

**Fratelli Branca Distillerie S.p.A.**

**Modello di organizzazione, gestione e controllo**

**(d. lgs. 231/2001)**

**Parte Speciale**

## Sommario

<b>Parte Speciale A</b> .....	<b>5</b>
<b>Reati contro la Pubblica Amministrazione (Artt. 24 e 25 del d. lgs. 231/2001)</b> .....	<b>5</b>
1. Attività sensibili.....	5
<b>Parte speciale B</b> .....	<b>7</b>
<b>Criminalità informatica (art. 24 bis del d. lgs. 231/2001)</b> .....	<b>7</b>
1. Attività sensibili.....	7
2. Presupposti normativi.....	8
<b>Parte speciale C</b> .....	<b>9</b>
<b>Criminalità organizzata, anche transnazionale (art. 24 ter del d. lgs. 231/2001 - L. 146/2006)</b> ....	<b>9</b>
1. Attività sensibili.....	9
2. Principi generali.....	9
<b>Parte speciale D</b> .....	<b>12</b>
<b>Falsità nummarie (art. 25 bis del d. lgs. 231/2001)</b> .....	<b>12</b>
<b>1. Attività sensibili</b> .....	<b>12</b>
<b>Parte Speciale E</b> .....	<b>13</b>
<b>Reati contro commercio e industria (art. 25 bis.1 del d. lgs. 231/2001)</b> .....	<b>13</b>
1. Attività sensibili.....	13
2. Principi di riferimento e presupposti organizzativi .....	14
<b>Parte Speciale F</b> .....	<b>16</b>
<b>Reati societari (art. 25 ter del d. lgs. 231/2001)</b> .....	<b>16</b>
1. Attività sensibili.....	16
<b>Parte Speciale G</b> .....	<b>18</b>
<b>Delitti di terrorismo e di eversione dell' ordine democratico (art. 25 quater del d. lgs. 231/2001)</b> .....	<b>18</b>
1. Attività sensibili.....	18
<b>Parte Speciale H</b> .....	<b>19</b>
<b>Delitti contro la persona (art. 25 quater.1 e quinquies del d. lgs. 231/2001)</b> .....	<b>19</b>

1. Attività sensibili.....	19
<b>Parte Speciale I.....</b>	<b>20</b>
<b>Abusi di mercato (art. 25 sexies del d. lgs. 231/2001).....</b>	<b>20</b>
<b>Parte Speciale L.....</b>	<b>21</b>
<b>Sicurezza sul lavoro (art. 25 septies del d. lgs. 231/2001) .....</b>	<b>21</b>
1. Attività sensibili.....	21
2. Presupposti normativi e adempimenti correlati .....	21
<b>Parte Speciale M.....</b>	<b>25</b>
<b>Ricettazione, riciclaggio e autoriciclaggio (art. 25 octies del d. lgs. 231/2001) .....</b>	<b>25</b>
1. Attività sensibili.....	25
<b>Parte Speciale N .....</b>	<b>26</b>
<b>Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori .....</b>	<b>26</b>
1. Attività sensibili.....	26
<b>Parte Speciale O .....</b>	<b>27</b>
<b>Delitti contro il diritto d’ autore (art. 25 novies del d. lgs. 231/2001).....</b>	<b>27</b>
1. Attività sensibili.....	27
<b>Parte Speciale P .....</b>	<b>28</b>
<b>Delitti contro l’ Autorità Giudiziaria (art. 25 decies del d. lgs. 231/2001) .....</b>	<b>28</b>
1. Attività sensibili.....	28
2. Principi di comportamento .....	28
<b>Parte Speciale Q .....</b>	<b>29</b>
<b>Reati ambientali (art. 25 undecies del d. lgs. 231/2001).....</b>	<b>29</b>
1. Attività sensibili.....	29
2. Presupposti normativi e adempimenti correlati .....	29
<b>Parte Speciale R .....</b>	<b>31</b>
<b>Reati di clandestinità e xenofobia (art. 25 duodecies e art. 25 terdecies del d. lgs. 231/2001) ..</b>	<b>31</b>
1. Attività sensibili.....	31

<b>Parte Speciale S .....</b>	<b>32</b>
<b>Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25 quaterdecies d. lgs. 231/2001) .....</b>	<b>32</b>
1. Attività sensibili.....	32
<b>Parte Speciale T.....</b>	<b>33</b>
<b>Reati tributari (art. 25 quinquiesdecies del d. lgs. 231/2001).....</b>	<b>33</b>
1. Attività sensibili.....	33
<b>Parte Speciale U .....</b>	<b>35</b>
<b>Contrabbando (art. 25 sexiesdecies del d. lgs. 231/2001).....</b>	<b>35</b>
1. Attività sensibili.....	35
<b>Parte Speciale V .....</b>	<b>36</b>
<b>Delitti contro il patrimonio culturale e riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25 septiesdecies e 25 duodecimes del d. lgs. 231/2001) ....</b>	<b>36</b>
1. Attività sensibili.....	36

## Parte Speciale A

### Reati contro la Pubblica Amministrazione (Artt. 24 e 25 del d. lgs. 231/2001)

#### 1. Attività sensibili

Si precisa che la Società non partecipa a gare di fornitura per la Pubblica Amministrazione. I reati contro la Pubblica Amministrazione rappresentano un rischio in relazione alle attività di seguito indicate:

- ◆ predisposizione di dichiarazioni, istanze o richieste alla Pubblica Amministrazione, anche per via telematica: si tratta di tutte le dichiarazioni o richieste avanzate innanzi alla Pubblica Amministrazione nelle quali si attestino dati ovvero volte a dichiarare la sussistenza in capo alla Società di specifici requisiti per il rilascio di un atto o provvedimento amministrativo di interesse aziendale. Il rischio maggiore è quello inerente alla veridicità delle documentazioni di supporto o delle dichiarazioni attestanti l'esistenza di condizioni o requisiti essenziali in effetti non presenti. Si evidenzia la stretta attinenza con le aree sensibili nei termini indicati:

- presentazione di istanze alla Pubblica Amministrazione, anche in via telematica. Nel caso di specie, si aggiunge anche il rischio correlato all'utilizzo di un sistema informatico o telematico, ove può esercitarsi un'azione manipolatoria sui dati;
- ottenimento o rinnovo di concessioni, licenze, abilitazioni e autorizzazioni da parte della Pubblica Amministrazione: si tratta di tutte le richieste o rinnovi di qualsivoglia autorizzazione, licenza, abilitazione all'esercizio di specifiche attività societarie, in qualsiasi ambito richieste, con riguardo a tutte le ipotesi di rilascio di provvedimenti che prevedano di doversi interfacciare con la Pubblica Amministrazione. Il rischio principale si correla alla falsa attestazione dei requisiti;
- gestione fiscale e previdenziale, anche con riferimento alle ipotesi di modifica in via telematica dei dati fiscali o previdenziali di interesse della Società già in possesso della Pubblica Amministrazione;
- presentazione di istanze per finanziamenti, contributi o altre erogazioni pubbliche e relativa gestione, con particolare riferimento al rischio di attestazioni false, anche attraverso produzioni documentali non veritiere o complete, e non corretta destinazione delle erogazioni pubbliche per le finalità per le quali sono state ottenute;
- rapporti con uffici pubblici per i depositi di brevetti e marchi: ci si riferisce, in particolare, alla gestione delle richieste di nuovi marchi e agli adempimenti correlati ove il rapporto con la Pubblica Amministrazione evidenzia il possibile rischio;

