A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

MODELLO ORGANIZZATIVO

DI

AMRA S.P.A.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO A

REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

(Artt. 24 e 25 D.Lgs. 231/01)

(Rubrica modificata dall'art. 1, comma 77, lett. a) della Legge 6 novembre 2012 n. 190)

1. REATI PRESUPPOSTO

Si riportano, di seguito, le rubriche dei reati contro la Pubblica Amministrazione presi in considerazione dal D.Lgs. 231/01:

- *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 c.p., 2° comma, n. 1);
- *Truffa aggravata per il conseguimento di erogazioni pubbliche* (art. 640-*bis* c.p.);
- *Frode informatica in danno dello Stato o di altro ente pubblico* (art. 640-*ter* c.p.);
- *Corruzione per l'esercizio della funzione* (art. 318 c.p. - art. 321 c.p.);
- *Istigazione alla corruzione* (art. 322 c.p.);
- *Concussione* (art. 317 c.p.);
- *Corruzione per un atto contrario ai doveri di ufficio* (art. 319 c.p. - art. 319-*bis* c.p. - art. 321 c.p.);
- *Corruzione in atti giudiziari* (art. 319-*ter* c.p. - art. 321 c.p.);
- *Corruzione di persona incaricata di un pubblico servizio* (art. 320 c.p.);
- *Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri* (art. 322-*bis* c.p.);
- *Induzione indebita a dare o promettere utilità* (art. 319 – *quater* c.p.).

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

I reati qui considerati hanno come presupposto l'instaurazione e la gestione di rapporti con la Pubblica Amministrazione.

Per "*Pubblica Amministrazione*" si intendono tutti quei soggetti, pubblici o privati, che svolgono una funzione pubblica o un pubblico servizio. Tale categoria di reati comporta necessariamente un contatto o un rapporto con soggetti appartenenti alla Pubblica Amministrazione, che possono essere distinti in pubblici ufficiali o incaricati di pubblico servizio.

Il "*pubblico ufficiale*" è colui che esercita una pubblica funzione legislativa, giudiziaria o amministrativa e può formare o manifestare la volontà della pubblica amministrazione ovvero esercitare poteri autoritativi o certificativi.

A titolo esemplificativo e non esaustivo si considerano Pubblici Ufficiali i membri delle amministrazioni statali e territoriali, i membri delle amministrazioni sovranazionali (ad esempio, dell'Unione Europea), i NAS, i membri delle Autorità di Vigilanza, i membri delle Forze dell'Ordine e della Guardia di Finanza, i membri delle Camere di Commercio, gli amministratori di enti pubblici economici, i membri delle Commissioni Edilizie, i Giudici, gli Ufficiali Giudiziari, gli organi ausiliari dell'Amministrazione della Giustizia (ad esempio, i curatori fallimentari).

L'"*incaricato di un pubblico servizio"* è invece colui il quale a qualunque titolo presta un pubblico servizio.

A norma dell'art. 358 c.p. "*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"*.

A titolo esemplificativo e non esaustivo si considerano incaricati di pubblico servizio i dipendenti del SSN, gli addetti all'ufficio cassa di un Ente pubblico, i dipendenti di Enti Ospedalieri, dell'ASL, dell'INAIL, dell'INPS, i dipendenti di Aziende Energetiche Municipali; i dipendenti di Uffici Postali ed Uffici Doganali; i membri dei

Consigli Comunali, i dipendenti delle Ferrovie dello Stato e della Società Autostrade.

Sulla scorta della documentazione raccolta a riguardo della Società, nell'ambito delle attività che:

- implicano rapporti con pubblici ufficiali, incaricati di pubblico servizio, organi ispettivi, enti pubblici erogatori di contributi e finanziamenti agevolati, enti pubblici e soggetti incaricati di pubblico servizio titolari di poteri autorizzativi, concessori, abilitativi, certificativi o regolatori;

- comportano la partecipazione a pubbliche gare o a trattative con enti pubblici per l'affidamento di lavori in appalto o in concessione, in riferimento alle procedure di selezione, di autorizzazione del subappalto, di gestione dell'eventuale contenzioso con il committente, di collaudo delle opere eseguite o di controllo di conformità del prodotto rispetto alle previsioni di contratti, disciplinari o capitolati;

sono individuate, presso la Società, le operazioni a rischio individuate nella *Check List* prodotta dalla Direzione Aziendale e messa a disposizione dell'Organismo di Vigilanza, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui agli artt. 24 e 25 del D.Lgs. 231/01.

Ne è emerso, in particolare, che la Società abitualmente partecipa a gare d'appalto indette dalle pubbliche amministrazioni, rilevandone l'esistenza attraverso il monitoraggio dei siti degli enti che abitualmente utilizzano i prodotti della Società stessa. La partecipazione avviene attraverso la raccolta e l'invio della documentazione alla pubblica amministrazione.

Tenuto anche conto della rilevanza via via maggiore che gli adempimenti in materia di anticorruzione assumono (cfr. ad esempio la Legge 6 novembre 2012, n. 190 recante le "*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità della pubblica amministrazione*"), si ritiene quindi di adottare apposita procedura da utilizzarsi.

La Società intrattiene altresì rapporti con l'amministrazione finanziaria e, in caso di

verifiche o ispezioni, con le rilevanti pubbliche autorità.

Talvolta, adotta politiche marketing e di omaggistica ai clienti che vanno regolate per i casi in cui i medesimi riguardino in via incidentale soggetti facenti parte della Pubblica Amministrazione.

Alla luce di quanto sopra e dell'individuazione delle attività sensibili relative alla presente Sezione Speciale, si è ritenuto opportuno predisporre apposite procedure di:

i) partecipazione a gare ed appalti;
ii) gestione delle risorse finanziarie;
iii) gestione dei rapporti occasionali con l'amministrazione finanziaria e le autorità di vigilanza e controllo;
iv) marketing ed omaggistica a clienti;

che vengono di seguito riportate.

3. PROCEDURE GENERALI

La presente sezione prevede l'espresso obbligo, a carico di tutto il personale direttivo ed i dipendenti interessati, e, tramite apposite clausole contrattuali, a carico di consulenti, fornitori e partner, di:

1. una stretta osservanza di tutte le leggi e regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione ed alle attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio;

2. gestione di qualsiasi rapporto con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza.

La presente sezione prevede, conseguentemente, l'espresso divieto a carico degli esponenti aziendali in via diretta e a carico dei collaboratori esterni tramite apposite clausole contrattuali, di porre in essere:

1. comportamenti tali da integrare le fattispecie di reato sopra considerate;

2. comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

3. qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Per ciascuna delle operazioni di carattere significativo, rientranti nei tipi individuati all'articolo che precede sono previste specifiche procedure, in forza delle quali:

a) sia sempre individuato un responsabile relativo al procedimento;

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

c) sia possibile procedere alla tracciabilità e verificabilità *ex post* delle transazioni fatte con la Pubblica Amministrazione;

d) tutta la comunicazione in entrata ed uscita da e verso la Pubblica Amministrazione deve avvenire in forma scritta;

e) non vi sia identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;

f) i documenti riguardanti l'attività di impresa siano archiviati e conservati, a cura della funzione aziendale competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;

g) qualora il servizio di archiviazione e/o conservazione dei documenti sia svolto, per conto della Società, da un soggetto ad essa estraneo, il servizio deve essere regolato da un contratto nel quale si preveda, tra l'altro, che il soggetto che presta il servizio alla Società rispetti specifiche procedure di controllo idonee a

non permettere la modificazione successiva dei documenti archiviati, se non con apposita evidenza;

h) sia garantito il controllo dei flussi finanziari aziendali ed in particolare dei flussi relativi alle fatture passive;

i) l'accesso ai documenti già archiviati, di cui alle due lettere precedenti, sia sempre motivato e consentito solo alle persone autorizzate in base alle norme interne, al Collegio Sindacale, al revisore dei conti ed all'Organismo di Vigilanza;

j) non siano corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, agenti o a soggetti pubblici in misura non congrua rispetto alle prestazioni rese alla Società e non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;

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

l) fermo il rispetto del D.Lgs. 231/07 in materia di antiriciclaggio, nessun tipo di pagamento può esser effettuato in contanti o in natura**,** al di fuori dei pagamenti di modico valore ed ove – per ragioni concrete – non sia possibile provvedere tramite canali bancari o attraverso titoli non trasferibili;

m) coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle attività di pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

Nell'ambito dei suddetti comportamenti, è comunque fatto divieto, in particolare, di:

- effettuare prestazioni in favore di *outsourcer*, consulenti, partner, collaboratori e terzi in generale che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi, o in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;

- effettuare elargizioni in denaro o accordare indebiti vantaggi di qualsiasi natura – anche a favore di terzi collegati - (ad esempio la promessa di assunzione) a funzionari pubblici.

In generale, nella predisposizione delle proprie procedure e nell'esercizio delle attività che coinvolgono la Pubblica Amministrazione, la Società tiene conto dei contenuti del *Codice di comportamento dei dipendenti pubblici* (Consiglio dei Ministri n. 72 dell' 8 marzo 2013 in attuazione della legge anticorruzione n. 190 del 6 novembre 2012) e trae ispirazione anche dalla *best practice* internazionale, come ad esempio dai contenuti del *Bribary Act Guidance* del *Ministery of Justice* della Gran Bretagna consultabile anche al seguente link:
http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

Le procedure adottate dalla Società si conformeranno pertanto ai seguenti principi:

- proporzionatezza delle procedure adottate all'effettivo rischio di commissione dei reati tenuto conto della tipologia, delle dimensioni e del tipo di attività della Società;

- impegno del *top management* nella lotta ai comportamenti illeciti con adozione di una diffusa cultura aziendale nella quale i comportamenti corruttivi non sono in alcun modo incentivati e/o ritenuti tollerabili;

- valutazione periodica del rischio di commissione dei reati da effettuarsi sulla base di informazioni documentate o documentabili;

- controllo costante delle attività concretamente poste in essere (c.d. *due diligence*) con livelli di approfondimento correlato al rischio di commissione dei reati;

- formazione costante ai Destinatari sui contenuti delle procedure;
- verifica ed adeguamento nel tempo delle procedure adottate.

4. PROCEDURE SPECIFICHE

A) Il responsabile interno

Per tutte le operazioni a rischio che concernono le attività sensibili individuate nella presente Parte Speciale, va individuato un responsabile interno per l'attuazione dell'operazione, che corrisponde, salvo diversa indicazione, al Procuratore a tal fine incaricato per la gestione dell'operazione a rischio considerata.

Il responsabile interno:

- può chiedere informazioni e chiarimenti a tutte le funzioni aziendali, alle unità operative o ai singoli soggetti che si occupano o si sono occupati dell'operazione a rischio;
- informa periodicamente l'Organismo di Vigilanza dei fatti rilevanti relativi alle operazioni a rischio della propria funzione;
- informa tempestivamente l'Organismo di Vigilanza di qualunque criticità o conflitto di interessi sorto nell'ambito dei rapporti tra la propria funzione e la Pubblica Amministrazione.

