate da parte dei Responsabili Amministrativi delle società stesse;
- istruzioni rivolte alle Funzioni, con cui si stabilisce quali dati e notizie debbano essere forniti ad Amministrazione e Bilancio in relazione alle chiusure annuali e infrannuali (per i relativi documenti contabili societari), quali modalità e relativa tempistica, anche attraverso la formale definizione e verifica di un calendario delle operazioni di bilancio;
- verifiche, supportate da evidenze formali, atte ad accertare la completezza delle informazioni presenti in fattura al fine di procedere al pagamento;
- segregazione delle funzioni tra chi provvede all'esecuzione dei pagamenti e chi provvede alla verifica di coerenza del benestare al pagamento;
- tracciabilità, attraverso i sistemi informativi aziendali, di tutte le fatture e verifica dell'esistenza di un benestare (fattura firmata, e-mail, comunicazione interna o altro) al fine di rendere la fattura pagabile;
- esistenza di un sistema di archiviazione delle registrazioni contabili;
- trascrizione, pubblicazione e archiviazione del verbale di assemblea ai sensi di legge;
- archiviazione e conservazione, a cura di ciascuna funzione, di tutta la documentazione prodotta;
- formalizzazione degli eventuali rapporti con soggetti esterni (consulenti legali, terzi rappresentanti o altro) incaricati di svolgere attività di supporto, prevedendo nei contratti una specifica clausola che li vincoli al rispetto dei principi etico-comportamentali adottati da QUID INFORMATICA.

PARTE SPECIALE Q – DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

La presente Parte Speciale "Q" si applica alle tipologie di reati identificati dall'art. 25- octies1 del Decreto.

Q.1 Reati applicabili alla Società

L'art. 3, comma 1, lett. a) del D.Lgs. 8 novembre 2021, n. 184, in attuazione della Direttiva UE 2019/713, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, ha introdotto l'art. 25-octies.1, D. Lgs. 231/01, rubricato "Delitti in materia di strumenti di pagamento diversi dai contanti".
Tale modifica ha comportato un ulteriore arricchimento del novero dei reati presupposto, che viene esteso ai delitti di:

a) Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 ter c.p.);

b) Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 quater c.p.);

c) Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640 ter c.p.)

I delitti di cui alle lettere a) e b) appartengono alla famiglia dei "Delitti contro la fede pubblica", mentre quello di cui alla lettera c) appartiene alla famiglia dei "Delitti contro il patrimonio". La *ratio* della loro collocazione nello stesso art. 25-octies.1 del D.Lgs. 231/2001 e in posizione di immediata contiguità e prosecuzione funzionale all'art. 25-octies, è quella di indicare, seppur implicitamente, le aree organizzative e i processi sensibili e potenzialmente a "rischio" di commissione dei reati stessi.
In relazione agli art. 493-quater e 640-ter c.p., tali delitti vengono in rilievo ai fini della responsabilità dell'ente, solo ove commessi nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale.
Il comma secondo dell'art. 25-octies.1, infine, è costruito come una clausola di riserva che apre le porte, ove il fatto non integri altro illecito amministrativo sanzionato più gravemente, ad ogni altro delitto previsto dal Codice penale "*contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio*", purché avente "*ad oggetto strumenti di pagamento diversi dai contanti*".
Fermo che l'art. 25-bis, D. Lgs. 231/01 già annovera quali reati presupposto alcuni delitti contro la fede pubblica, assumono rilievo, *ex* art. 25-octies.1, i delitti dall'art. 453 all'art. 458 c.p., riguardanti la falsità in monete ed in carte di pubblico credito, a condizione che l'oggetto materiale della condotta sia uno strumento di pagamento diverso dal contante.
La Legge 137/2023 avente ad oggetto la conversione in legge, con modificazioni, del Decreto-Legge 10 agosto 2023 n. 105 recate "disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistrature e della pubblica

amministrazione" ha apportato anche alcune modifiche al D. Lgs. 231/2001. Al riguardo, per quanto di pertinenza del presente capitolo, ha inserito nell'art. 25 octies-1 il reato di trasferimento fraudolento di valori (art. 512-bis c.p.).

a) Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti

Il reato punisce chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi o comunque ogni altro strumento di pagamento diverso dai contanti.