- ◆ attività ispettive di enti pubblici e Autorità (ad es. ATO, Arpa, Provincia, Regione, ASL, Autorità giudiziaria, ...): si tratta di tutte le ipotesi in cui enti pubblici a qualsiasi titolo svolgano accessi a fini ispettivi presso la Società. In genere si richiamano i rapporti con autorità fiscali, doganali, sanitarie, ambientali, previdenziali nonché autorità regolamentari;
- ◆ gestione legale: si fa riferimento a tutte le ipotesi in cui la Società si trovi a gestire contenziosi penali, civili, giuslavoristici, amministrativi, tributari e fiscali, ove si presenti il rischio di influenzare illecitamente, con denaro o altre utilità, anche tramite terzi, le decisioni giudiziali o le attività transattive.

Attività sensibili da considerarsi, in via prevalente, strumentali a quelle elencate poiché rappresentano un mezzo per la commissione dei c.d. reati presupposto richiamati, sono:

- ◆ selezione, assunzione e gestione del personale (anche appartenente a categorie protette): si fa riferimento alle ipotesi in cui le utilità conferite e conferibili per la commissione dei reati presupposto siano fornite mediante l'assunzione del personale e la sua gestione, con riguardo a possibili interferenze con la Pubblica Amministrazione o Autorità ispettive in via assuntiva (possibili conflitti di interesse) e in merito agli avanzamenti di carriera e alla gestione premiale nonché all'assunzione e gestione di categorie protette;
- ◆ selezione dei fornitori e gestione dei relativi rapporti: la selezione dei fornitori può rappresentare uno strumento volto a determinare una forma di influenza anche indiretta nei rapporti con la Pubblica Amministrazione;
- ◆ selezione dei consulenti e gestione dei relativi rapporti: la selezione dei consulenti può rappresentare uno strumento volto a determinare una forma di influenza anche indiretta nei confronti della Pubblica Amministrazione;
- ◆ sponsorizzazioni: tale attività può determinare una forma di influenza ed essere veicolo di indebite forme di pagamento nei rapporti con la Pubblica Amministrazione;
- ◆ gestione dei flussi finanziari: la circolazione di flussi in uscita, in particolare, può rappresentare veicolo di pratiche corruttive o di condotte concussorie in senso lato, attraverso, ad esempio, false fatturazioni;
- ◆ gestione dei rapporti infragruppo, se atti a determinare rischi di creazione di risorse finanziarie da destinare a finalità corruttive o concussorie;
- ◆ gestione note spese e spese di rappresentanza: tali spese possono nascondere illecite erogazioni nei confronti di soggetti legati, direttamente o indirettamente, alla Pubblica Amministrazione;
- ◆ gestione delle donazioni e regalie: l'attività rappresenta rischi correlati alla possibile identificazione di forme di corruzione o concussione celate da donazioni da parte della Società.

## Parte speciale B

### Criminalità informatica (art. 24 bis del d. lgs. 231/2001)

#### 1. Attività sensibili

Il rischio di attività di criminalità informatica è riconducibile alle seguenti attività sensibili:

- ◆ utilizzo dei propri sistemi informatici da parte degli utenti: si fa riferimento a possibili vantaggi della Società derivanti da forme di hackeraggio o accesso abusivo o danneggiamento di sistemi informatici di terzi. Si precisa che le possibili condotte delineate presuppongono necessariamente un livello di competenze informatiche non comune, che rende l'ascrivibilità delle stesse difficile per l'utente medio. A titolo cautelativo, si riconoscono i rischi di:
  - falsificazioni di documenti informatici, anche contenenti gli importi dovuti dall'ente alla P.A. nel caso di flussi informatizzati dei pagamenti, o correlata all'utilizzo illecito di dati identificativi altrui nell'esecuzione di determinate operazioni informatiche o telematiche in modo che risultino svolte da legittimi titolari dei dati;
  - cancellazione o alterazione di informazioni a valenza probatoria presenti sui propri sistemi;
  - danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso enti pubblici;
  - rilascio di certificati digitali da parte di un ente certificatore, senza che siano soddisfatti gli obblighi di legge;
- ◆ utilizzo dei sistemi informatici da parte dell'Amministratore di Sistema e di utilizzatori di *pc administrator* oppure utenti con accessi/permessi privilegiati: si fa riferimento a possibili vantaggi della Società derivanti da forme di hackeraggio o accesso abusivo o danneggiamento di sistemi informatici di terzi. Si evidenziano anche gli utenti con accessi/permessi privilegiati, determinati dalla disponibilità di credenziali per accesso a portali della P.A. Si rimanda alle seguenti casistiche:
  - falsificazioni di documenti informatici, anche contenenti gli importi dovuti dall'ente alla PA nel caso di flussi informatizzati dei pagamenti, o correlata all'utilizzo illecito di dati identificativi altrui nell'esecuzione di determinate operazioni informatiche o telematiche in modo che risultino svolte da legittimi titolari dei dati;
  - cancellazione o alterazione di informazioni a valenza probatoria presenti sui propri sistemi;
  - danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso enti pubblici;
  - rilascio di certificati digitali da parte di un ente certificatore, senza che siano soddisfatti gli

obblighi di legge.

## **2. Presupposti normativi**

Si ravvisa, in ordine alle aree di rischio individuate, l'obbligatorietà per la Società di rispettare il Regolamento europeo in materia di protezione dei dati personali n. 2016/679 (c.d. G.D.P.R.), punto di partenza indefettibile per prevenire la possibile commissione dei reati indicati. Il G.D.P.R. richiede l'introduzione e l'attuazione di *misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio* (art. 32 G.D.P.R.). Le misure tecniche rimandano a strumenti ed elaboratori o macchine che siano programmati in maniera corretta per gestirne la funzionalità in sicurezza; le misure organizzative introducono *standards* e protocolli operativi di comportamenti dei destinatari. Fondamentale, in tal senso, è l'introduzione di un regolamento informatico, che garantisca il confine tra ciò che l'utente può fare oppure non è autorizzato a fare. Le misure definite devono tenere conto delle aree di rischio tipiche della Società, sia sotto il profilo delle minacce e degli abusi provenienti dall'interno che delle insidie provenienti dall'esterno. In tal senso la Società è tenuta ad attuare *best practices* in materia di *Cyber Security*, volte a garantire riservatezza, integrità e disponibilità delle informazioni oltre che continuità e affidabilità dei servizi erogati. Le misure definite devono assicurare un adeguato livello di sicurezza dell'infrastruttura informatica di cui si avvale la Società, bilanciando da un lato lo stato dell'arte e i costi di attuazione, dall'altro i rischi di varia probabilità e gravità correlati alla stessa. Inoltre, la Società ha intrapreso un percorso di adeguamento alla NIS 2 (Directive (EU) 2022/2555), normativa che presuppone un rafforzamento delle misure di gestione dei rischi in materia di cybersecurity.