B) Partecipazione a procedure di gara indette da enti od organismi pubblici italiani o stranieri

Con riferimento a tale area le procedure devono prevedere che:

- sia verificata la corretta applicazione della procedura di partecipazione ai bandi, sia con riferimento alla fase di ricezione dell'informazione circa la natura del bando cui si vorrà partecipare anche in forma associata (ovvero il modo con cui si è venuti a conoscenza del bando), sia con riferimento alla valutazione del

bando stesso, alla sua approvazione, sia alla predisposizione e spedizione della documentazione all'ente (o alla capofila) che indice il relativo bando;

- sia verificata l'esistenza di eventuali conflitti di interessi, inerenti anche la possibilità di partecipare al bando;
- vengano effettuati i controlli sulla documentazione attestante l'esistenza di condizioni essenziali per partecipare ai bandi sia direttamente che tramite raggruppamenti temporanei di imprese;
- nel caso di ATI o RTI, si effettuerà il controllo sulla sussistenza dei requisiti di onorabilità e professionalità dei partner della Società;
- si proceda alla tracciabilità e verificabilità *ex post* delle transazioni fatte con la Pubblica Amministrazione tramite adeguati supporti documentali/informativi;
- i partner, i collaboratori ed i consulenti che possono eventualmente partecipare al bando o che richiedono la partecipazione della Società, devono essere scelti e valutati con metodi trasparenti e secondo specifica procedura aziendale;
- siano monitorati i poteri anche con riferimento alla verifica delle firme autorizzative per i bandi vinti e per quelli a cui si partecipa;
- nel caso in cui le pratiche per l'ammissione alle suddette procedure fossero affidate dalla Società a terzi soggetti a ciò specializzati, tali attività dovranno essere regolate da un contratto nel quale si preveda, tra l'altro, che il soggetto incaricato a prestare il servizio in favore della Società disponga delle necessarie competenze tecnico-professionali ed autorizzazioni a svolgere il servizio richiesto e garantisca alla Società specifiche procedure di controllo idonee a verificare il contenuto delle comunicazioni, dichiarazioni, istanze, documenti e quant'altro previsto dai bandi di gara che verranno inviati e/o depositati in nome e per conto della Società stessa presso gli enti e/o gli organismi suddetti.

Poiché, come sopra esposto, la Società partecipa con costante frequenza a gare d'appalto indette da società partecipate da enti pubblici, il responsabile interno,

d'intesa con l'Organismo di Vigilanza, dovrà curare con la massima attenzione l'implementazione e la conoscenza da parte dei soggetti aziendali coinvolti, delle relative procedure.

C) Gestione delle risorse finanziarie

Per le operazioni di carattere significativo relative alla gestione delle risorse finanziarie, la procedura prevede quanto segue:

a) non vi sia identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;

b) siano stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la fissazione di soglie quantitative coerenti alle competenze gestionali e alle responsabilità organizzative affidate alle singole persone;

c) il superamento dei limiti di cui al punto precedente possa avvenire solo nel rispetto delle vigenti procedure di autorizzazione e previa adeguata motivazione;

d) le operazioni che comportano utilizzazione o impiego di risorse economiche o finanziarie debbano avere una causale espressa ed essere documentate e registrate in conformità ai principi di correttezza professionale e contabile. Il processo decisionale deve essere verificabile;

e) l'impiego di risorse finanziarie sia motivato dal soggetto richiedente, che ne attesta la congruità;

f) sia effettuato un completo ed attento controllo sulla documentazione contabile aziendale ed in particolar modo sulle fatture passive.

D) Gestione dei rapporti occasionali con l'amministrazione finanziaria e le autorità di vigilanza e di controllo (ad esempio, in caso di ispezioni)

Con riferimento a tale area di rischio, le procedure devono prevedere che:

- durante eventuali ispezioni giudiziarie, tributarie e amministrative e quelle poste in essere dalle Attività di Vigilanza di settore (quali ad esempio quelle preposte al rispetto della normativa sulla sicurezza, alle verifiche tributarie, INPS), deve essere individuato in ambito aziendale un responsabile, incaricato di assicurare il coordinamento tra gli addetti delle diverse unità aziendali, ai fini del corretto espletamento da parte di questi ultimi delle attività di propria competenza e nell'ottica della massima collaborazione e trasparenza nei confronti dell'Autorità;

- tale responsabile ha inoltre il compito di assicurare il coordinamento tra i diversi uffici aziendali competenti ed i funzionari delle Autorità, ai fini dell'acquisizione da parte di questi ultimi degli elementi richiesti;

- di tutto il procedimento relativo all'ispezione devono essere redatti e conservati gli appositi verbali;

- il responsabile incaricato provvede a stendere un'apposita informativa sull'indagine avviata dall'Autorità, che deve essere periodicamente aggiornata in relazione agli sviluppi dell'indagine stessa ed al suo esito;

- tale informativa deve essere inviata all'Organismo di Vigilanza, nonché agli altri uffici aziendali competenti in relazione alla materia trattata.

E) <u>Marketing ed omaggistica ai clienti</u>

E' fatto divieto di distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale, vale a dire, ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale.

In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri, o a loro familiari, che possa influenzarne la discrezionalità o l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda.

Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore, o perché volti a promuovere la *brand image* della Società.

Tutti i regali offerti eccedenti il modico valore devono essere documentati in modo idoneo, per consentire all'Organismo di Vigilanza di effettuare verifiche al riguardo.

Qualora la Società sponsorizzi o comunque contribuisca economicamente alla realizzazione di eventi indetti dalla Pubblica Amministrazione, l'importo sponsorizzato od erogato dalla Società dovrà mantenersi entro i limiti del modico valore.

Il responsabile della funzione si assicurerà che l'erogazione venga effettuata in favore dell'ente organizzatore e non di soggetti persone fisiche appartenenti allo stesso.

Per ogni sponsorizzazione effettuata dalla Società deve essere redatto un breve resoconto scritto contenente quantomeno il nominativo dell'ente beneficiario, la natura dell'elargizione, le ragioni che hanno sostenuto la valutazione ad accoglierla ed il valore complessivo della stessa.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nel presente Allegato.

Il presente Allegato e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale, al fine di garantire il raggiungimento delle finalità del Modello.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO B

FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO

(Art. 25 bis D.Lgs. 231/01)

(Articolo aggiunto dall'art. 6 del Decreto Legge 25 settembre 2001 n. 350 convertito, con modificazioni, con Legge 23 novembre 2001 n. 409. Articolo successivamente modificato dall'art. 17 della Legge 23 luglio 2009 n. 99)

1. REATI PRESUPPOSTO

Si riportano, di seguito, le rubriche di tutti i reati presi in considerazione dal D.Lgs. 231/01:

- *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.).

L'art. 17 della legge 23 luglio 2009, n. 99 ha modificato l'art. 25 *bis* D.Lgs. 231/01 estendendone l'ambito di applicazione, originariamente limitato alla "*falsità in monete, carte di pubblico redito e valori in bollo*" alle azioni contrarie alle

disposizioni normative che tutelano gli strumenti e i segni di riconoscimento.

Sono quindi stati inseriti tra i nuovi reati presupposto:

- *la contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni* (Art. 473 c.p.)*;*
- *l'introduzione nello Stato e commercio di prodotti con segni falsi* (Art. 474 c.p.).

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Sulla base dell'analisi dell'attività della Società e dei suoi processi, si ritiene che non vi siano operazioni a rischio.

Si ritiene, pertanto, che non vi siano ravvisabili rischi specifici con riferimento ai reati contemplati nel presente Allegato.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO C

REATI SOCIETARI

(Art. 25 ter D.Lgs. 231/01)

(Articolo aggiunto dall'art. 3 del D.Lgs. 11 aprile 2002 n. 61. Articolo successivamente modificato dall'art. 39, comma 5 della Legge 28 dicembre 2005 n. 262 e quindi dall'art. 12 della Legge 27 maggio 2015 n. 69 in materia di "Disposizioni in materia di delitti contro la pubblica amministrazione, di associazioni di tipo mafioso e di falso in bilancio")

1. REATI PRESUPPOSTO

Si riportano, di seguito, le rubriche di tutti i reati presi in considerazione dal D.Lgs. 231/01:

- *False comunicazioni sociali* (art. 2621 c.c. come sostituito dall'art. 9 della Legge 27 maggio 2015 n. 69);
- *Fatti di lieve entità* (art. 2621-*bis* c.c., aggiunto dall'art. 10 Legge 27 maggio 2015 n. 69);
- *False comunicazioni sociali delle società quotate* (art. 2622 c.c., come sostituito dall'art. 11 della Legge 27 maggio 2015 n. 69);
- *Falsità nelle relazioni o nelle comunicazioni delle società di revisione* (art. 2624, comma 2 c.c.);
- *Impedito controllo* (art. 2625, comma 2 c.c.);
- *Indebita restituzione dei conferimenti* (art. 2626 c.c.);
- *Illegale ripartizione di utili e riserve* (art. 2627 c.c.);
- *Illecite operazioni sulle azioni o quote sociali o della società controllante* (art. 2628 c.c.);
- *Operazioni in pregiudizio ai creditori* (art. 2629 c.c.);
- *Omessa comunicazione del conflitto di interessi* (art. 2629-*bis* c.c.)
- *Formazione fittizia del capitale sociale* (art. 2632 c.c.);
- *Indebita ripartizione dei beni sociali da parte dei liquidatori* (art. 2633 c.c.);
- *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 c.c.);
- *Corruzione tra privati* (art. 2635 c.c., aggiunto dall'art. 1, comma 77, lettera b) della Legge 6 novembre 2012 n. 190);
- *Istigazione alla corruzione tra privati* (art. 2635-*bis* c.c., aggiunto dall'art. 4, comma 1 D.Lgs. 15 marzo 2017 n. 38).

Si segnala che il reato di "*Falsità nelle relazioni o nelle comunicazioni delle società di revisione"* di cui all'art. 2624, comma 2 cod. civ. – incluso nell'elenco dei reati presupposto in materia societaria di cui sopra - è stato dapprima sostituito con D.Lgs. 11.4.2002 n. 61 e successivamente abrogato dall'art. 37, comma 34 del D.Lgs. 27.1.2010 n. 39 attuativo della direttiva 2006/43/CE, relativa alle revisioni legali dei conti annuali e dei conti consolidati, che modifica le direttive 78/660/CEE e 83/349/CEE, e che abroga la direttiva 84/253/CEE.
Conseguentemente, il reato previsto dall'art. 2624 c.c. è ora disciplinato dall'art. 27 cit. D.Lgs. 39/2010 che salvaguarda l'applicazione dei principi a suo tempo inclusi nell'art. 2624 c.c. ora abrogato.