Il reato punisce inoltre chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

Le due ipotesi sono autonome e vi si può rispondere anche in concorso.

Astrattamente la commissione del reato di cui all'art. 493-ter c.p. non esclude la configurabilità del delitto di riciclaggio.

b) Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti

Salvo che il fatto costituisca più grave reato, il delitto in oggetto punisce chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a se' o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

c) Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale

Il reato è stato introdotto nel Codice penale nell'ambito di una più ampia modifica volta a disciplinare quei fenomeni criminali che si caratterizzano nell'uso distorto o nell'abuso della tecnologia informatica hardware e software (c.d. computer crimes) e, nello specifico, trova la sua genesi nella difficoltà di ricondurre le ipotesi incriminate nell'ambito applicativo della truffa.

Punisce chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.

Il bene giuridico tutelato dal delitto di frode informatica non può essere iscritto esclusivamente nel perimetro della salvaguardia del patrimonio del danneggiato, in quanto viene in discorso anche l'esigenza di salvaguardare la regolarità di funzionamento dei sistemi informatici, la tutela della riservatezza dei dati, spesso sensibili, ivi gestiti, e, infine, la stessa certezza e speditezza del traffico giuridico fondata sui dati gestiti dai diversi sistemi informatici.

e) Trasferimento fraudolento di valori

Salvo che il fatto costituisca più grave reato chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648 648-bis e 648-ter è punito con la reclusione da due a sei

anni.

Q.2 Attività sensibili

In relazione al reato previsto dall' art. 25-octies1 del D.lgs. 231/2001 sono state individuate la seguenti attività sensibili:

- riguardanti i flussi monetari e finanziari in entrata e uscita aventi l'obiettivo di assolvere le obbligazioni di varia natura contratte dalla Società, ovvero:

- gestione e ottimizzazione del ciclo operativo di tesoreria, costituito:
  - dagli incassi, inclusa la gestione dei crediti, e dai pagamenti di natura ordinaria, cioè relativi alla gestione operativa (clienti, fornitori, imposte e tasse, salari e stipendi, utenze, assicurazioni, ecc.);
  - dagli incassi, inclusa la gestione dei crediti, e dai pagamenti di natura straordinaria, cioè relativi alla gestione non operativa (aumenti/riduzioni di capitale, distribuzione di dividendi, vendita/acquisto di assets, ecc.);
  - dai flussi inter-company di natura commerciale e finanziaria

tramite le varie tipologie di mezzo di pagamento (bonifico, assegno, direct debit, ri.ba., lettera di credito, ecc.) e secondo procedure di tipo manuale e/o elettronico, con l'obiettivo di massimizzarne l'efficienza operativa e minimizzarne i costi;

- impiego di liquidità e finanziamenti;
- pianificazione, consuntivazione e controllo dei flussi finanziari, della posizione finanziaria e della borrowing capacity;
- gestione e utilizzo dei sistemi informatici circa le attività di definizione dei criteri e delle modalità operative volte ad un corretto utilizzo dei sistemi informatici e dei privilegi di accessi ai sistemi e ai servizi di Information Technology forniti dall'azienda.