Necessaria è l'attivazione di corsi di formazione in materia di sicurezza informatica, congiuntamente a un monitoraggio sul rispetto delle misure previste da parte dei dipendenti e l'applicazione.

Le prescrizioni, sebbene rivolte alla protezione dei dati personali, rappresentano un presidio importante anche per evitare di incorrere nei reati previsti dal d. lgs. 231/2001.

Il mancato rispetto delle previsioni indicate rappresenta di per sé una violazione delle prescrizioni contenute nel presente Modello ed espone, pertanto, a sanzioni disciplinari.

## Parte speciale C

**Criminalità organizzata, anche transnazionale (art. 24 ter del d. lgs. 231/2001 – L. 146/2006)**

### 1. Attività sensibili

L'esposizione al rischio di reati di criminalità organizzata è di bassa entità per la Società. Tuttavia, possono essere annoverate le seguenti aree sensibili:

- ◆ selezione, assunzione e gestione del personale: nel caso di specie, ci si riferisce ai casi in cui l'assunzione del personale, ovvero le progressioni di carriera e gli incentivi premiali siano volti ad agevolare o partecipare a fenomeni di criminalità organizzata;
- ◆ selezione dei fornitori e gestione dei relativi rapporti: ci si riferisce al rischio di identificare fornitori per agevolare o partecipare direttamente a fenomeni di criminalità organizzata. In quest'area si identifica anche il dovere di monitoraggio di rapporti con soggetti coinvolti in procedimenti giudiziari;
- ◆ selezione dei consulenti e gestione dei relativi rapporti: ci si riferisce al rischio di identificare consulenti per agevolare o partecipare direttamente a fenomeni di criminalità organizzata;
- ◆ gestione dei rapporti con clienti, anche esteri: ci si riferisce a ipotesi di agevolazione o partecipazione diretta a fenomeni di criminalità organizzata;
- ◆ rapporti con agenti e distributori: ci si riferisce a ipotesi di agevolazione o partecipazione diretta a fenomeni di criminalità organizzata;
- ◆ rapporti infragruppo, per il possibile ruolo tra le società del Gruppo nell'agevolare condotte di cui alla presente parte;
- ◆ gestione dei flussi finanziari, per verificarne la lecita destinazione;
- ◆ gestione fiscale, considerata come area di rischio precauzionalmente dal momento che vi sono interpretazioni estensive, in giurisprudenza e dottrina, che tendono a riconoscere i reati associativi quale mezzo per il raggiungimento del reato. Si ritiene, comunque, presidiata tale area dalla presenza dei reati tributari;
- ◆ donazioni: ci si riferisce a erogazioni liberali che possano determinare forme di finanziamento di attività illecite.

### 2. Principi generali

Si richiama, quale utile ausilio per la prevenzione dei rischi di cui alla presente Parte speciale, il Codice antimafia per le imprese (Vigna, Fiandaca, Masciandaro), specificando, tuttavia, che la Società non riveste una posizione significativa di rischio in materia. La prevenzione ha il duplice obiettivo di:

- proteggere e incrementare l'integrità aziendale;

- contribuire alla tutela dell'ordine pubblico economico e alla difesa della legalità.

Fondamentale diviene l'analisi del territorio e del contesto in cui la Società opera, per verificarne i possibili rischi connessi alla presente area. In tal senso, per tale valutazione preventiva delle controparti contrattuali, si richiamano i seguenti aspetti:

- provvedimenti o documenti giudiziari o di polizia, ove disponibili;
- relazioni periodiche, ove accessibili, di istituzioni pubbliche competenti;
- rilevazioni degli ispettorati del lavoro;
- statistiche ISTAT;
- studi sociologici e criminologici disponibili o richiesti ad esperti qualificati;
- rilevazioni ed elaborazioni delle camere di commercio, delle associazioni imprenditoriali e sindacali, delle associazioni antiracket nonché di ogni altro soggetto pubblico e privato svolgente funzioni similari nell'ambito dei diversi contesti territoriali;
- inchieste e cronache giornalistiche.

Precisando sin da ora che la Società non svolge attività riconducibili a particolari situazioni di rischio della presente Parte Speciale, si suggerisce quale utile strumento non vincolante, l'analisi di indicatori di rischio rispetto alle controparti contrattuali, quali:

- sottoposizione a procedimento per l'applicazione di misure di prevenzione, ai sensi della normativa antimafia;
- applicazione di misure cautelari coercitive nell'ambito di procedimenti penali o pronunce di sentenza di condanna, ancorché non definitiva, compresa quella prevista dall'art. 444 c.p.p. – patteggiamento – nei confronti di imprenditori, soci, amministratori o dipendenti delle imprese per i reati che incidono sull'affidabilità professionale (delitti contro la P.A., reati associativi, delitti di usura, estorsione, ricettazione, riciclaggio, impiego di beni provenienti da delitti e altre ipotesi connesse alla criminalità organizzata);
- applicazione di misure cautelari nell'ambito di un procedimento penale e pronuncia di sentenza di condanna, ancorché non definitiva, compresa quella emessa su richiesta delle parti, nei confronti di enti, ai sensi del d. lgs. 231/2001, per reati contro la Pubblica Amministrazione, reati contro la persona, reati di riciclaggio e di associazione a delinquere di natura transnazionale, e per altre figure di reato che assumono rilievo nell'ambito della criminalità organizzata;
- costituzione di enti nei quali figurano, come soci, amministratori o gestori, persone (o prossimi congiunti) che partecipano o abbiano partecipato alle imprese

od enti nelle situazioni indicate nei punti precedenti ovvero manifestamente sprovvisti, per età o formazione, dei requisiti indispensabili per l'esercizio dell'attività imprenditoriale;

- imprese che siano da ritenere, sulla base di elementi di fatto, costituite soltanto allo scopo di occultare o favorire soggetti appartenenti a gruppi criminali o, comunque, di eludere divieti nello svolgimento di attività imprenditoriali;
- imprese od enti che risultino privi di rapporti con aziende di credito;
- intervento, nelle trattative commerciali, di persone od enti privi di legittimazione ad interloquire nelle trattative medesime; mancata consegna, qualora richiesta, del certificato penale generale, del certificato dei carichi pendenti, del certificato antimafia, o di autocertificazione sostitutiva;
- mancata esibizione di documenti comprovanti l'iscrizione ad albi, ordini, elenchi, qualora l'iscrizione sia requisito necessario per lo svolgimento dell'attività. Coloro che rivestano ruoli decisionali devono disporre di apposita delega o procura per agire in nome e per conto della Società.