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Sulla scorta della documentazione raccolta a riguardo della Società, nell'ambito:

- delle attività di rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nelle relazioni, nei bilanci e in altri documenti di impresa;

- delle attività o delle condotte tenute in relazione allo svolgimento dei controlli previsti dalla legge, dalle procedure contemplate dal sistema di controllo interno, dal Modello o dalle procedure per la sua attuazione, idonee a ostacolare i controlli sull'attività o sulla rappresentazione contabile dell'attività di impresa;

- delle situazioni o attività in potenziale conflitto di interessi e, in genere,

potenzialmente pregiudizievoli per i soci, i creditori e i terzi;

sono individuate, presso la Società quali operazioni a rischio nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui all'art. 25-*ter* del Decreto le ordinarie attività gestionali della Società riferibili alla tenuta della contabilità, alla redazione del bilancio ed alla *corporate governance*.

Inoltre, la Legge n. 190 del 6 novembre 2012 pubblicata in Gazzetta ufficiale del 13 novembre 2012 titolata "*Disposizioni per la prevenzione e la repressione della corruzione e l'illegalità nella pubblica amministrazione*" ha introdotto tra i reati presupposto del D.Lgs. 231/01 alla lettera s-bis dell'art. 25-ter il reato di "*Corruzione tra privati*" di cui all'art. 2635 co. 3 c.c.

A riguardo, l'art. 4, comma 1 del D.Lgs. 15 marzo 2017 n. 38 in materia di "*Attuazione della decisione quadro 2003/568/GAI del Consiglio, del 22 luglio 2003, relativa alla lotta contro la corruzione nel settore privato*", pubblicato in Gazzetta Ufficiale del 30 marzo 2017, n. 75, ha introdotto tra i reati presupposto anche il reato di "*Istigazione alla corruzione privata*" (art. 25-*ter*, lett. s-*bis*) di cui all'art. 2635-*bis* c.c. che punisce «*chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà…*».

Ai fini del D.Lgs. 231/01, vengono quindi a rilevanza i reati di corruzione tra privati e di istigazione alla corruzione privata esclusivamente dal lato attivo del soggetto corruttore.

In entrambe la fattispecie di reato sopra citate, la condotta rilevante ai fini della presente Parte Speciale consiste nella "*promessa o nella dazione di danaro o di altra utilità*" ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori di società terze.

Peraltro, la formulazione del comma 3 dell'art. 2635 c.c. nonché del comma 1 dell'art. 2635 *bis* c.c. non specifica a quale fine deve essere data o promessa l'utilità perché si configuri il reato, né se serve che sia compiuto od omesso un atto da parte del corrotto in violazione dei propri obblighi perché il corruttore sia punito.

Pare quindi consigliabile attenersi ai criteri più rigorosi possibili.

In questa ottica, vanno presidiati i processi che possono consentire da un lato la materializzazione in capo alla Società del beneficio derivante dall'accordo corruttivo, dall'altro la formazione della provvista di danaro necessaria all'esecuzione dell'attività corruttiva.

Va, altresì, impedito che vengano concesse consulenze o intermediazioni prive di causa ed al fine di mascherare dazioni illecite.

Da ultimo, la Legge 27 maggio 2015 n. 69 recante le "*Disposizioni in materia di delitti contro la Pubblica Amministrazione, di associazioni di tipo mafioso e di falso in bilancio*" ha apportato le seguenti novità in materia di reati societari:

- il reato di "*false comunicazioni sociali*" di cui all'art. 2621 c.c. – previsto come reato presupposto dall'art. 25-*ter*, comma 1, lettera a) D.Lgs. 231/01 – viene ora qualificato come delitto e non più come contravvenzione, con conseguente inasprimento, rispetto al passato, delle sanzioni pecuniarie previste a carico dell'ente;

- è stato introdotto il nuovo reato presupposto dei c.d. "*fatti di lieve entità*" di cui all'art. 2621 *bis* c.c. (art. 25-ter, comma 1, lettera a-bis D.Lgs. 231/01), che vanno valutati in considerazione delle dimensioni della società e delle modalità o degli effetti della condotta, ovvero se si tratta di società che non soddisfano i requisiti di assoggettabilità al fallimento o al concordato di cui al Regio Decreto 16 marzo 1942 n. 267 (Legge Fallimentare);

- il reato presupposto di "*false comunicazioni sociali in danno della società, dei soci o dei creditori" ex* art. 2622 c.c. (art. 25-*ter*, comma 1, lett. b) viene ora rubricato come "*false comunicazioni sociali delle società quotate*" di cui ne è

stato riformulato il testo.

Conseguentemente alla nuova formulazione dell'art. 2622 c.c., l'art. 25-*ter*, comma 1, lettera c) D.Lgs. 231/01 che prevedeva quale reato presupposto le "*false comunicazioni sociali in danno dei soci o dei creditori*" di cui all'art. 2622, comma 3 c.c., è stato abrogato.

Per quanto attiene alla valutazione da parte della Società in tema di reati societari, si ritiene quindi opportuno predisporre apposite procedure a riguardo:

i) della redazione del bilancio;
ii) della tenuta della contabilità;
iii) della gestione, archiviazione e conservazione delle informazioni;
iv) ai rapporti con il collegio sindacale e con il revisore dei conti;
v) alla gestione delle risorse finanziarie;
vi) ai rapporti con le autorità di vigilanza;
vii) del marketing ed omaggistica a clienti;
viii) della valutazione della clientela, stipula dei contratti e gestione delle condizioni economico – finanziarie (prezzi – sconti) definite nei contratti con i clienti;
ix) dell'incarico a consulenti ed intermediari.

3. PROCEDURE GENERALI

La presente sezione prevede l'espresso divieto a carico dei Destinatari del Modello di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate nel presente Allegato;

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

La presente sezione prevede, conseguentemente, l'espresso obbligo a carico dei Destinatari di conoscere e rispettare:

- i principi di *corporate governance* che rispecchiano le normative applicabili e le *best practices internazionali*;

- il sistema di controllo interno, le procedure aziendali, la documentazione e le disposizioni inerenti la struttura gerarchico – funzionale aziendale ed organizzativa della Società;

- le norme interne concernenti il sistema amministrativo, contabile, finanziario, di *reporting*;

- in generale, la normativa applicabile.

Nell'ambito dei suddetti comportamenti, è tassativamente imposto di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio d'esercizio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale, finanziaria della Società;

- 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 della Società stessa;

- astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false o non corrette, idonee a provocare una sensibile distorsione dei risultati economici/patrimoniali e finanziari conseguiti dalla Società;

- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche anche di vigilanza e di controllo, non frapponendo alcun ostacolo all'esercizio

delle funzioni di vigilanza da queste esercitate.

Per ciascuna delle operazioni di carattere significativo individuate nella presente sezione, sono previste specifiche procedure in forza delle quali:

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

b) non vi sia identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;

c) la Società ponga in essere attività specifica di formazione di base verso tutti i responsabili di funzione, affinché conoscano almeno le principali nozioni sul bilancio (norme di legge, sanzioni, principi contabili ecc.)

d) l'accesso ai dati della Società sia conforme al D.Lgs. n. 196 del 2003 e successive modifiche e integrazioni, anche regolamentari ed in generale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati); l'accesso e l'intervento sui dati della Società sia consentito esclusivamente alle persone autorizzate; sia garantita la riservatezza nella trasmissione delle informazioni;

e) i documenti riguardanti l'attività di impresa siano archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;

f) qualora il servizio di archiviazione e/o conservazione dei documenti sia svolto, per conto della Società, da un soggetto ad essa estraneo, il servizio deve essere regolato da un contratto nel quale si preveda, tra l'altro, che il soggetto che presta il servizio alla Società rispetti specifiche procedure di controllo idonee a

non permettere la modificazione successiva dei documenti archiviati, se non con apposita evidenza;

g) l'accesso ai documenti già archiviati, di cui alle due lettere precedenti, sia sempre motivato e consentito solo alle persone autorizzate in base alle norme interne, al Collegio Sindacale, al revisore dei conti ed all'Organismo di Vigilanza;

h) si tengano incontri periodici tra il collegio sindacale e l'Organismo di Vigilanza anche per verificare l'osservanza della disciplina prevista in tema di normativa societaria e *corporate governance*, nonché il rispetto dei comportamenti conseguenti da parte degli Amministratori, del management, dei dipendenti;

i) gli amministratori comunichino al Consiglio di Amministrazione, al Collegio Sindacale ed all'Organismo di Vigilanza, le cariche assunte o le partecipazioni di cui sono titolari, direttamente o indirettamente, in altre società o imprese, le quali, per la natura o la tipologia, possono lasciar ragionevolmente prevedere l'insorgere di conflitti di interesse;

j) la scelta di consulenti esterni avvenga sulla base di requisiti di professionalità, indipendenza e competenza e, in riferimento a essi, sia motivata la scelta;

k) non siano corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, agenti o a soggetti pubblici in misura non congrua rispetto alle prestazioni rese alla Società e non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;

l) eventuali sistemi di remunerazione premianti ai dipendenti e collaboratori rispondano a obiettivi realistici e coerenti con le mansioni e l'attività svolta e con le responsabilità affidate;

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

dell'Unione Europea.

Con riferimento ai reati di corruzione tra privati e di istigazione alla corruzione privata, è inoltre fatto espresso divieto di offrire o promettere denaro o altra utilità a soggetti privati al fine di cedere con maggiore facilità i servizi che la Società rende.

Inoltre, le procedure devono garantire una stratificazione nei poteri autorizzativi dei processi di offerta e vendita dei servizi ed una distinzione di ruoli nell'ambito dell'organizzazione tra responsabilità nella definizione del prezzo di offerta e delle condizioni e tempi di pagamento e concessione e definizione di scontistica o condizioni di favore; le stesse devono altresì individuare e definire criteri generali di formazione del prezzo dei servizi.

4. PRINCIPI E PROCEDURE SPECIFICHE

A) Redazione del bilancio e delle altre scritture contabili

La Società si adopera per disporre di un sistema amministrativo – contabile affidabile, al fine di rappresentare correttamente i fatti di gestione nell'interesse dei soci, dei creditori e dei terzi.

Le rilevazioni contabili devono pertanto basarsi su informazioni precise, esaustive, verificabili e riflettere la natura e la tipologia dell'operazione cui si riferiscono, nel rispetto dei vincoli esterni (disposizioni legislative e regolamentari e principi contabili), nonché delle politiche, dei piani e delle procedure interne: le stesse, inoltre, devono essere corredate della relativa documentazione di supporto, necessaria a consentire analisi e verifiche obiettive dei dati in esse contenuti.

Le suddette rilevazioni contabili devono:

- consentire la ricostruzione della situazione economica, patrimoniale e finanziaria della Società, sia per scopi interni (report), che nei rapporti con i terzi (bilanci, documenti informativi, etc.);
- fornire gli strumenti per identificare, prevenire e gestire, nei limiti del possibile,

rischi di natura finanziaria o frodi a danno dei creditori o dei terzi potenzialmente interessati ad entrare in contatto con la Società;

- permettere l'effettuazione di controlli volti a garantire la salvaguardia del valore delle attività e la protezione dalle perdite.