Q.3 Regole Comportamentali

Al fine di evitare il verificarsi dei suddetti reati previsti dal D. Lgs. 231/2001, a tutti i Destinatari, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti della Società, a titolo meramente esemplificativo e non esaustivo, è fatto divieto di:

- aprire conti o libretti di risparmio in forma anonima o con intestazione fittizia e utilizzare conti aperti presso filiali in Paesi esteri ove ciò non sia correlato alla sottostante attività economica/commerciale;
- creare fondi a fronte di pagamenti non giustificati;
- detenere/trasferire denaro contante o libretti di deposito bancari o postali al portatore o titoli al portatore in euro o in valuta estera per importi, anche frazionati, complessivamente pari o superiori ai limiti indicati dalla normativa vigente;
- emettere assegni bancari e postali per importi pari o superiori ai limiti indicati dalla normativa vigente che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
- effettuare pagamenti non adeguatamente documentati e autorizzati;
- promettere o versare somme di denaro, anche attraverso soggetti terzi, a funzionari della Pubblica Amministrazione, anche a titolo personale, con la finalità di promuovere o favorire illecitamente gli interessi della Società;
- effettuare pagamenti o riconoscere compensi in favore di soggetti terzi che operino per conto della Società, che non trovino adeguata giustificazione in relazione al tipo di incarico

svolto;

- accettare pagamenti frazionati se non supportati da accordi commerciali (quali anticipo e saldo alla consegna e pagamenti rateizzati);
- utilizzare i beni aziendali e, in particolare, le dotazioni informatiche aziendali, per commettere o indurre alla commissione di reati o per perpetrare una truffa o una frode informatica a danno di terzi, per perseguire qualsiasi finalità contraria a norme di legge vigenti o che possa costituire una minaccia per l'ordine pubblico, la tutela dei diritti umani o il buon costume;
- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente ai sistemi informatici o telematici aziendali e/o di soggetti pubblici o privati anche al fine di acquisire illecitamente, alterare o cancellare dati e/o informazioni;
  - procurarsi, riprodurre, diffondere, comunicare o consegnare codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornire indicazioni o istruzioni idonee al predetto scopo;
  - procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare o, comunque, mettere a disposizione di altri apparecchiature, dispositivi o programmi informatici 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;
  - intercettare fraudolentemente e/o impedire e/o interrompere comunicazioni relative a sistemi informatici o telematici e/o intercorrenti tra più sistemi;
  - installare apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative sistemi informatici o telematici e/o intercorrenti tra più sistemi;
  - installare software non autorizzati, duplicare abusivamente software protetti da licenza, effettuare registrazioni o riproduzioni audiovisive, elettroniche, cartacee o fotografiche di documenti aziendali, salvo i casi in cui tali attività rientrino nel normale svolgimento delle funzioni affidate;
  - utilizzare programmi non originali;
  - utilizzare mezzi intesi a consentire o facilitare la rimozione arbitraria o l'elusione di protezioni di un software;
  - formare falsamente ovvero alterare o sopprimere, anche parzialmente, il contenuto, anche occasionalmente intercettato, di comunicazioni relative a sistemi informatici o telematici e/o intercorrenti tra più sistemi;
  - distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici altrui, dello Stato o di altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità;
  - distruggere, danneggiare, rendere, anche parzialmente, inservibili sistemi informatici o telematici altrui o di pubblica utilità o ostacolarne gravemente il funzionamento attraverso condotte di danneggiamento o l'introduzione o la trasmissione di dati, informazioni o programmi;
  - accedere senza autorizzazione a sistemi informativi utilizzati dalla Pubblica Amministrazione o di alterarne, in qualsiasi modo, il funzionamento o di intervenire con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a questo pertinenti per ottenere e /o modificare informazioni a vantaggio della Società, o comunque al fine di procurare un indebito vantaggio alla Società;
  - lasciare il proprio Personal Computer incustodito e senza protezione password;

- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
- memorizzare dati sensibili su cartelle non protette del PC aziendale senza formale autorizzazione da parte del Responsabile della Funzione di riferimento;
- raccogliere dati sensibili in un modo non pertinente e completo ovvero eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservare i dati sensibili in un modo tale da non consentire l'identificazione dell'interessato, ovvero per un periodo di tempo superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;
- occultare o distruggere corrispondenza o ogni altra documentazione relativa al presente Processo.