## Parte speciale D

**Falsità nummarie (art. 25 bis del d. lgs. 231/2001)**

### **1. Attività sensibili**

La presente sezione è richiamata in quanto si pongono limitati profili di gestione di contante anche in valuta estera. Per quanto attiene, invece, l'utilizzo di contrassegni legati alla gestione delle accise, tale attività risulta esternalizzata. L'aspetto che può avere, tuttavia, maggior significatività, sebbene si ritenga dal rischio trascurabile, è riconducibile all'uso di marchi o segni distintivi.

Si rimanda in linea generale a:

- ◆ gestione dei pagamenti in contanti, correlati al rischio di messa in circolazione di moneta falsificata da terzi, ricevuta in buona fede;
- ◆ uso di valori di bollo;
- ◆ selezione e gestione dei rapporti con fornitori (anche per materie prime e packaging) e controparti contrattuali, in relazione alle attività di approvvigionamento, in considerazione del rischio di utilizzo o introduzione nel territorio dello Stato prodotti industriali con marchi o segni distintivi, nazionali ed esteri, contraffatti al fine di trarne profitto;
- ◆ acquisizione, rivendica, registrazione di marchi, brevetti, disegni, modelli o altri titoli o diritti di proprietà, correlati al rischio remoto di contraffazione, alterazione, utilizzo di marchi o segni distintivi ovvero di introduzione e messa in commercio di prodotti con segni falsi, anche al di fuori di un ruolo nella contraffazione.

## Parte Speciale E

### Reati contro commercio e industria (art. 25 bis.1 del d. lgs. 231/2001)

#### 1. Attività sensibili

Data l'attività tipica di impresa svolta dalla Società, il rischio di commissione di reati contro il commercio e l'industria è da ritenersi rilevante. Si precisa che la Società, in materia di sicurezza alimentare, dispone di Manuale Qualità e Sicurezza Alimentare secondo norma UNI EN ISO 22000, oggetto di certificazione annuale.

Si menzionano le seguenti attività sensibili:

- ◆ realizzazione e sviluppo di nuovi prodotti.

Si evidenziano i seguenti rischi, anche in parte riproposti di seguito con riguardo a specifiche attività sensibili autonome:

- frode nell'esercizio del commercio: si fa riferimento ad una molteplicità di condotte fraudolente commesse nell'esercizio dell'attività aziendale. I processi aziendali interessati sono i seguenti:
  1. distribuzione e vendita;
  2. approvvigionamento materie prime;
  3. controllo qualità sicurezza e igiene del processo;
  4. selezione e controllo dei fornitori;
  5. marketing e pubblicità;
  6. etichettatura;
  7. gestione resi/sottoprodotti/scarti di lavorazione;
  8. gestione procedure ritiro/ricambio;
  9. distribuzione e vendita.
  
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti: il rischio attiene alla possibile alterazione delle indicazioni ovvero delle denominazioni del prodotto.  
Sono di seguito indicate le aree maggiormente esposte al rischio:
  1. etichettatura;
  2. marketing e pubblicità;
  3. controlli metrologici;
  4. gestione analisi in autocontrollo;
  5. gestione procedure di rintracciabilità;

6. approvvigionamento materie prime.

- Vendita di sostanze alimentari non genuine come genuine: l'ambito di rischio riguarda la possibilità di vendere ed esportare prodotti adulterati, contraffatti o che non rispettano i requisiti imposti per legge ma necessari per la loro qualificazione. I processi e le attività che possono essere coinvolti nella commissione di tale reato riguardano:
  1. produzione diretta e terziarizzata;
  2. approvvigionamento materie prime;
  3. controllo qualità sicurezza e igiene del processo;
  4. controlli metrologici;
  5. distribuzione e vendita.
- ◆ selezione dei fornitori e gestione dei relativi rapporti: si fa riferimento alla necessità di identificare adeguati fornitori, per scongiurare il rischio di immissione di prodotti in violazione del titolo di proprietà o prodotti alterati o contraffatti;
- ◆ rapporti con clienti, agenti e distributori, interessati dall'immissione in commercio di prodotti;
- ◆ rapporti con consulenti, ai fini di un adeguato supporto nella gestione dei profili individuati;
- ◆ acquisizione, rivendica, registrazione di marchi, brevetti, disegni, modelli o altri titoli o diritti di proprietà, con onere di attenta verifica in merito al fine di evitare rischi di frode o messa in circolazione di prodotti in violazione del diritto d'autore.

## **2. Principi di riferimento e presupposti organizzativi**

Si stabilisce il rispetto e l'osservanza dei principi di riferimento di seguito indicati:

- tutela del diritto all'informazione da parte degli acquirenti, siano essi operatori commerciali o consumatori finali;
- impegno nell'assicurare che l'etichettatura, la presentazione, la pubblicità ed ogni altra forma di comunicazione commerciale rivolta al consumatore siano realizzate in maniera da assicurarne la corretta e la trasparente informazione;
- rifiuto nell'esercitare pratiche fraudolente o ingannevoli ed ogni altro tipo di pratica in grado di indurre in errore il consumatore;
- rispetto della normativa sulla sicurezza alimentare e garanzia di tutela della salute del consumatore.

Tali profili presuppongono una costante attenzione al rispetto dei contenuti previsti dalle norme ISO di riferimento nonché all'ottenimento e mantenimento dei requisiti previsti dalle certificazioni in essere presso la Società nell'ottica di prevenire i reati richiamati.

In particolare, si ritiene utile la presenza di:

- una politica aziendale che preveda la posizione dell'azienda in materia e gli impegni assunti;
- misure di divulgazione della citata politica aziendale;
- chiara definizione dei ruoli e delle procure o deleghe previste in materia di sicurezza alimentare e degli *standards* richiamati;
- procedure di selezione e valutazione dei fornitori;
- procedure di selezione, valutazione e controllo dei fornitori di attività terziarizzate;
- contratti e capitolati tecnici di acquisto;
- attività di autocontrollo interno anche mediante audit;
- applicazione degli *standards* richiamati e del Manuale HACCP;
- applicazione dei sistemi di rintracciabilità e gestione delle procedure di ritiro e richiamo dei prodotti;
- gestione delle non conformità;
- formazione del personale;
- gestione delle autorizzazioni;
- procedure per l'approvazione delle etichette e della comunicazione pubblicitaria, anche in caso di prodotti per conto di terzi;
- monitoraggio continuo sull'evoluzione della normativa nazionale e internazionale;
- procedura di gestione dei marchi e degli altri segni distintivi con previsione delle ricerche di anteriorità e verifica della confondibilità e ingannevolezza del marchio;
- procedure per lo svolgimento di controlli metrologici;
- definizioni delle attività di monitoraggio da parte dell'Organismo di Vigilanza;
- riesame periodico delle procedure e delle istruzioni operative;
- definizione della modalità di registrazione e archiviazione della documentazione relativa alle attività di gestione delle attività di sistema identificate con individuazione dei soggetti responsabili;
- verifiche periodiche di controllo dell'adeguatezza ed efficacia delle procedure e istruzioni adottate;
- riesame a seguito di cambiamenti organizzativi, violazioni di norme o altri mutamenti che redano necessaria una rivisitazione delle procedure e delle istruzioni del sistema di gestione;
- individuazione delle figure responsabili della predisposizione delle singole procedure e istruzioni;
- individuazione di sistemi di contrapposizione di funzione idonei ad evitare che i processi sensibili siano gestiti in autonomia da una singola figura.