Il personale delle funzioni interessate è tenuto ad operare affinché i fatti di gestione siano rappresentati correttamente e tempestivamente, in modo che il sistema amministrativo–contabile possa conseguire tutte le finalità sopra descritte.

La Società, nello svolgimento dell'attività di formazione del bilancio e delle altre comunicazioni sociali, si ispira ai seguenti principi e criteri operativi:

- l'adozione di procedure contabili costantemente aggiornate che prevedano una chiara elencazione dei dati e delle notizie che ciascuna funzione aziendale deve fornire alla funzione che cura la predisposizione del bilancio e dei documenti contabili, con relativa tempistica di consegna;

- la trasmissione dei dati e delle informazioni alla funzione responsabile deve avvenire attraverso un supporto che consenta di tenere tracciati i vari passaggi: copia della trasmissione deve essere conservata ed archiviata, a cura delle funzioni coinvolte;

- i soggetti che forniscono i dati alla funzione incaricata dell'amministrazione e della finanza e/o ad eventuali soggetti esterni che li affianchino nell'attività, devono essere in grado di attestare la veridicità, la completezza e la coerenza delle informazioni trasmesse, mediante esplicita dichiarazione debitamente sottoscritta, ed all'occorrenza devono fornire le relative evidenze documentali;

- qualora siano formulate ingiustificate richieste di variazione dei criteri di rilevazione, registrazione e rappresentazione contabile, chi ne sia a conoscenza informi senza indugio l'Organismo di Vigilanza;

- la bozza di bilancio e gli altri documenti contabili siano messi a disposizione degli Amministratori, dei Sindaci e del revisore dei conti con ragionevole

anticipo rispetto alla riunione dell'Organo di Amministrazione per l'approvazione dello stesso.

B) Tenuta della contabilità

Ogni operazione aziendale che si riflette sul sistema contabile, inclusa la mera attività di inserimento dei dati, deve avvenire sulla scorta di adeguata evidenza documentale.

Si considera adeguato ogni valido ed utile supporto documentale atto a fornire tutti gli elementi, dati ed informazioni necessari alla puntuale ricostruzione, all'occorrenza, dell'operazione e dei motivi che le hanno dato luogo.

Il supporto documentale deve essere adeguato alla complessità dell'operazione e deve consentire un agevole controllo.

Le movimentazioni finanziarie attive e passive della Società devono sempre essere riconducibili ad eventi certi, documentati e strettamente inerenti.

C) Gestione, documentazione, archiviazione e conservazione delle informazioni

Le procedure devono prevedere che:

- i documenti riguardanti la formazione delle decisioni che governano le operazioni delle attività sensibili indicate nella presente parte speciale, nonché quelli che danno attuazione alle decisioni, siano archiviati e conservati a cura della funzione competente per l'operazione;
- l'accesso ai documenti già archiviati sia consentito solo alle persone autorizzate in base alle procedure operative aziendali, al collegio sindacale, al revisore dei conti ed all'Organismo di Vigilanza;
- chi fornisce o riceve informazioni sulla Società o sulle sue attività sia tenuto a garantirne la sicurezza e la completezza;
- la funzione alla quale sia legittimamente richiesta un'informazione, la fornisca in tempi ragionevoli, attestando, ove possibile, la completezza e la veridicità

delle informazioni rese o indicando i soggetti che possono fornire tale attestazione;

- la trasmissione delle informazioni nell'ambito della Società sia consentita esclusivamente alle persone autorizzate e avvenga solo attraverso mezzi tecnici che garantiscano la sicurezza della trasmissione e il rispetto del principio di riservatezza delle informazioni.

D) Rapporti con il Collegio Sindacale e con il revisore dei conti

Le procedure prevedono che:

- per ciascuna funzione sia individuato un responsabile della raccolta e dell'elaborazione delle informazioni richieste e trasmesse al collegio sindacale ed al revisore dei conti;
- il responsabile della funzione a cui è richiesta un'informazione dal collegio sindacale o dal revisore dei conti verifichi la completezza, inerenza e correttezza della documentazione trasmessa;
- le richieste e le trasmissioni di dati e informazioni, nonché ogni rilievo, comunicazione o valutazione espressa dal collegio sindacale e dal revisore dei conti, siano documentate e conservate a cura del responsabile di funzione;
- tutti i documenti relativi ad operazioni all'ordine del giorno delle riunioni dell'assemblea o del Consiglio di Amministrazione o, comunque, relativi a operazioni sulle quali il Collegio Sindacale debba esprimere parere siano messi a disposizione di quest'ultimo con ragionevole anticipo rispetto alla data della riunione;
- sia garantito al revisore dei conti il libero accesso alla contabilità aziendale per un corretto svolgimento dell'incarico.

E) Gestione delle risorse finanziarie

La procedura deve prevedere quanto segue:

a) non vi sia identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;

b) siano stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la fissazione di soglie quantitative coerenti alle competenze gestionali ed alle responsabilità organizzative affidate alle singole persone;

c) il superamento dei limiti di cui al punto precedente possa avvenire solo nel rispetto delle vigenti procedure di autorizzazione e previa adeguata motivazione;

d) le operazioni che comportano utilizzazione o impiego di risorse economiche o finanziarie debbano avere una causale espressa ed essere documentate e registrate in conformità ai principi di correttezza professionale e contabile. Il processo decisionale deve essere verificabile;

e) l'impiego di risorse finanziarie sia motivato dal soggetto richiedente, che ne attesta la congruità:
   i) in caso di operazioni ordinarie, se comprese entro la soglia quantitativa stabilita, la motivazione può essere limitata al riferimento alla classe o tipologia di spesa alla quale appartiene l'operazione;
   ii) in caso di operazioni diverse dalle ordinarie o eccedenti la soglia quantitativa stabilita, la motivazione deve essere analitica.

F) <u>Rapporti con le autorità di vigilanza</u>

Nella predisposizione di comunicazioni alle Autorità pubbliche di Vigilanza e nella gestione dei rapporti con le stesse, la Società pone particolare attenzione al rispetto:

- delle disposizioni di legge e di regolamento concernenti le comunicazioni, periodiche e non, da inviare a tali Autorità;

- degli obblighi di trasmissione alle Autorità suddette dei dati e documenti previsti dalle norme in vigore, ovvero specificamente richiesti dalle predetta Autorità (ad esempio bilanci, verbali delle riunioni degli organi societari);

- degli obblighi di collaborazione da fornire nel corso di eventuali accertamenti ispettivi.

Inoltre, la Società adotta idonee procedure per la gestione ed il controllo delle comunicazioni alle Autorità pubbliche di Vigilanza.

Le procedure da osservare, per garantire il rispetto di quanto espresso al precedente punto, devono essere conformi ai seguenti criteri:

1) deve essere data attuazione a tutti gli interventi di natura organizzativo – contabile necessari a garantire che il processo di acquisizione ed elaborazione di dati ed informazioni assicuri la corretta e completa predisposizione delle comunicazioni ed il loro puntuale invio alle Autorità pubbliche di Vigilanza, secondo le modalità ed i tempi previsti dalla normativa di settore;

2) deve essere data adeguata evidenza delle procedure seguite in attuazione di quanto richiesto al precedente punto, con particolare riferimento all'individuazione dei responsabili che hanno proceduto alla raccolta ed all'elaborazione dei dati e delle informazioni ivi previste;

3) deve essere assicurata, in caso di accertamenti ispettivi svolti dalle Autorità in questione, una adeguata e trasparente collaborazione da parte delle unità aziendali competenti e di tutti i dipendenti;

4) per il caso di ispezioni disposte dalle Autorità, si fa integrale richiamo alla relativa procedura riportata nell'Allegato A.

G) <u>Procedure a presidio del rischio di commissione dei reati di corruzione tra privati e di istigazione alla corruzione privata</u>

Vanno utilizzate anche nei rapporti con i privati le procedure:

- relative alla gestione delle risorse finanziarie di cui alla lettera E) del presente paragrafo;

- di gestione del marketing ed eventuale omaggistica a clienti posta a presidio dei reati contro la pubblica amministrazione (già trattate nell'Allegato A);

- sulla valutazione della clientela, stipula dei contratti e gestione delle condizioni economico–finanziarie (prezzi–sconti) definite nei contratti con i clienti indicata nell'Allegato J relativo alle procedure da adottare al fine di evitare la commissione di reati transnazionali;

- sul conferimento dell'incarico a consulenti ed intermediari.

Le dette procedure – con l'esclusione di quella sulla gestione delle risorse finanziarie già indicata nel presente Allegato – si trascrivono di seguito:

(I) <u>Marketing ed omaggistica ai clienti</u>

a) E' fatto divieto di distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale, vale a dire, ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale.

b) In particolare, è vietata qualsiasi forma di regalo ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, i sindaci o i liquidatori di aziende fornitrici o clienti, o a loro familiari, che possa influenzarne la discrezionalità o l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società.

c) Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore, o perché volti a promuovere la *brand image* della Società.

d) Tutti i regali offerti eccedenti il modico valore devono essere documentati in modo idoneo, per consentire all'Organismo di Vigilanza di effettuare verifiche al riguardo.

e) Sono ammesse in via episodica e per motivate ragioni commerciali iniziative promozionali di maggior valore come convention aziendali, meeting o incontri anche di più giorni volte a promuovere il brand della Società presso i maggiori clienti e fornitori; tali iniziative non dovranno tuttavia essere finalizzate ad acquisire trattamenti di favore da parte di un soggetto specifico, ma dovranno rivolgersi ad un congruo numero di destinatari ed essere sottese a mere ragioni di promozione commerciale. Di tali iniziative deve essere data informativa all'Organismo di Vigilanza.

f) Qualora la Società sponsorizzi o comunque contribuisca economicamente alla realizzazione di eventi indetti da aziende fornitrici o clienti, l'importo sponsorizzato od erogato dalla Società dovrà mantenersi entro i limiti del modico valore.

g) Il responsabile della funzione si assicurerà che l'erogazione venga effettuata in favore dell'ente organizzatore e non di soggetti persone fisiche appartenenti allo stesso.

h) Per ogni sponsorizzazione effettuata dalla Società deve essere redatto un breve resoconto scritto contenente quantomeno il nominativo dell'ente.