Q.4 Principi di controllo specifici

La Società ha adottato, oltre ai principi comportamentali sopra individuati, i seguenti principi di controllo specifici in relazione ai Delitti previsti dalla presente parte speciale, fra cui:

- Esistenza di soggetti diversi operanti nelle attività riguardanti i flussi monetari e finanziari in entrata e uscita aventi l'obiettivo di assolvere le obbligazioni di varia natura contratte dalla Società ;
- Esistenza di livelli autorizzativi per la richiesta o disposizione di pagamento, per la gestione dei crediti, dei finanziamenti articolati in funzione della natura dell'operazione e dell'importo;
- Esistenza di un flusso informativo sistematico che garantisca il costante allineamento fra procure, deleghe operative e profili autorizzativi residenti nei sistemi informativi;
- Effettuazione di periodica attività di riconciliazione dei conti intrattenuti con istituti di credito;
- Definizione delle norme operative per la gestione dei crediti commerciali come indicato;
- Valutazione preventiva da parte della Direzione preposta dell'iscrizione di perdite su crediti con o senza utilizzo del fondo svalutazione crediti;
- Tracciabilità degli atti e delle singole fasi del processo (con specifico riferimento all'annullamento dei documenti che hanno già originato un pagamento).
- Definizione di un sistema di sicurezza volto alla protezione e al controllo dei sistemi informativi aziendali;
- Esistenza di misure di accesso ai sistemi con credenziali di accesso;
- Esistenza di sistemi di impedimento di installazione di software o programmi non preventivamente autorizzati dalla Società sugli strumenti di lavoro assegnati;
- Esistenza di sistemi di impedimento di accesso a risorse IT mediate strumenti privati;
- Esistenza di policy specifiche per definire modalità di utilizzo dei diversi strumenti informatici e di mobile office;
- Definizione di un sistema di controllo volto alla definizione di adeguate misure di sicurezza, nonché al monitoraggio dell'uso degli strumenti informatici e telematici;

Eventuali modalità *non standard* (relative sia a operazioni di natura ordinaria sia straordinaria) devono essere considerate "in deroga" e soggette, pertanto, a criteri di autorizzazione e controllo specificamente definiti e riconducibili a:

- individuazione del soggetto che può richiedere l'operazione;
- individuazione del soggetto che può autorizzare l'operazione;
- indicazione, a cura del richiedente, della motivazione;
- designazione (eventuale) della risorsa abilitata all'effettuazione e alla autorizzazione dell'operazione attraverso procura *ad hoc*.

ALLEGATO A

1 Elenco fattispecie di reato ricomprese nel D.Lgs. 231/01

Sono elencati, di seguito, tutti i reati attualmente ricompresi nell'ambito di applicazione del Decreto suddivisi per macro-categorie.

1. Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (Art. 24, D.Lgs. n. 231/2001)) [articolo modificato dalla L. 161/2017, dal D. Lgs. 75/2020 e dalla L. 137/2023]

- Malversazione a danno dello Stato (art. 316-bis c.p.)
- Indebita percezione di erogazioni a danno dello Stato (art.316-ter c.p.)
- Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art.640, comma 2, n.1, c.p.)
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)
- Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)
- Frode nelle pubbliche forniture (art. 356 c.p.) (introdotto dal D.Lgs. n. 75/2020)
- Frode ai danni del Fondo europeo agricolo (art. 2 L. 23/12/1986, n. 898) (introdotto dal D.Lgs. n. 75/2020)
- Turbata libertà degli incanti (art. 353 c.p.) (introdotto dalla L. n. 137/2023)
- Turbata libertà del procedimento di scelta del contraente (art. 353 c.p.) (introdotto dalla L. n. 137/2023)

2. 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. 7/2016, dal D.Lgs. n. 8/2016 e dal D.L. n. 105/2019]

- Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.)
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.) [articolo modificato dalla Legge n. 238/2021]
- Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.) [articolo modificato dalla Legge n. 238/2021]
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) [articolo modificato dalla Legge n. 238/2021]
- Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-

quinquies c.p.) [articolo modificato dalla Legge n. 238/2021]

- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)
- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)
- Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)
- Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, D.L. 21 settembre 2019 n. 105)

3. Delitti di criminalità organizzata (Art. 24-ter, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 94/2009; modificato dalla L. 69/2015]

- Associazione per delinquere (art. 416 c.p.p.)
- Associazione di tipo mafioso (art. 416-bis c.p.) [modificato dalla L. n. 69/2015]
- Scambio elettorale politico-mafioso (art. 416-ter c.p.)
- Sequestro di persona a scopo di estorsione (art. 630 c.p.)
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74, DPR 9 ottobre 1990, n. 309)
- Tutti i delitti se commessi avvalendosi delle condizioni previste dall´art. 416-bis c.p. per agevolare l´attività delle associazioni previste dallo stesso articolo (L. n. 203/1991)
- Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (art. 407, comma 2, lett. a), numero 5), c.p.p.)

4. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (Art. 25, D.Lgs. n. 231/2001) [articolo modificato dalla L. n. 190/2012, dal L. n. 3/2019 e dal D. Lgs n. 75/2020]

- Concussione (art. 317 c.p.) [modificato dalla L. n. 69/2015]
- Corruzione per l'esercizio della funzione (art. 318 c.p.) [articolo modificato dalla L. n. 190/2012, L. n. 69/2015 e L. n. 3/2019]
- Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.) [modificato dalla L. n. 69/2015]

- Circostanze aggravanti (art. 319-bis c.p.)
- Corruzione in atti giudiziari (art. 319-ter c.p.) [modificato dalla L. n. 69/2015]
- Induzione indebita a dare o promettere utilità (art. 319-quater) [articolo aggiunto dalla L. n. 190/2012] [modificato dalla L. n. 69/2015]
- Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)
- Pene per il corruttore (art. 321 c.p.)
- Istigazione alla corruzione (art. 322 c.p.)
- Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi degli delle Comunità europee e di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.) [articolo modificato dalla L. n. 190/2012 e dalla L. n. 3/2019]
- Traffico di influenze illecite (art. 346-bis c.p.)
- Peculato (limitatamente al primo comma) (art. 314 c.p.) (introdotto dal D. Lgs. n. 75/2020)
- Peculato mediante profitto dell'errore altrui (art. 316 c.p.) (introdotto dal D.Lgs. n. 75/2020)
- Abuso d'ufficio (art. 323 c.p.) (introdotto dal D.Lgs. n. 75/2020)

5. 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]

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.)
- Alterazione di monete (art. 454 c.p.)
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.)
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.)
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.)
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.)
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.)
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.)

- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)

- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

6. Delitti contro l'industria e il commercio (Art. 25-bis.1, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

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

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

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

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

- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)

- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)

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

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

7. Reati societari Art. 25-ter, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 61/2002, modificato dalla L. n. 190/2012, dalla L. n. 69/2015, dal D.Lgs. n. 38/2017 e dal D. Lgs. 19/2023]

- False comunicazioni sociali (art. 2621 c.c.) [modificato dalla L. n. 69/2015]

- Fatti di lieve entità (art. 2621-bis c.c.) [aggiunto dalla L. n. 69/ 2015]

- False comunicazioni sociali delle società quotate (art. 2622 c.c.) [modificato dalla L. n. 69/2015]

- Impedito controllo (art. 2625, comma 2, c.c.)

- Indebita restituzione di conferimenti (art. 2626 c.c.)