## Parte Speciale F

### Reati societari (art. 25 ter del d. lgs. 231/2001)

#### 1. Attività sensibili

Il rischio di commissione di reati societari è connesso a qualsivoglia società di capitali in quanto tenuta agli adempimenti tipici. In particolare, la Società presenta le seguenti aree sensibili:

- ◆ predisposizione dei bilanci e delle scritture contabili, con specifico riferimento alla redazione del bilancio, delle relazioni o delle comunicazioni sociali previste dalla legge e, più in generale, di qualunque documento giuridicamente rilevante nel quale si evidenzino elementi economici, patrimoniali e finanziari della Società, ancorché relativi al gruppo al quale essa appartiene o alle sue partecipazioni;
- ◆ gestione dei possibili conflitti di interessi da parte degli amministratori, in presenza di possibili interessi propri o di familiari nelle operazioni societarie;
- ◆ gestione dei rapporti con il Collegio sindacale e con la Società di revisione: il rischio è correlato alla possibilità che gli amministratori tengano una condotta non corretta e trasparente, occultando o alterando la documentazione utile a rappresentare i processi applicativi in sede aziendale;
- ◆ gestione dei rapporti con i soci, con particolare riferimento al rischio di non condivisione di documentazione corretta e veritiera da parte del Consiglio di Amministrazione al fine di impedire adeguato controllo e decisioni consapevoli in sede di approvazione del bilancio, influenzando illecitamente l'assemblea;
- ◆ gestione dei rapporti infragruppo, per le ripercussioni sui bilanci delle singole società e del Gruppo;
- ◆ investimenti finanziari, per il rischio di utilizzo strumentale per la commissione dei reati di cui alla presente Parte Speciale;
- ◆ operazioni straordinarie (fusioni e scissioni), per il rischio di confusione delle masse passive dei soggetti coinvolti, rilevanti in particolare nei rapporti con i creditori. Si inserisce anche un rimando al rischio, in caso di operazioni straordinarie transfrontaliere, di false od omesse dichiarazioni per il rilascio del certificato preliminare previsto dalla normativa di riferimento;
- ◆ gestione dei flussi finanziari, che assumono particolare rilevanza in quanto alla base delle scritture contabili, della gestione fiscale nonché di eventuali rischi corruttivi nei confronti di privati;
- ◆ gestione note spese e spese di rappresentanza, nell'ottica della corretta gestione delle stesse nonché della prevenzione dal rischio di corruzione tra privati;
- ◆ selezione dei consulenti e gestione dei relativi rapporti: ci si riferisce alla necessità di affidarsi a

consulenti competenti per le attività correlate al bilancio e alle scritture contabili;

- ◆ rapporti con clienti, anche esteri: ci si riferisce al rischio di forme di corruzione tra privati;
- ◆ rapporti con agenti e distributori, con riguardo al rischio di corruzione tra privati;
- ◆ rapporti con enti ispettivi e Autorità di vigilanza, nell'ottica di garantire l'assenza di ostacolo alle attività di vigilanza.

## **Parte Speciale G**

### **Delitti di terrorismo e di eversione dell'ordine democratico (art. 25 quater del d. lgs. 231/2001)**

#### **1. Attività sensibili**

L'esposizione a reati di terrorismo e di eversione dell'ordine democratico, in ragione delle attività svolte all'interno della Società, presenta un rischio non rilevante, giacché non se ne evidenzia alcun possibile vantaggio o interesse per la medesima.

A titolo cautelativo, si riporta il rischio di finanziamento di terrorismo nei casi di violazioni informatiche tramite attacchi ransomware, ove il pagamento del riscatto, volto a consentire la prosecuzione dell'attività societaria con lo sblocco dei sistemi oggetto di attacco, può diventare una forma di sostegno economico alle attività illecite connesse al terrorismo. Si rimanda a misure di sicurezza informatica la gestione di tale profilo e monitoraggio dei flussi finanziari.

## **Parte Speciale H**

### **Delitti contro la persona (art. 25 quater.1 e quinquies del d. lgs. 231/2001)**

#### **1. Attività sensibili**

Il rischio di commissione di delitti contro la persona rilevanti ai sensi del d. lgs. 231/2001 è di scarsissima rilevanza e rappresenta una dichiarazione di principio piuttosto che un effettivo monito operativo, al fine di garantire la più totale estraneità della Società e di qualsivoglia interesse alle condotte richiamate.

Si tenga pertanto presente che, per il tipo di attività di impresa svolta, una possibile ma remota area di rischio potrebbe ravvisarsi nella seguente ipotesi:

- ◆ selezione e gestione del personale.

## **Parte Speciale I**

**Abusi di mercato (art. 25 sexies del d. lgs. 231/2001)**

Si esclude il rischio di commissione di abusi di mercato, data l'attività societaria.

## Parte Speciale L

### Sicurezza sul lavoro (art. 25 septies del d. lgs. 231/2001)

#### 1. Attività sensibili

In ragione dell'attività svolta, il rischio di esposizione ai reati richiamati in ambito di sicurezza sul lavoro è rilevante. L'ambito in questione è da ricollegarsi per lo più ad una politica societaria di gestione della salute, della sicurezza sui luoghi di lavoro e del rispetto e attuazione delle norme antinfortunistiche. In quest'ottica, la Società deve costantemente ricercare il miglioramento delle pratiche in essere al fine di tutelare il proprio personale, garantendo l'adeguata utilizzazione delle risorse, anche economiche, per il raggiungimento di tale obiettivo. Particolare attenzione deve, inoltre, essere garantita rispetto all'informazione, formazione e addestramento del personale, presupposti indefettibili per garantire il rispetto del d. lgs. 81/2008 nell'ottica di una consapevolezza dei rischi dell'attività lavorativa e delle misure preventive da porre in essere. Si richiamano, in merito, le misure indicate nel presente Modello relative all'assunzione e gestione del personale, anche tenuto conto di quanto previsto dal d. lgs. 81/2008.