(II) <u>Valutazione della clientela, stipula dei contratti e gestione delle condizioni economico–finanziarie (prezzi–sconti) definite nei contratti con i clienti</u>

La procedura deve prevedere quanto segue:

a) ogni rapporto di cessione di beni o servizi sia disciplinato da contratto scritto, sottoscritto esclusivamente dal soggetto dotato di idonei poteri secondo il sistema di deleghe e procure vigente, nel quale sia chiaramente prestabilito il prezzo del bene o della prestazione da effettuare o i criteri per determinarlo;

b) siano previste modalità e limiti per la concessione di sconti commerciali rispetto al listino prezzi della Società, anche tenendo conto delle oscillazioni dei prezzi di mercato;

c) non vi sia identità soggettiva fra coloro che propongono, coloro che autorizzano la concessione del credito al cliente, coloro che devono dare evidenza contabile dell'operazione e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;

d) siano stabiliti limiti alla concessione di credito alla clientela da parte del responsabile della funzione, mediante la fissazione di soglie quantitative coerenti alle competenze gestionali ed alle responsabilità organizzative affidate; le operazioni che superino la soglia quantitativa siano preventivamente valutate e approvate dall'organismo superiore a quello che cura la funzione;

e) l'affidamento della clientela sia sempre subordinato a una valutazione generale della affidabilità finanziaria e della consistenza patrimoniale del cliente, svolta attraverso la raccolta di informazioni da fonti interne (struttura e organizzazione della Società, protesti, visure ipotecarie e catastali, ecc.) e da fonti esterne, ricorrendo a banche dati ufficiali aggiornate. In caso di rilascio di garanzie personali da parte di terzi a favore dei clienti, siano effettuati accertamenti idonei sul soggetto garante, individuando indici di rischio o anomalia;

f) le operazioni di affidamento della clientela siano documentate a cura della funzione proponente e, una volta approvate, siano registrate nell'anagrafica clienti in conformità ai principi di correttezza professionale;

g) siano effettuati controlli periodici da parte del responsabile della funzione di controllo crediti di sede sugli affidamenti in essere presso la Società, anche in relazione all'esposizione aggiornata del cliente;

h) qualora l'esposizione del cliente superi i parametri indicati dalle procedure interne, la fornitura sia bloccata, salva diversa valutazione responsabile della funzione di controllo crediti, opportunamente motivata;

i) chiunque ne sia a conoscenza segnali immediatamente all'Organismo di Vigilanza oppure al proprio superiore gerarchico, che riferirà all'Organismo di Vigilanza, eventuali anomalie nelle prestazioni dovute al cliente, discordanze significative o ripetute tra materiale ceduto o servizio prestato rispetto a quanto concordato o particolari richieste avanzate dal cliente alla Società.

(III) Incarico a consulenti ed intermediari

La procedura deve necessariamente prevedere quanto segue:

a) sia formalizzato il processo di selezione e valutazione di consulenti ed intermediari, nonché della gestione del rapporto con i medesimi;

b) per le fasi di selezione e di valutazione dei consulenti e degli intermediari siano individuati idonei criteri e modalità di scelta dei medesimi che garantiscano un processo comparativo degli offerenti. Qualora il processo comparativo non sia possibile o sia giudicato non necessario, la funzione competente lo segnali al livello gerarchico superiore, dando adeguata motivazione;

c) siano stabilite idonee modalità di raccolta e conservazione della documentazione relativa al processo di selezione, valutazione e gestione di intermediari e consulenti;

d) ogni rapporto con consulenti e intermediari sia disciplinato da contratto scritto, sottoscritto esclusivamente dal soggetto dotato di idonei poteri secondo il sistema di deleghe e procure vigente, nel quale sia chiaramente prestabilito il prezzo della prestazione da ricevere o i criteri per determinarlo;

e) non siano corrisposti compensi, provvigioni o commissioni a consulenti o intermediari in misura non congrua rispetto alle prestazioni rese alla Società e non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;

f) non siano effettuate prestazioni in favore di consulenti o intermediari o terzi in genere che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi, o in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale

g) ove l'intermediario o il consulente abbiano sede in Paesi c.d. *black list* di cui al Decreto Ministeriale 4 maggio 1999 "*Individuazione di Stati e territori aventi un regime fiscale privilegiato*" e ss.mm.ii. ed al Decreto del Ministero dell'Economia e delle Finanze 21 novembre 2001 "*Individuazione degli Stati o territori a regime fiscale privilegiato di cui all'art. 127-bis, comma 4, del testo unico delle imposte sui redditi (cd. "black list") - (BLACK LIST 2)*" e ss.mm.ii, ne venga data pronta informativa all'Organismo di Vigilanza;

h) chiunque ne sia a conoscenza, segnali immediatamente all'Organismo di Vigilanza oppure al proprio superiore gerarchico, che riferirà all'Organismo di Vigilanza, eventuali anomalie nelle prestazioni dovute dal consulente o dall'intermediario, discordanze significative o ripetute tra materiale o servizio ricevuto rispetto a quanto concordato o particolari richieste avanzate dal medesimo alla Società.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nel presente Allegato.

Il presente Allegato e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale, al fine di garantire il raggiungimento delle finalità del Modello.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO D

DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO

(Art. 25-quater D.Lgs. 231/01)

(Articolo inserito dall'art. 3 della Legge 14 gennaio 2003 n. 7)

1. REATI PRESUPPOSTO

L'art. 25 *quater* del D.Lgs. 231/02 prende in considerazione i delitti aventi finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali ed i delitti posti in essere in violazione di quanto previsto dall'art. 2 della Convenzione internazionale per la repressione del finanziamento al terrorismo fatta a New York il 9 dicembre 1999.

All'interno di tali fattispecie si possono includere i seguenti reati:

- *Associazioni sovversive* (art. 270 c.p.)
- *Associazione con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico* (Art. 270 *bis* 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* c.p.);
- *Sottrazione di beni o denaro sottoposti a sequestro* (Art. 270 *quinquies.2* c.p.);
- *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* c.p.);

- *Sequestro di persona a scopo di terrorismo o di eversione* (Art. 289 *bis* c.p.);
- *Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo del Titolo I, Libro secondo del codice penale* (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 Legge 10 maggio 1976, n. 342 in materia di "*Repressione di delitti contro la sicurezza della navigazione aerea*")
- *Danneggiamento delle installazioni a terra* (art. 2 cit. Legge n. 342/1976)
- *Sanzioni previste dall'art. 3 della Legge 28 dicembre 1989, n. 422 di* "*Ratifica ed esecuzione della convenzione per la repressione dei reati diretti contro la sicurezza della navigazione marittima, con protocollo per la repressione dei reati diretti contro la sicurezza delle installazioni fisse sulla piattaforma continentale, firmata a Roma il 10 marzo 1988, e disposizioni penali in materia di delitti contro la sicurezza della navigazione marittima e delle installazioni fisse sulla piattaforma continentale*"
- *Pentimento operoso* di cui all'art. 5 del D.L. 15 dicembre 1979, n. 625 convertito, con modificazioni, in Legge 6 febbraio 1980, n. 15 in materia di "*Misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica*" – c.d. legge "*Cossiga–Antiterrorismo*")
- *Reati previsti dall'art. 2 della* "*Convenzione Internazionale per la Repressione del Finanziamento del Terrorismo*", fatta a New York il 9 dicembre 1999

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

La Società non intrattiene rapporti con paesi a rischio terroristico e, pertanto, non si ravvisano rischi specifici con riferimento alla presente Parte Speciale.

Ad ogni buon conto, la Società provvederà quanto prima alla nomina di un "*Responsabile Addetto alle Segnalazioni alla Pubblica Autorità di Sicurezza*",

incaricato di ricevere (e conseguentemente inoltrare alle competenti autorità) eventuali segnalazioni da parte dei dipendenti aziendali in merito a persone in forza presso la Società ovvero prodotti di stampa o di comunicazione anche informatica per le quali si possa sospettare il collegamento con il terrorismo nazionale e/o internazionale.

A tal riguardo, la Società garantirà - compatibilmente con le disposizioni della vigente normativa in materia - la massima riservatezza sia per quanto concerne l'identità del soggetto che ha effettuato la segnalazione, sia in ordine al contenuto delle comunicazioni stesse.

Sino al momento della nomina, le funzioni di Responsabile Addetto alle Segnalazioni alla Pubblica Autorità di Sicurezza saranno svolte dal Responsabile delle Risorse Umane.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO E

PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI

(Art. 25-quater.1)

(Articolo inserito dall'art. 3 della Legge 9 gennaio 2006 n. 7)

1. REATO PRESUPPOSTO

Si riporta, nel seguito, la fattispecie di delitto prevista dall'art. 25-*quater.1* del D.Lgs. 231/01 come reato presupposto:

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

Detto reato è stato introdotto con Legge 9 gennaio 2006 n. 7, contenente disposizioni in materia di prevenzione e divieto delle pratiche di infibulazione.

Data la specificità del delitto in questione, la norma è necessariamente rivolta a quegli enti (quali ad esempio le strutture sanitarie, le organizzazioni di volontariato, ecc.) che svolgono attività natura medica e sanitaria, potendosi rendere responsabili della realizzazione, al loro interno, di pratiche mutilative vietate dalla legge.

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Sulla scorta della documentazione raccolta e dell'analisi dei processi correlati allo svolgimento della propria attività, emerge che la Società non svolge attività che prevede la prestazione di servizi di natura medico-sanitaria nei confronti di soggetti terzi, né intrattiene rapporti con enti che operano in tale settore o che comunque, pratichino trattamenti chirurgici e/o sanitari in contrasto con la vigente normativa in materia.

Si ritiene, pertanto, che non vi siano ravvisabili rischi specifici con riferimento al reato trattato nel presente Allegato.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO F

DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE

(Art. 25-quinquies)

(Articolo inserito dall'art. 5 della Legge 11 agosto 2003 n. 228)

1. REATI PRESUPPOSTO

Si riportano, di seguito, le rubriche dei reati presi in considerazione dall'art. 25-*quinquies* D.Lgs. 231/01:

- *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., 1° e 2° comma);
- *Detenzione di materiale pornografico* (art. 600-*quater* c.p.);
- *Pornografia virtuale (art*. 600-*quater.1* c.p.);
- *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* c.p.);
- *Adescamento di minorenni (art*. 609-*undecies* c.p.).

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

La Legge n. 38/2006 contenente le "*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo internet*" ha comportato una sostanziale modifica dell'ambito di applicazione dei delitti di prostituzione minorile, pornografia minorile e detenzione di materiale pornografico (delitti previsti e puniti dagli artt. 600-*bis*, 600-*ter* e 600-*quater* c.p.) - già rilevanti ai fini della responsabilità amministrativa degli enti – includendo, tra le fattispecie di reato presupposto, anche le ipotesi in cui tali illeciti vengano commessi mediante

l'utilizzo di materiale pornografico raffigurante immagini virtuali di minori di anni diciotto o parti di esse (c.d. pedopornografia virtuale) potenzialmente reperibili e/o comunque diffondibili attraverso gli ordinari canali di comunicazione telematica (*internet*, posta elettronica, etc.).