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

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

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

- Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.) [aggiunto dalla L. n. 262/2005]

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

- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)
- Corruzione tra privati (art. 2635 c.c.) [aggiunto dalla L. n. 190/2012; modificato dal D.lgs. 38/2017 e dalla L. n. 3/2019]
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.) [aggiunto dal D.Lgs. 38/2017 e modificato dalla L. n. 3/2019]
- Illecita influenza sull'assemblea (art. 2636 c.c.)
- Aggiotaggio (art. 2637 c.c.)
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.)
- False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D.Lgs. 19/2023) [articolo aggiunto dal D.Lgs. 19/2023]

8. 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]

- Associazioni sovversive (art. 270 c.p.)
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270-bis c.p.)
- Circostanze aggravanti e attenuanti (art. 270-bis1 c.p.)
- Assistenza agli associati (art. 270-ter c.p.)
- Arruolamento con finalità di terrorismo anche internazionale (art. 270-quater c.p.)
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-quinquies c.p.)
- Finanziamento di condotte con finalità di terrorismo (art. 270 quinquies.1)
- Sottrazione di beni o denaro sottoposti a sequestro (art. 270 quinquies.2)
- Condotte con finalità di terrorismo (art. 270-sexies c.p.)
- Attentato per finalità terroristiche o di eversione (art. 280 c.p.)
- Atto di terrorismo con ordigni micidiali o esplosivi (art. 280-bis c.p.)
- Atti di terrorismo nucleare (art. 280 ter)
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289-bis c.p.)
- Sequestro a scopo di coazione (art. 289-ter c.p.)

- Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo (art. 302 c.p.)
- Cospirazione politica mediante accordo (art. 304 c.p.)
- Cospirazione politica mediante associazione (art. 305 c.p.)
- Banda armata: formazione e partecipazione (art. 306 c.p.)
- Assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.)
- Impossessamento, dirottamento e distruzione di un aereo (art. 1, L. n. 342/1976)
- Danneggiamento delle installazioni a terra (art. 2, L. n. 342/1976)
- Sanzioni (art. 3, L. n. 422/1989)
- Pentimento operoso (art. 5, D.Lgs. n. 625/1979)
- Convenzione di New York del 9 dicembre 1999 (art. 2)

9. 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]

- Pratiche di mutilazione degli organi genitali femminili (art. 583-bis)

10. Delitti contro la personalità individuale (Art. 25-quinquies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 228/2003] [articolo modificato dalla L. n. 199/2016]

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)
- Prostituzione minorile (art. 600-bis c.p.)
- Pornografia minorile (art. 600-ter c.p.)
- Detenzione o accesso a materiale pornografico (art. 600-quater)[articolo modificato dalla Legge n. 238/2021]
- Pornografia virtuale (art. 600-quater.1 c.p.) [aggiunto dall'art. 10, L. 6 febbraio 2006, n. 38]
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.)
- Tratta di persone (art. 601 c.p.)
- Acquisto e alienazione di schiavi (art. 602 c.p.)
- Intermediazione illecita e sfruttamento del lavoro (art. 603-bis)
- Adescamento di minorenni (art. 609-undecies) [articolo modificato dalla Legge n. 238/2021]

11. Reati di abuso di mercato (Art. 25-sexies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 62/2005]

- Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione ai altri alla commissione di abuso di informazioni privilegiate (art. 184, D.Lgs. n. 58/1998)
- Manipolazione del mercato (art. 185, D.Lgs. n. 58/1998)

12. Altre fattispecie in materia di abuso di mercato (art. 187-quinquies TUF)[articolo modificato dal D.Lgs. 107/2018]

- Divieto di manipolazione del mercato (art. 15 Reg. UE n. 596/2014)
- Divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate (art.14 Reg. UE n. 596/2014)

13. 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, mod. dalla L. 3/2018]

- Omicidio colposo (art. 589 c.p.)
- Lesioni personali colpose (art. 590 c.p.)

14. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonchè autoriciclaggio (Art. 25-octies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 231/2007, modificato dalla L. n. 186/2014 e dal D. Lgs. 195/2021]

- Ricettazione (art. 648 c.p.)
- Riciclaggio (art. 648-bis c.p.)
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)
- Autoriciclaggio (art. 648-ter.1 c.p.)