Si può ritenere la rilevanza di quanto segue:

- ◆ politiche di gestione della sicurezza e adempimenti correlati:
  - attività d'ufficio: con specifico riferimento alla sicurezza sul lavoro, assumono rilevanza tutte le esposizioni a rischio di infortuni determinati dalle attività prettamente d'ufficio;
  - attività operative: si ha riguardo a tutte le attività connesse all'uso di macchinari, gestione del prodotto, dalla produzione al carico/scarico del prodotto;
  - accesso esterno alla struttura: si ha riguardo a tutta l'area esterna di accesso allo stabilimento produttivo ed agli uffici, ove si può presentare un pericolo di infortunio tenuto conto delle attività di manovra, come quelle di carico/scarico merci, stante l'accesso di vetture e automezzi;
  - trasferta: si ha riguardo ai rischi connessi al personale commerciale in trasferta;
- ◆ gestione dei servizi di terzi (appalti).

#### 2. Presupposti normativi e adempimenti correlati

La Società ha adottato un Sistema di Gestione integrato Ambiente Sicurezza e Salute in rispondenza dei criteri ISO 45001 e ISO 14001, oggetto di revisione e certificazione annuale.

Il Manuale si informa alle buone pratiche ma anche al rispetto della normativa di riferimento in materia di salute e sicurezza sul lavoro, con specifico riguardo a quanto previsto dal d. lgs. 81/2008. In merito si precisano le seguenti prescrizioni:

- ◆ definire la politica aziendale in tema di salute e sicurezza nei luoghi di lavoro, individuare gli

- obiettivi da raggiungere ed infine predisporre un Piano di Miglioramento, all'interno del quale è necessario individuare le responsabilità, le tempistiche, le priorità degli interventi da realizzare e le risorse umane, strumentali e finanziarie necessarie alla loro realizzazione;
- ◆ procedere alla redazione e all'aggiornamento periodico del Documento di Valutazione dei rischi (DVR) e, se previsto, del Documento di Valutazione dei rischi interferenziali (DUVRI) e procedere alla predisposizione delle misure di prevenzione e protezione conseguenti;
  - ◆ rispettare gli *standards* tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
  - ◆ compiere attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
  - ◆ procedere alla nomina del Responsabile del Servizio Prevenzione e Protezione e, se del caso, di Addetti al Servizio Prevenzione e Protezione;
  - ◆ acquisire la documentazione e le certificazioni obbligatorie di legge;
  - ◆ individuare l'organigramma della sicurezza;
  - ◆ effettuare le attività di informazione, formazione e addestramento previste dalla normativa;
  - ◆ attuare la sorveglianza sanitaria, laddove previsto dalla normativa;
  - ◆ redigere il Piano di emergenza e primo soccorso;
  - ◆ predisporre riunioni periodiche di sicurezza e consultazione dei rappresentanti dei lavoratori per la sicurezza, al fine di assicurare l'informazione ed il coinvolgimento delle persone;
  - ◆ definire attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
  - ◆ procedere con attività di vigilanza da attuare attraverso verifiche periodiche volte al controllo del rispetto, della corretta applicazione e dell'efficacia delle procedure adottate nonché con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
  - ◆ attuare tutte le altre misure, anche non previste dalla normativa, volte ad assicurare la sicurezza di tutti i destinatari della normativa individuata, nonché piani di miglioramento per quanto già in essere;
  - ◆ predisporre idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1 dell'art. 30 del d.lgs. 81/2008;
  - ◆ prevedere, per quanto richiesto dalla natura e dalle dimensioni dell'organizzazione e del tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, la valutazione, la gestione ed il controllo del rischio così come previsto al comma

3 dell'art. 30 del d.lgs. 81/2008;

- ◆ predisporre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
- ◆ prevedere un idoneo sistema di controllo sull'attuazione del medesimo Modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del Modello devono essere adottati quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e dell'igiene del lavoro ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

Per quanto concerne la ISO 45001, basata sul Plan-Do-Check-Act (pianifica, fai, verifica, agisci), il Sistema di gestione mira a:

- miglioramento continuo delle prestazioni relative alla salute e sicurezza sui luoghi di lavoro;
- soddisfacimento dei requisiti legali e di altri requisiti;
- raggiungimento degli obiettivi per la salute e sicurezza sui luoghi di lavoro.

Si articola secondo una serie di fattori chiave:

- leadership, impegno, responsabilità e obbligo di rendere conto dell'alta direzione;
- sviluppo, guida e promozione da parte dell'alta direzione di una cultura nell'organizzazione che supporti il conseguimento dei risultati attesi dal sistema di gestione;
- comunicazione;
- consultazione e partecipazione dei lavoratori e dei rappresentanti dei lavoratori;
- assegnazione delle risorse necessarie per mantenerlo;
- politiche per la salute e sicurezza, che siano compatibili con gli obiettivi strategici globali e con gli indirizzi dell'organizzazione;
- processi efficaci per identificare i pericoli, tenere sotto controllo i rischi per la salute e sicurezza sui luoghi di lavoro e sfruttarne le opportunità;
- valutazione continua delle prestazioni e monitoraggio del sistema di gestione per migliorare le prestazioni;
- integrazione del sistema di gestione per la salute e sicurezza nei processi di *business* dell'organizzazione;
- obiettivi in materia di salute e sicurezza allineati alla relativa politica e che tengano conto dei pericoli, dei rischi e delle opportunità per l'organizzazione;

- conformità a requisiti, anche legali.

## Parte Speciale M

### Ricettazione, riciclaggio e autoriciclaggio (art. 25 octies del d. lgs. 231/2001)

#### 1. Attività sensibili

In ragione dell'attività svolta, si ritiene prudenzialmente di individuare le seguenti aree sensibili:

- ◆ gestione fiscale: si evidenzia tale aspetto per il rischio correlato principalmente al reato di autoriciclaggio. A titolo esemplificativo si evidenzia il possibile risparmio di imposta proveniente da illecito tributario;
- ◆ rapporti infragruppo: si rimanda, tra gli altri, al rischio di autoriciclaggio riconducibile a condotte di gruppo, prevalentemente per possibili illeciti tributari e investimenti infragruppo;
- ◆ rapporti con clienti, distributori e agenti, anche transnazionali: si richiama il rapporto con clientela, distributori e agenti, coinvolti a vario titolo in società esposte al rischio di riciclaggio;
- ◆ selezione e gestione del rapporto con fornitori, anche transnazionali (anche in relazione alle materie prime ed al packaging): tali attività sono riconducibili al rischio di fornitori, coinvolti a vario titolo in società esposte al rischio di ricettazione e riciclaggio;
- ◆ investimenti finanziari, per il rischio di utilizzo strumentale per la commissione dei reati di cui alla presente Parte Speciale;
- ◆ gestione dei flussi finanziari, anche transnazionali: si rimanda al profilo strumentale per la commissione dei reati presupposto.