La disciplina dei reati presupposto in esame è stata, inoltre, oggetto di ulteriori e successive modifiche ad opera di successivi interventi normativi, tra cui si segnalano: la Legge n. 108/2010; la Legge n. 172/2012 recante la "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale fatta a Lanzarote il 25 ottobre 2007, nonché norme di adeguamento dell'ordinamento interno*", che ha introdotto nel codice penale il delitto di "*adescamento di minorenni*" previsto e punito dall'art. 609-*undecies* (a sua volta introdotto nel novero dei reati presupposto previsti dall'art. 25-*quinquies* del D.Lgs. 231/01 dal D.Lgs. n. 39/2014) e il D.Lgs. n. 24/2014, che ha modificato le fattispecie di reato di cui agli artt. 600 e 601 c.p.

Da, ultimo, il Decreto Legge 13 agosto 2011, n. 138, conv. con modif. in Legge 14 settembre 2011, n. 148 "*Ulteriori misure urgenti per la stabilizzazione finanziaria e per lo sviluppo (MANOVRA BIS)*" ha introdotto nell'elenco dei reati presupposto il reato di "*Intermediazione illecita e sfruttamento del lavoro*" disciplinato dall'art. 603-*bis* c.p. (norma recentemente oggetto di modifica ad opera dell'art. 1, comma 1, della Legge 29 ottobre 2016, n. 199 "*Disposizioni in materia di contrasto ai fenomeni del lavoro nero, dello sfruttamento del lavoro in agricoltura e di riallineamento retributivo nel settore agricolo*") che punisce chiunque, con ovvero senza violenza o minaccia:

a) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;
b) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno».

Ai fini della configurabilità del reato sopra descritto, costituisce indice di

sfruttamento:

1) 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;
2) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
3) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
4) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

Benché la Società non intrattenga rapporti con soggetti terzi che hanno sede in Paesi che non garantiscono un'adeguata protezione dei diritti individuali ed ove è, purtroppo, diffusa la piaga della pornografia anche minorile ovvero dello sfruttamento del lavoro, si è comunque ritenuto opportuno – anche in considerazione del fatto che alcuni dei reati previsti dalla presente sezione speciale si prestano a poter essere commessi mediante l'utilizzo degli ordinari strumenti informatici messi a disposizione da parte della Società in favore dei propri lavoratori per lo svolgimento delle relative mansioni - individuare ed adottare specifiche misure e procedure finalizzate ad eliminare il rischio di commissione dei reati stessi da parte del personale aziendale, ovvero da parte dei soggetti che comunque rappresentano, amministrano e dirigono la Società.

D'altra parte la Società, in occasione dello svolgimento della propria attività, entra in contatto con soggetti estranei all'organizzazione aziendale, che appartengono a molteplici e differenti realtà professionali – senza garanzia alcuna che da parte di detti soggetti terzi vi sia una correlativa *policy* finalizzata ad evitare la commissione dei reati previsti dalla presente sezione - con evidenti potenziali problematiche in termini di tutela della Società stessa contro il rischio di trovarsi, anche solo indirettamente, coinvolta in episodi rientranti nelle fattispecie previste dall'art. 25-*quinquies* del D.Lgs. 231/01.

3. PROCEDURE SPECIFICHE

Sulla scorta della documentazione raccolta e dell'analisi dei processi della Società, sono state individuate ed adottate le seguenti misure e procedure ritenute idonee a eliminare il rischio di commissione dei reati di cui si tratta:

a) in primo luogo la Società vieta espressamente l'introduzione ed in particolare l'uso all'interno del proprio sito produttivo, da parte dei lavoratori, di personal computer, *tablet*, telefoni cellulari o altre apparecchiature personali che siano in grado di connettersi alla rete informatica globale esterna (*internet*);

b) in secondo luogo, la Società ha individuato ed adottato tutte le misure di protezione della propria rete informatica ritenute più idonee ad evitare il rischio di eventuali aggressioni esterne ovvero il rischio di introduzione, all'interno della rete aziendale stessa, di dati informatici e *files* aventi contenuto non autorizzato.

   A tal riguardo, la Società ha provveduto a formare ed informare i propri dipendenti circa le modalità di corretto utilizzo degli strumenti informatici che ciascun lavoratore ha ricevuto dall'Azienda, per la cui la dettagliata disamina delle relative procedure dalla stessa adottate, si rimanda a quanto previsto e disciplinato nell'Allegato K che tratta i "*Delitti informatici e trattamento illecito di dati*" del presente Modello Organizzativo;

c) inoltre, la navigazione su *internet* per scopo personale utilizzando gli strumenti informatici concessi in uso da parte della Società (sia per il tramite di connessione privata che attraverso la connessione telematica aziendale), è vietata dalle norme contenute nel regolamento adottato dalla Società (documento che è stato portato a conoscenza di tutti i dipendenti mediante consegna agli stessi di una copia del regolamento aziendale stesso, nonché mediante affissione del regolamento stesso nei locali aziendali), fatto salvo il caso in cui si disponga di espressa autorizzazione da parte della Società;

d) anche l'utilizzo della posta elettronica aziendale è consentito per esclusive finalità di produzione.

Anche in questo caso, la corrispondenza informatica sia in entrata, sia in uscita da/per ciascun *account* personale assegnato dalla Società a ciascun lavoratore è soggetta ad un sistema di monitoraggio e filtraggio come meglio dettagliato nell'Allegato K in tema di "*Delitti informatici e trattamento illecito di dati*".

Inoltre, al fine di ridurre ulteriormente il rischio di veicolazione all'interno della rete aziendale di materiale informatico idoneo ai fini della commissione dei reati previsti nella presente sezione, la Società ha adottato un sistema che prevede la limitazione della dimensione degli allegati che possono essere inoltrati e/o ricevuti, bloccandone conseguentemente la trasmissione di quelli aventi dimensione superiore a quella stabilita.

Attualmente tale limitazione è impostata, compatibilmente con il regolare svolgimento dell'attività aziendale, come segue: 10 Mb per la posta in uscita e 30 Mb per la posta in entrata;

e) infine, a garanzia dell'osservanza da parte del proprio personale delle norme interne che disciplinano l'utilizzo degli strumenti informatici aziendali, la Società si riserva di effettuare ispezioni, anche personali e non programmate, sulle macchine e sugli elaboratori concessi in uso ai propri dipendenti, aventi ad oggetto la verifica delle macchine stesse al fine di individuare l'eventuale presenza di programmi non licenziati, ovvero regolarmente detenuti con licenza ma mai autorizzati dall'azienda, ovvero individuare l'eventuale accesso a siti internet non consentiti e tutto quanto può comunque mettere in pericolo la sicurezza dell'azienda.

   L'eventuale ritrovamento di programmi non autorizzati verrà ritenuto dalla Società quale fatto grave in grado di minacciare il patrimonio aziendale sanzionato secondo quanto descritto nella sezione dedicata al "*Sistema Disciplinare*" contenuta nella Parte Generale del Modello.

   A tal riguardo, la Società ha preventivamente informato tutti i lavoratori della possibilità da parte dell'azienda di svolgere le suddette ispezioni, che verranno in ogni caso effettuate con le specifiche modalità previste dal Garante della Privacy con le "*Linee Guida del Garante per posta elettronica e internet*" - Registro delle deliberazioni n. 13 del 1° marzo 2007, pubblicate in Gazzetta

Ufficiale n. 58 del 10 marzo 2007.

Sul fronte, invece, delle misure contro il rischio di commissione dei reati connessi alla schiavitù ed allo sfruttamento del lavoro – pure presi in considerazione dall'art. 25-*quinquies* del D.Lgs. 231/01 quali reati presupposto – si segnala in primo luogo che la Società si prefigge di conformare i rapporti con il proprio personale e tra i lavoratori stessi (ed in special modo i rapporti fra le maestranze e la classe dirigente) ai canoni del più assoluto rispetto delle norme e del buon vivere civile, alla cortesia ed alla salvaguarda della dignità del lavoratore, vietando qualsiasi forma di discriminazione tra i dipendenti, che sia essa correlata al sesso, alla razza, alla lingua, alla religione, alle opinioni politiche, ovvero alle condizioni personali e sociali del lavoratore, così come le molestie sessuali ed il *mobbing*.

A tal riguardo, la Società ha predisposto ed adottato il proprio Codice Etico, nel quale i rapporti con i propri dipendenti e nei confronti degli altri soggetti che, direttamente o indirettamente, stabilmente o temporaneamente, instaurano rapporti e relazioni con la Società stessa od operano per perseguirne gli obiettivi, vengono ispirati ai principi di onestà, correttezza, integrità, trasparenza e reciproco rispetto, anche in armonia con la legislazione vigente a tutela delle condizioni di lavoro.

In ottemperanza a quanto sopra, la Società pertanto:

a) rifiuta ogni forma di sfruttamento dei lavoratori ed in particolar modo, lo sfruttamento del lavoro minorile, nonché lo svolgimento di qualsiasi attività che possa mettere a repentaglio od interferire con l'educazione dei bambini, con la loro salute ed il loro sviluppo fisico, mentale, morale e sociale;

b) impiega lavoratori immigrati solo se muniti di regolare permesso di lavoro;

c) provvede a mettere in atto tutte le misure ritenute più idonee che garantiscano l'incolumità fisica dei propri dipendenti e richiede al proprio personale che la conduzione delle proprie attività si fondi sulla prevenzione dei rischi e sulla tutela della salute e della sicurezza di sé stessi, dei colleghi e dei terzi;

d) vigila affinché:

(i) i rapporti tra i dipendenti siano improntati ai principi di una civile convivenza e si svolgano nel rispetto reciproco dei diritti e della libertà delle persone;

(ii) i rapporti tra i diversi livelli di responsabilità all'interno del proprio organico siano improntati alla più assoluta lealtà e correttezza;

(iii) i responsabili delle unità organizzative esercitino i poteri connessi alla delega ricevuta con obiettività ed equilibrio, curando adeguatamente il benessere e la crescita professionale dei propri collaboratori;

(iv) i dipendenti prestino la massima collaborazione verso i loro responsabili, osservando con diligenza le disposizioni di lavoro loro impartite;

(v) i soggetti che la rappresentano avanti ai terzi informino adeguatamente questi ultimi circa gli obblighi imposti dal proprio Codice Etico, esigendone il rispetto da parte di tali soggetti ed adottando tutte le idonee ed opportune iniziative in caso di mancato adempimento, rifiutandosi così di intraprendere rapporti d'affari con soggetti di non provata o, comunque, sospetta integrità morale.

Inoltre, la Società osserva con la più assoluta scrupolosità, la disciplina vigente in materia di lavoro, regolando in conformità della stessa la gestione del proprio personale aziendale. A tal riguardo:

a) ciascun lavoratore è assunto con regolare contratto sottoscritto e comunicato ai competenti enti;

b) il trattamento retributivo riconosciuto a ciascun lavoratore viene parametrato agli standard indicati dal CCNL applicato dalla Società;

c) ogni singolo rapporto di lavoro in essere con i propri dipendenti, viene disciplinato dalle norme di legge vigenti e da quelle contenute nel CCNL applicato e gestito in conformità delle stesse dall'Ufficio delle Risorse Umane che fa vertice nella persona del proprio Direttore.