15. Delitti in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies1, D. Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs 184/2021 e modificato dalla L. n. 137/2023]

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.)
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.)
- Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.)
- Trasferimento fraudolento di valore (art. 512-bis) (aggiunto dalla L. n. 137/2023)

Altre fattispecie in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies 1 comma 2, D. Lgs. 231/2001)

- Altre fattispecie

16. Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009 e modificato dalla L. n. 93/2023]

- 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, comma 1, lett. a-bis), L. n. 633/1941)

- 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, comma 3, L. n. 633/1941)

- 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, comma 1, L. n. 633/1941)

- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis, comma 2, L. n. 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-ter, L. n. 633/1941, modificazione dalla L. n. 93/2023)

- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies, L. n. 633/1941)

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

17. 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]

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità

giudiziaria (art. 377-bis c.p.)

18. Reati ambientali (Art. 25-undecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 121/2011] [modificato dalla L. n. 68/2015, dal D.Lgs. 21/2018 e dalla L. n. 137/2023]

- Inquinamento ambientale (art. 452-bis c.p.) [introdotto dalla L. n. 68/2015, modificato dalla L. n. 137/2023]
- Disastro ambientale (art. 452-quater c.p.) [introdotto dalla L. n. 68/2015, modificato dalla L. n. 137/2023]
- Delitti colposi contro l'ambiente (art. 452-quinquies c.p.) [introdotto dalla L. n. 68/2015]
- Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.) [introdotto dalla L. n. 68/ 2015]
- Circostanze aggravanti (art. 452-octies c.p.) [introdotto dalla L. n. 68/2015]
- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.)
- Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p.)
- Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (artt. 1 e 2, L. n. 150/1992)
- Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (art. 137, D.Lgs. n.152/2006)
- Attività di gestione di rifiuti non autorizzata (art. 256, D.Lgs n.152/2006)
- Traffico illecito di rifiuti (art. 259, D.Lgs. n.152/2006)
- Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.)
- Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (art. 257, D.Lgs. n. 152/2006)
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258, D.Lgs. n.152/2006)
- False indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti (art. 260-bis, D.Lgs. n.152/2006)
- Inquinamento doloso provocato da navi (art. 8, D.Lgs. n. 202/2007)

- Inquinamento colposo provocato da navi (art. 9, D.Lgs. n. 202/2007)

- Cessazione e riduzione dell´impiego delle sostanze lesive (L. n. 549/1993 art. 3)

19. 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, modificato dalla L. 161/2017]

- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12-bis, D.Lgs. n. 286/1998)

- Disposizioni contro le immigrazioni clandestine (art. 12, comma 3, 3 bis, 3 ter e comma 5, D.lgs. n.286/1998)

20. Razzismo e xenofobia (Art. 25-terdecies, D.lgs. n. 231/2001) [articolo aggiunto dalla L. 20 novembre 2017 n. 167, modificato dal D. Lgs. n. 21/2018]

- Propaganda e istigazione a delinque per motivi di discriminazione razziale, etnica e religiosa (art. 604-bis c.p.)

21. Reati transnazionali (L. n. 146/2006) [Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale]

- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5, del Testo Unico di cui al D.Lgs. 25 luglio 1998, n. 286)

- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del Testo Unico di cui al D.P.R. 9 ottobre 1990, n. 309)

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

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

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

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

- Associazione di tipo mafioso (art. 416-bis c.p.) [modificato dalla L. n. 69/2015]

22. Frode in competizione sportiva (Art.25-quaterdecies, D.Lgs 231/2001) [introdotto con la legge 3 maggio 2019, n. 39 con la quale è stata data attuazione alla Convenzione del Consiglio d'Europa sulla manipolazione di competizioni sportive, Magglingen 18 settembre 2014].

Legge 13 dicembre 1989, n. 401:

- art 1) incrimina "chiunque offre o promette denaro o altre utilità o vantaggio a taluno dei partecipanti ad una competizione sportiva organizzata dalle federazioni riconosciute, al fine di raggiungere un risultato diverso da quello conseguente al corretto e leale svolgimento

della competizione, ovvero compie altri atti fraudolenti volti al medesimo scopo" nonché "il partecipante alla competizione che accetta il denaro o altre utilità o vantaggio, o ne accoglie la promessa";

- art. 4) contempla, invece, diverse fattispecie connesse all'esercizio, organizzazione, vendita di attività di giochi e scommesse in violazione di autorizzazioni o concessioni amministrative.