## Parte Speciale N

### Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori

#### 1. Attività sensibili

In ragione dell'attività svolta, si ritiene prudenzialmente di individuare, quali aree sensibili:

- gestione dei flussi finanziari, con rimando all'ipotesi di pagamento in criptovalute a fronte di attacchi informatici.
- gestione dei sistemi informativi da parte di utenti, dell'Amministratore di Sistema e di utilizzatori di *pc administrator* oppure utenti con accessi/permessi privilegiati poiché le condotte in esame possono essere perpetrate attraverso condotte di detenzione, produzione e, nel caso di specie, uso di programmi informatici, rispetto ai quali coloro che abbiano accessi o permessi privilegiati possono incorrere nel rischio qui richiamato.

## Parte Speciale O

### Delitti contro il diritto d'autore (art. 25 novies del d. lgs. 231/2001)

#### 1. Attività sensibili

In ragione dell'attività svolta, si presentano i seguenti rischi, per lo più connessi all'utilizzo di strumenti informatici e relativi *software*:

- ◆ utilizzo di prodotti coperti da licenze o brevetti o *copyright*: il personale, in particolare, nel proprio operato può agire in violazione del diritto d'autore in caso di eventuali utilizzi abusivi, connessi a un possibile risparmio di costi per la Società medesima;
- ◆ utilizzo dei sistemi informatici da parte dell'Amministratore di sistema e di utilizzatori di Pc Administrator oppure utenti con accessi/permessi privilegiati: tale attività è equiparabile al punto precedente. Tuttavia, si ritiene opportuna una specifica puntuale, dal momento che i soggetti indicati, per posizione, sono maggiormente in grado di attuare *upload/download* in violazione.
- ◆ selezione dei fornitori., affinché siano in grado di garantire la corretta gestione del diritto d'autore sulle forniture;
- ◆ utilizzo dei propri sistemi informatici da parte degli utenti: si vuole evidenziare la necessità di attuare forme di controllo in merito alla gestione dei propri dispositivi (Pc, tablet, cellulari) per evitare che si verificano condotte di *upload/download*, riguardanti l'utilizzo, l'immissione e la condivisione di contenuti protetti da diritti d'autore e *file sharing*, consistente, invece, nello scambio di file al di fuori degli ordinari e leciti circuiti commerciali oggetto di proprietà intellettuale.

## **Parte Speciale P**

### **Delitti contro l'Autorità Giudiziaria (art. 25 decies del d. lgs. 231/2001)**

#### **1. Attività sensibili**

Sebbene non vi sia alcun richiamo all'attività svolta né, tantomeno, vi siano precedenti idonei a far ritenere sussistente il rischio di cui al presente paragrafo, non può escludersi a priori che, nella remota ipotesi dell'istaurarsi di un procedimento penale in capo alla Società o a soggetti che vi rivestano ruoli connessi a specifiche responsabilità, vi sia la rilevanza della seguente area sensibile:

- ◆ rapporti con l'Autorità Giudiziaria (nell'ambito di procedimenti penali): si pensi alle ipotesi in cui la Società o le società clienti fossero coinvolti in accertamenti penali e venisse richiesto, da parte dell'Autorità Giudiziaria, al personale di fornire informazioni circa i fatti oggetto dell'istaurando procedimento penale o di fornire la propria collaborazione.

#### **2. Principi di comportamento**

In merito alla presente attività sensibile si precisa, in termini generali, che i destinatari del presente Modello devono attenersi alle disposizioni societarie, al presente Modello di organizzazione e gestione e al Codice Etico.

Ogni destinatario è tenuto a collaborare con l'Autorità Giudiziaria in piena libertà e correttezza, nel rispetto della verità dei fatti.

Nessuna influenza può essere attuata nei confronti di dipendenti ovvero destinatari del presente Modello per evitare di garantire la più ampia collaborazione con l'Autorità Giudiziaria nel caso di procedimenti penali che prevedano il coinvolgimento della Società o delle altre società appartenenti al Gruppo.

In presenza di rischi di pressioni, anche solo potenziali, deve essere data tempestiva informativa all'Organismo di Vigilanza affinché possano attivare misure di controllo.

Eventuali violazioni delle presenti prescrizioni non rispondono al volere societario e sono da considerarsi violazioni disciplinari, passibili di sanzione.

## Parte Speciale Q

### Reati ambientali (art. 25 undecies del d. lgs. 231/2001)

#### 1. Attività sensibili

In ragione dell'attività di impresa svolta si ritiene opportuno riconoscere un rischio correlato ai reati individuati.

In tal senso è possibile individuare le seguenti aree di rischio:

- ◆ gestione dei rifiuti, da considerarsi rilevanti sia per quanto attiene gli imballaggi che altri rifiuti, quali toner, neon, solventi di laboratorio, che richiedono smaltimenti secondo disposizione normativa. Occorre, inoltre, considerare la corretta gestione, sia in termini di luoghi idonei sia per il rischio di violazione delle prescrizioni in materia di depositi temporanei di rifiuti ovvero di violazione dei limiti prescritti nelle autorizzazioni;
- ◆ gestione delle immissioni in atmosfera: il rischio è correlato alla corretta gestione delle immissioni in atmosfera nel rispetto della normativa di riferimento e delle autorizzazioni di cui dispone la Società (AUA);
- ◆ gestione degli scarichi di acque reflue industriali: il rischio è correlato alla corretta gestione degli scarichi di acque reflue industriali nel rispetto della normativa di riferimento e delle autorizzazioni di cui dispone la Società (AUA);
- ◆ selezione dei fornitori e gestione dei relativi rapporti: i rischi derivanti dai rapporti con i fornitori sono di due tipi, in questa area sensibile:
  - di acquisto di esemplari di specie vegetali selvatiche protette, in violazione dell'artl 727 bis c.p., tenuto conto delle prescrizioni CITES;
  - relativi all'instaurazione di rapporti con soggetti non dotati delle prescritte autorizzazioni ovvero collusi con organizzazioni criminali, per le società di smaltimento dei rifiuti;
- ◆ predisposizione di dichiarazioni o richieste alla Pubblica Amministrazione, anche per via telematica: relativamente ai reati ambientali questa attività presenta rischi connessi alla formazione di autorizzazioni sulla base di false attestazioni da parte della Società.

#### 2. Presupposti normativi e adempimenti correlati

La Società intende perseguire una politica di gestione ambientale e ha adottato un Sistema di Gestione integrato Ambiente Sicurezza e Salute conforme ai requisiti UNI EN ISO 14000, UNI EN ISO 45001 e al Regolamento EMAS, per soddisfare le continue necessità e aspettative, nel rispetto dell'ambiente e della salute e sicurezza nei luoghi di lavoro, come parte integrante del proprio processo di sviluppo.