Annualmente la Società, in occasione dell'approvazione del Bilancio, provvede:

(i) a verificare la regolarità dei rapporti instaurati nel corso dell'anno e la congruità della retribuzione riconosciuta a ciascun lavoratore rispetto ai canoni stabiliti nel CCNL;

(ii) ad esaminare gli episodi che sono stati segnalati, nel corso dell'anno, al Responsabile delle Risorse Umane e da questo contestati ed eventualmente sanzionati disciplinarmente, che hanno avuto ad oggetto la violazione da parte dei dipendenti delle regole di buon comportamento nei confronti dei lavoratori, individuando le misure e le procedure ritenute più idonee da implementare, volte a scoraggiare il verificarsi di ulteriori episodi.

A tal fine, il Responsabile delle Risorse Umane riferisce all'Amministratore Unico in merito ai punti sopra indicati e, ove occorra, anche all'Organismo di Vigilanza.

4. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nel presente Allegato.

Il presente Allegato e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale del Modello, al fine di garantire il raggiungimento delle finalità dallo stesso preposte.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO G

ABUSI DI MERCATO

(Art. 25-sexies)

(Articolo inserito dall'art. 9, comma 3 della Legge 18 aprile 2005 n. 62)

1. REATI PRESUPPOSTO

Si riportano, di seguito, le rubriche dei reati di abuso del mercato presi in considerazione dal D.Lgs. 231/01:

- *Abuso di informazioni privilegiate* (art. 184 D.Lgs. 24 febbraio 1998 n. 58 - TUF);
- *Manipolazione del mercato* (art. 185 TUF).

Il TUF, come modificato dalla legge n. 62 del 2005, prevede all'art. 187-*quinquies* la responsabilità amministrativa degli enti per gli illeciti amministrativi relativi agli abusi di mercato, di seguito elencati:

- *Abuso di informazioni privilegiate* (art. 187-*bis* TUF);
- *Manipolazione del mercato* (art. 187-*ter* TUF).

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

La Società non svolge attività inerente agli strumenti finanziari di cui all'art. 180 lett. a) e lett. b) del TUF.

Si ritiene, quindi, che non siano ravvisabili rischi specifici con riferimento ai reati trattati nel presente Allegato.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO H

REATI DI OMICIDIO COLPOSO E LESIONI GRAVI O GRAVISSIME COMMESSI CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

(Art. 25-septies)

(Articolo inserito dall'art. 9 della Legge 3 agosto 2007 n. 123 e successivamente sostituito dall'art. 300 del D.Lgs. 9 aprile 2008 n. 81)

1. REATI PRESUPPOSTO

Si riportano, di seguito, le rubriche dei reati presi in considerazione dall'art. 25-*septies* del D.Lgs. 231/01 ove gli stessi vengono commessi con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro:

- *Omicidio colposo (art. 589 c.p.);*
- *Lesioni personali colpose (art. 590, terzo comma, c.p.)*

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Sulla scorta della documentazione raccolta e dell'analisi dei processi della Società, nell'ambito:

- di tutti i settori di attività della Società e delle sue unità produttive;
- di tutte le attività e delle unità produttive alle quali siano addetti sia lavoratori dipendenti della Società sia i lavoratori dipendenti di imprese esterne e/o lavoratori autonomi, a cui la Società affida lavori in appalto e/o in subappalto;

sono individuati i fattori di rischio riportati nel Documento di Valutazione dei Rischi predisposto dalla Società in ottemperanza alle disposizioni previste dal D.Lgs. 9 aprile

2008 n. 81 attuativo dell'articolo 1 della Legge 3 agosto 2007, n. 123, in materia di "*Tutela della salute e della sicurezza nei luoghi di lavoro*", nonché nella *Check List* allegata al Modello, entrambi consegnati all'Organismo di Vigilanza che ha il compito di provvedere agli aggiornamenti relativi.

Si rileva, peraltro, che la Società non presenta elementi di criticità ulteriori rispetto a quelli ineliminabili connessi all'ordinaria attività imprenditoriale che costituisce l'oggetto sociale.

Vista l'estrema sensibilità della Società per la sicurezza sul luogo di lavoro, si raccomanda a tutti i Destinatari di attenersi con la massima scrupolosità alle disposizioni di legge ed ai principi che seguono.

3. PROCEDURE GENERALI

Nell'ambito della fattispecie di reato introdotta con l'art. 9 della legge 3 agosto 2007, n. 123 recante "*Misure in tema di tutela della salute e della sicurezza sul lavoro*", le disposizioni di cui al D.Lgs. 231/01 sono state integrate con la previsione normativa di cui all'art. 25 *septies* del D.Lgs. 231/01 relativo al reato di "*omicidio colposo e lesioni colpose gravi o gravissime, commessi con la violazione delle norme sulla tutela della salute e sicurezza sul lavoro*".

Con riferimento a tale fattispecie, è poi intervenuto il D.Lgs. 9 aprile 2008, n. 81 recante l'attuazione dell'art. 1 della legge 3 agosto 2007, n. 123 (il c.d. "*Testo Unico sulla Sicurezza*") che ha imposto specifici requisiti che devono sussistere in capo ai modelli organizzativi.

A tale fine, la presente sezione impone:

- il rispetto degli standard tecnico–strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- lo svolgimento delle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;

- lo svolgimento delle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;

- lo svolgimento delle attività di informazione e formazione dei lavoratori;

- lo svolgimento delle attività con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

- l'acquisizione e predisposizione di tutti i documenti e le certificazioni obbligatorie di legge;

- periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

L'avvenuta effettuazione delle attività sopra indicate deve essere registrata con sistemi idonei e su supporto duraturo.

La presente sezione prevede altresì l'espresso obbligo a carico di tutti gli esponenti aziendali in via diretta e tramite apposite clausole contrattuali a carico dei collaboratori esterni, dei fornitori e dei *partners* della Società di:

1. osservare tutte le leggi e regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro in conformità alle Linee Guida Uni–Inail del 28 settembre 2001 o al *British Standard* OHSAS 18001/2007;

2. gestire qualsiasi rapporto con la Pubblica Amministrazione al fine dell'applicazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro sulla base di criteri di massima correttezza e trasparenza.

Conseguentemente, è sancito l'espresso divieto a carico degli esponenti aziendali in via diretta ed a carico dei collaboratori esterni, dei fornitori e dei *partners* tramite apposite clausole contrattuali, di porre in essere:

1. comportamenti tali da integrare le fattispecie di reato considerate nel presente Allegato;

2. comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

3. qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione e/o nei confronti di qualunque autorità preposta in relazione a quanto previsto dalle suddette ipotesi di reato.

Al fine di prevenire la commissione di tali reati, è necessario:

- conoscere ed osservare tutte le leggi ed i regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle disposizioni legislative in materia di sicurezza e salute dei lavoratori contenute nel D.Lgs. 9 aprile 2008, n. 81 (Testo Unico sulla Sicurezza);

- gestire qualsiasi rapporto inerente la normativa per la sicurezza sulla base di criteri di massima correttezza e trasparenza.

Nell'ambito dei suddetti comportamenti:

- la Società gestisce le aree di attività riguardanti la pianificazione, l'organizzazione e la revisione del servizio di prevenzione e protezione dai rischi in modo unitario, individuando il responsabile per ogni operazione o pluralità di operazioni;

- gli incarichi conferiti in materia di sicurezza sui luoghi di lavoro vengono redatti per iscritto, conservati e protocollati unitamente alle qualifiche dell'incaricato;

- le eventuali deleghe di funzioni da parte del datore di lavoro dovranno risultare da atto scritto recante data certa, dovranno essere conferite a soggetti che posseggano tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate, dovranno attribuire al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate, dovranno attribuire al delegato l'autonomia di spesa

necessaria allo svolgimento delle funzioni delegate e la delega dovrà essere accettata per iscritto.

Il Modello deve essere integrato con il sistema degli adempimenti aziendali nascenti dagli obblighi di prevenzione e protezione imposti dall'ordinamento legislativo e con le procedure interne nascenti dalle esigenze di gestione della sicurezza sul lavoro.

A tal fine, il soggetto nominato Responsabile dei Servizi di Prevenzione e Protezione provvederà, d'intesa con il delegato alla sicurezza e con l'Organismo di Vigilanza, ad armonizzare le attività già svolte dalla Società in materia di gestione della sicurezza con quanto previsto dal D.Lgs. 231/01 evitando, per quanto possibile, duplicazioni.

Nell'ambito di un sistema integrato di controllo in materia di sicurezza sul lavoro, il Responsabile dei Servizi di Prevenzione e Protezione assumerà il controllo tecnico – operativo o di primo grado, mentre l'Organismo di Vigilanza, interagendo con il delegato alla sicurezza, viene incaricato del controllo sull'efficienza ed efficacia delle procedure rilevanti ai sensi del D.Lgs. 231/01 o di secondo grado.

4. PROCEDURE SPECIFICHE

A) Adozione di un Sistema di gestione della salute e sicurezza sul lavoro conforme alle Linee guida UNI–INAIL del 28.9.2001 e successive modifiche ovvero al *British Standard* OHSAS 18001/2007 e ss.mm.ii.

La Società è, in primo luogo, conforme alle previsioni stabilite dalle vigenti disposizioni normative in materia di tutela della salute e sicurezza sul lavoro di cui al D.Lgs. 9 aprile 2008 n. 81 e ss.mm.ii.

Ad ogni buon conto, data la particolare sensibilità dell'azienda per le tematiche connesse con la sicurezza dei propri lavoratori, la Società valuterà l'opportunità - ove ciò si rendesse necessario ai fini dell'adeguamento della Società stessa all'evoluzione delle attuali disposizioni normative in materia, anche con riferimento agli standard sovranazionali e/o ai canoni universalmente riconosciuti in detto settore - di adottare un Sistema di Gestione della Sicurezza sul Lavoro (nel seguito "SGSL") che dovrà,

pertanto, essere redatto conformemente alle "*Linee Guida UNI–INAIL per un sistema di gestione della salute e sicurezza sul lavoro*" del 28 settembre 2001 e succ. modd., ovvero al *British Standard* OHSAS 18001/2007 e ss.mm.ii.

Il SGSL deve essere finalizzato a garantire il raggiungimento degli obiettivi di salute e sicurezza che la Società si prefigura.

Con l'adozione di tale sistema la Società si propone di:

- ridurre progressivamente i costi complessivi della salute e sicurezza sul lavoro compresi quelli derivanti da incidenti, infortuni e malattie correlate al lavoro, minimizzando i rischi cui possono essere esposti i dipendenti o i terzi (clienti, fornitori, visitatori, ecc.);
- aumentare l'efficienza e le prestazioni della Società;
- contribuire a migliorare i livelli di salute e sicurezza sul lavoro;
- preservare e migliorare l'immagine interna ed esterna della Società.