23. Reati tributari (Art.25-quinquiesdecies, D.Lgs 231/2001) [introdotta con la L. 19 dicembre 2019, n. 157, di conversione del D.L. 26 ottobre 2019, n. 124 (c.d. decreto fiscale) e aggiornato dal d.Lgs. n. 75/2020]

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D. Lgs. n. 74/2000)
- Dichiarazione fraudolenta mediante altri artifici (art. 3 del D. Lgs n. 74/2000)
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 del D. Lgs. n. 74/2000)
- Occultamento o distruzione di documenti contabili (art. 10 del D. Lgs. n. 74/2000)
- Sottrazione fraudolenta al pagamento di imposte (art. 11 del D. Lgs. 74/2000)
- Dichiarazione infedele (art. 4 D.Lgs. n. 74/2020) (introdotto dal D.Lgs. n. 75/2020)
- Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000) (introdotto dal D.Lgs. n. 75/2020)
- Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000) (introdotto dal D.Lgs. n. 75/2020)

24. Contrabbando (Art.25-sexiesdecies, D.Lgs 231/2001) [articolo introdotto dal D.Lgs. n. 75/2020]

- Contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali (art. 282 DPR n. 43/1973)
- Contrabbando nel movimento delle merci nei laghi di confine (art. 283 DPR n. 43/1973)
- Contrabbando nel movimento marittimo delle merci (art. 284 DPR n. 43/1973)
- Contrabbando nel movimento delle merci per via aerea (art. 285 DPR n. 43/1973)
- Contrabbando nelle zone extra-doganali (art. 286 DPR n. 43/1973)
- Contrabbando per indebito uso di merci importate con agevolazioni doganali (art. 287 DPR n. 43/1973)
- Contrabbando nei depositi doganali (art. 288 DPR n. 43/1973)
- Contrabbando nel cabotaggio e nella circolazione (art. 289 DPR n. 43/1973)
- Contrabbando nell'esportazione di merci ammesse a restrizioni di diritto (art. 290 DPR n. 43/1973)
- Contrabbando nell'importazione od esportazione temporanea (art. 291 DPR n. 43/1973)
- Contrabbando di tabacchi lavorati esteri (art. 291-bis DPR n. 43/1973)
- Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati esteri (art. 291-ter DPR n. 43/1973)

- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater DPR n. 43/1973)
- Altri casi di contrabbando (art. 292 DPR n. 43/1973)
- Circostanze aggravanti del contrabbando (art. 295 DPR n. 43/1973)

25. Delitti contro il patrimonio culturale (Art. 25-septiesdecies, D. Lgs. 231/2001) [articolo aggiunto dalla L n. 22/2022 modificato dalla L. 6/2024]

- Furto di beni culturali (art. 518-bis c.p.)
- Appropriazione indebita di beni culturali (art. 518-ter c.p.)
- Ricettazione di beni culturali (art. 518-quater c.p.)
- Falsificazione in scrittura privata relativa a beni culturali (art. 518-octies c.p.)
- Violazioni in materia di alienazione di beni culturali (art. 518-novies c.p.)
- Importazione illecita di beni culturali (art. 518- decies c.p.)
- Uscita o esportazione illecita di beni culturali (art. 518-undecies c.p.)
- Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici(art. 518-duodecies c.p.)
- Contraffazione di opere d'arte (art. 518-quaterdecies c.p.)

26. Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (Art. 25-duodevicies, D. Lgs. 231/2001) [articolo aggiunto dalla L n. 22/2022]

- Riciclaggio di beni culturali (art. 518-sexies c.p.)
- Devastazione e saccheggiamento di beni culturali e paesaggistici (art. 518-terdecies)