Esso si pone i seguenti obiettivi, a partire dall'analisi ambientale del contesto di riferimento:

- proteggere l'ambiente mediante la prevenzione e mitigazione di impatti ambientali negativi;
- mitigare il potenziale effetto negativo delle condizioni ambientali sull'organizzazione;
- supportare l'organizzazione nell'adempimento dei propri obblighi di conformità;
- migliorare le prestazioni ambientali;
- controllare e influenzare il modo in cui i prodotti e servizi dell'organizzazione sono progettati, fabbricati, distribuiti, consumati e smaltiti, utilizzando una prospettiva di ciclo di vita che possa evitare lo spostamento involontario in un'altra fase del ciclo di vita degli impatti ambientali;
- raggiungere benefici finanziari e operativi che possono derivare dall'attuazione di valide alternative per l'ambiente in grado di rafforzare la posizione di mercato dell'organizzazione;
- comunicare informazioni ambientali alle parti interessate rilevanti.

Correntemente con la politica ambientale, gli esiti attesi di tale sistema sono:

- miglioramento delle prestazioni ambientali;
- soddisfacimento degli obblighi di conformità;
- raggiungimento degli obiettivi ambientali.

## **Parte Speciale R**

**Reati di clandestinità e xenofobia (art. 25 duodecies e art. 25 terdecies del d. lgs. 231/2001)**

### **1. Attività sensibili**

Il rischio legato a questa tipologia di reati si presenta estremamente basso.

Tuttavia, in via precauzionale, si potrebbero comunque individuare le seguenti aree di rischio:

- ◆ selezione, assunzione e gestione del personale (straniero): si ha particolare riguardo alle verifiche da attuare nel caso di assunzione di personale straniero che possa essere clandestino, mediante la predisposizione di una procedura specifica di controllo e l'implementazione di un sistema di monitoraggio delle vicende relative ai permessi di soggiorno dei lavoratori stranieri (scadenze, rinnovi...);
- ◆ gestione dei servizi di terzi (appalti), correlati al rischio di presenza di lavoratori irregolari.

## **Parte Speciale S**

**Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25 quaterdecies d. lgs. 231/2001)**

### **1. Attività sensibili**

Data l'attività tipica di impresa svolta dalla Società, è da escludersi la configurabilità dei reati in esame, di fatto non coerenti con le attività dalla stessa svolte.

## Parte Speciale T

### Reati tributari (art. 25 quinquiesdecies del d. lgs. 231/2001)

#### 1. Attività sensibili

I reati di natura tributaria rappresentano un rischio in relazione alle attività di seguito indicate:

- ◆ gestione fiscale, correlata alla predisposizione e presentazione delle dichiarazioni fiscali, liquidazione e versamento dei tributi, tenuta e custodia della documentazione obbligatoria;
- ◆ gestione dei sistemi informativi, correlata alla corretta archiviazione dei documenti contabili al fine di impedirne l'occultamento o la distruzione ovvero garantire la tracciabilità del processo;
- ◆ predisposizione dei bilanci e delle scritture contabili: si rimanda a tale profilo in quanto presupposto per la determinazione dell'imponibile fiscale e dei tributi societari. In particolare, si richiama la gestione amministrativo-contabile generale, alla gestione di incassi e pagamenti, alla contabilità fornitori e piccola cassa;
- ◆ rapporti infragruppo: ci si riferisce in particolare alle condotte che prevedano la gestione della fiscalità complessiva delle varie società del Gruppo; si sottolinea il carattere di transnazionalità del Gruppo, ove si evidenziano i rischi nell'ambito del transfer pricing e dei trasferimenti di fondi tra società del Gruppo e tra conti correnti della medesima Società. Anche in tale ambito si richiama la corretta gestione amministrativo-contabile;
- ◆ gestione delle operazioni straordinarie, con rimando alle ipotesi di acquisizione/cessione/fusione atte a determinare forme di sottrazione fraudolenta al pagamento di imposte;
- ◆ gestione dei flussi finanziari, in considerazione della corretta determinazione dei pagamenti rispetto alla prestazione;
- ◆ rapporti con i clienti, con specifico rimando alla prestazione effettivamente eseguita e alla relativa fatturazione o documentazione equipollente;
- ◆ rapporti con i fornitori, con specifico rimando alla prestazione effettivamente eseguita e alla relativa fatturazione o documentazione equipollente;
- ◆ rapporti con i consulenti, con specifico rimando alla prestazione effettivamente eseguita e alla relativa fatturazione o documentazione equipollente;
- ◆ gestione del personale, con riferimento al rischio di lavoratori in nero nonché agli adempimenti fiscali e previdenziali correlati;
- ◆ gestione delle note spese, in relazione alla relativa rendicontazione;
- ◆ gestione delle sponsorizzazioni, in considerazione dell'effettività dell'esecuzione contrattuale rispetto al contenuto della sponsorizzazione e della corretta contabilizzazione;

- ◆ gestione delle donazioni e regalie, per la loro rendicontazione.

## Parte Speciale U

### Contrabbando (art. 25 sexiesdecies del d. lgs. 231/2001)

#### 1. Attività sensibili

I reati individuati dalla presente sezione rappresentano un rischio in relazione alle attività di seguito indicate:

- predisposizione di dichiarazioni o richieste alla Pubblica Amministrazione, anche per via telematica, con specifica attinenza alle Autorità doganali;
- selezione dei fornitori e gestione dei relativi rapporti con riguardo:
  - alla selezione degli spedizionieri per le attività di esportazione, per il rischio che non adempiano alle norme di legge in materia doganale;
  - agli acquisti, nei limiti dell'importazione delle materie prime, per evitare il rischio correlato all'introduzione di merci estere in violazione delle prescrizioni stabilite dalla normativa doganale;
- realizzazione del prodotto, al fine di specificare l'assenza di fabbricazione clandestina secondo i termini di legge;
- gestione fiscale per le tematiche di rilevanza doganale;
- predisposizione e del bilancio e delle scritture contabili in relazione alla possibile indicazione nei registri in contabilità di merci importate effettuate effettuando manovre fraudolente dirette ad indurre in errore l'autorità doganale sugli elementi dell'accertamento, ovvero rendendo false dichiarazioni in ordine alla destinazione o all'uso dei prodotti ovvero alle caratteristiche degli stessi.

## **Parte Speciale V**

**Delitti contro il patrimonio culturale e riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25 septiesdecies e 25 duodecies del d. lgs. 231/2001)**

### **1. Attività sensibili**

L'unico rischio potenzialmente riconducibile all'area di attività della Società potrebbe essere legato alla compravendita di beni culturali, che, tuttavia, non viene esercitata dalla Società. Non si ravvisa, inoltre, alcun interesse o vantaggio per la Società negli ambiti di riferimento dei reati individuati. Se ne esclude, pertanto, la rilevanza.