Il SGSL deve operare sulla base della sequenza ciclica delle seguenti fasi: pianificazione, attuazione, monitoraggio e riesame del sistema.

Ciò deve avvenire per mezzo di un processo dinamico che coinvolge tutte le funzioni aziendali e soprattutto quelle di livello più elevato.

In applicazione dei principi dettati dalla Guida Operativa alle *Linee Guida UNI–INAIL per un sistema di gestione della salute e sicurezza sul lavoro* ovvero al *British Standard* OHSAS 18001/2007, il SGSL dovrà essere strutturato come segue:

1. Politica della sicurezza

Va stabilita in un documento scritto una politica della Salute e Sicurezza sul Lavoro ("SSL") che definisca gli impegni generali assunti dalla Società per la prevenzione dei rischi ed il miglioramento progressivo della SSL stessa.

La politica indica la visione, i valori essenziali e le convinzioni dell'azienda sul tema

della SSL e serve a definire la direzione, i principi d'azione ed i risultati a cui tendere ed esprime l'impegno del vertice aziendale nel promuovere nel personale la conoscenza degli obiettivi, la consapevolezza dei risultati da perseguire, la suddivisione ed accettazione delle responsabilità e le motivazioni dell'attività svolta.

Il documento sulla politica per la sicurezza sul lavoro deve includere tra l'altro:

- l'impegno al rispetto della legislazione e degli accordi applicabili alla SSL;
- l'affermazione che la responsabilità nella gestione della SSL riguarda l'intera organizzazione aziendale, dal datore di lavoro sino ad ogni lavoratore, ciascuno secondo le proprie attribuzioni e competenze;
- l'impegno a considerare la SSL ed i relativi risultati come parte integrante della gestione aziendale;
- l'impegno al miglioramento continuo ed alla prevenzione;
- l'impegno a fornire le risorse umane e strumentali necessarie;
- l'impegno a far sì che i lavoratori siano sensibilizzati e formati per svolgere i loro compiti in sicurezza e per assumere le loro responsabilità in materia di SSL;
- l'impegno al coinvolgimento ed alla consultazione dei lavoratori, anche attraverso i loro rappresentanti per la sicurezza;
- l'impegno a riesaminare periodicamente la politica stessa ed il sistema di gestione attuato;
- l'impegno a definire e diffondere all'interno dell'azienda gli obiettivi di SSL e i relativi programmi di attuazione.

2. Pianificazione

E' lo strumento attraverso cui si concretizza la politica della sicurezza definita dal vertice aziendale.

Il processo di pianificazione deve soddisfare i seguenti requisiti ed avere i seguenti contenuti:

- definizione e graduazione degli obiettivi finalizzati al mantenimento e/o al miglioramento del sistema;
- determinazione, preferibilmente al momento della definizione degli obiettivi, dei criteri di valutazione idonei a dimostrare l'effettivo raggiungimento degli obiettivi stessi;
- predisposizione di un piano per il raggiungimento di ciascun obiettivo contenente anche le mete intermedie, ove necessarie, l'individuazione delle figure/strutture coinvolte nella realizzazione del piano stesso e l'attribuzione dei compiti e delle responsabilità relative;
- definizione delle risorse necessarie, comprese quelle economiche;
- previsione delle modalità di verifica dell'effettivo ed efficace raggiungimento degli obiettivi.

3. Attuazione

Il SGSL deve:

- essere parte del sistema di gestione generale dell'impresa;
- contenere la struttura organizzativa, le responsabilità, le pratiche, le procedure, i processi, le risorse per realizzare la sua politica per la salute e sicurezza sul lavoro;
- essere adeguato alle attività svolte, alla dimensione aziendale, alla natura ed alle dimensioni dei rischi presenti in azienda;
- definire i compiti e le responsabilità della direzione aziendale, dei dirigenti, dei preposti e dei lavoratori;

- documentare e rendere note a tutti i livelli aziendali le funzioni ed i compiti del Responsabile del Servizio di Prevenzione e Protezione e degli eventuali addetti, del Rappresentante dei Lavoratori per la Sicurezza e degli addetti alla gestione delle emergenze, nonché i compiti e le responsabilità del Medico competente;

- definire modalità adeguate per realizzare il coinvolgimento dei lavoratori e/o dei loro rappresentanti attuando in particolare una consultazione preventiva in merito alla individuazione e valutazione dei rischi ed alla definizione di misure preventive, nonché riunioni periodiche da effettuarsi con frequenza e modalità che tengano conto delle richieste fissate dalla legislazione vigente;

- definire e mantenere attive attività di formazione ed addestramento del personale, sviluppando la consapevolezza dell'importanza della conformità delle azioni di ciascuno rispetto alla politica ed ai requisiti del SGSL;

- prevedere modalità di circolazione delle informazioni sia all'interno sia all'esterno (fornitori, collaboratori, clienti ecc.) dell'azienda;

- assicurare la tenuta e l'aggiornamento della documentazione rilevante (fra cui leggi, regolamenti, norme antinfortunistiche attinenti l'attività dell'azienda; regolamenti e accordi aziendali; manuale del SGSL, se esistente; quella richiesta dalla normativa vigente in materia di SSL; manuali, istruzioni per l'uso di macchine, attrezzature, dispositivi di protezione individuale (DPI) forniti dai costruttori; informazioni sui processi produttivi; schemi organizzativi; norme interne e procedure operative; piani di emergenza);

- prevedere l'integrazione dei processi aziendali della tutela della salute e sicurezza con la gestione complessiva dell'impresa, rendendoli integrati e congruenti.

4. Monitoraggio

Il SGSL deve prevedere una fase di verifica interna del raggiungimento degli obiettivi ed una fase di verifica della funzionalità del sistema stesso.

Le verifiche devono essere effettuate da persone competenti o rese tali da adeguata formazione e/o addestramento.

5. Riesame del sistema

Dopo la conclusione del ciclo di monitoraggio interno, il vertice aziendale deve sottoporre a riesame le attività del SGSL per valutare se il sistema sia adeguatamente attuato e si mantenga idoneo al conseguimento degli obiettivi e della politica della sicurezza stabilita dall'azienda.

Argomenti principali del riesame saranno:

- statistiche infortuni;
- risultati dei monitoraggi interni;
- azioni correttive intraprese;
- rapporti sulle emergenze (reali o simulate);
- rapporti del responsabile designato dalla direzione sulle prestazioni complessive del sistema;
- rapporti sulla efficacia del sistema di gestione;
- rapporti sulla identificazione dei pericoli e sulla valutazione e controllo dei rischi.

In conclusione del riesame, oltre a valutare lo stato di conseguimento degli obiettivi già fissati, la Società, alla luce dei risultati forniti dal monitoraggio del sistema, della esecuzione delle azioni correttive e preventive e delle eventuali modifiche della situazione, dovrà eventualmente stabilire nuovi obiettivi e piani, nell'ottica del miglioramento progressivo, considerando l'opportunità di modificare la politica, le procedure o eventuali altri elementi del sistema.

B) Adempimento degli obblighi giuridici

In ogni caso, le procedure dovranno assicurare l'adempimento di tutti gli obblighi giuridici relativi:

i) al rispetto degli standard tecnico – strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;

ii) alle attività di valutazione dei rischi, di predisposizione delle misure di prevenzione e protezione conseguenti;

iii) alle attività di natura organizzativa, quali le emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentati dei lavoratori per la sicurezza;

iv) alle attività di sorveglianza sanitaria;

v) alle attività di informazione e formazione dei lavoratori;

vi) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

vii) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;

viii) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Le procedure debbono prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività sopra esposte.

Le procedure dovranno assicurare un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

In relazione alle aree e fattori a rischio, vanno previste specifiche procedure in forza delle quali:

a) siano valutati tutti i rischi per la salute e sicurezza;

b) sia programmata la prevenzione, mirata ad un complesso che integri in modo coerente nella prevenzione le condizioni tecniche produttive dell'azienda

nonché l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro;

c) siano eliminati i rischi e, ove ciò non sia possibile, siano ridotti al minimo in relazione alle conoscenze acquisite in base al progresso tecnico;

d) siano rispettati i principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro e produzione, in particolare al fine di ridurre gli effetti sulla salute del lavoro monotono e di quello ripetitivo;

e) siano ridotti i rischi alla fonte;

f) sia sostituito ciò che è pericoloso con ciò che non lo è, o è meno pericoloso;

g) sia limitato al minimo il numero dei lavoratori che sono, o che possono essere, esposti al rischio;

h) sia limitato l'utilizzo degli agenti chimici, fisici e biologici sui luoghi di lavoro;

i) sia data priorità delle misure di protezione collettiva rispetto alle misure di protezione individuale;

j) vi sia il controllo sanitario dei lavoratori;

k) sia allontanato il lavoratore dall'esposizione al rischio per motivi sanitari inerenti la sua persona e l'adibizione, ove possibile, ad altra mansione;

l) siano informati ed adeguatamente formati i lavoratori;

m) siano informati e adeguatamente formati i dirigenti e i preposti;

n) siano informati e adeguatamente formati i rappresentanti dei lavoratori per la sicurezza;

o) siano date istruzioni adeguate ai lavoratori;

p) sia garantita la partecipazione e consultazione dei lavoratori;

q) sia garantita la partecipazione e consultazione dei rappresentanti dei lavoratori

per la sicurezza;

r) siano programmate le misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, anche attraverso l'adozione di codici di condotta e di buone prassi;

s) siano adottate le misure di emergenza da attuare in caso di primo soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato;

t) siano usati i segnali di avvertimento e di sicurezza;

u) vi sia la regolare manutenzione di ambienti, attrezzature, impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alla indicazione dei fabbricanti;

v) i soggetti responsabili dell'individuazione, dell'attuazione e del controllo sulle misure relative alla sicurezza, all'igiene e alla salute durante il lavoro dispongano del tempo, delle risorse e dei mezzi necessari per il corretto esercizio delle proprie funzioni.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nel presente Allegato.

Il presente Allegato e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale del Modello, al fine di garantire il raggiungimento delle finalità nello stesso previste.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO I

RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO

(Art. 25-octies)

(Articolo inserito dall'art. 63 del D.Lgs. 21 novembre 2007 n. 231, successivamente modificato dall'art. 3, comma 5 della Legge 15 dicembre 2014 n. 186)

1. REATI PRESUPPOSTO

Si riportano, di seguito, le rubriche dei reati presi in considerazione dall'art. 25-*octies* del D.Lgs. 231/01

- *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)*

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

La Legge 15 dicembre 2014 n. 186 ha introdotto nel nostro ordinamento, con decorrenza a partire dal 1° gennaio 2015, il nuovo reato presupposto di "*Autoriciclaggio*" previsto dall'art. 648 *ter.1* c.p. che punisce qualunque soggetto che impiega, sostituisce, trasferisce in attività economiche, finanziarie, imprenditoriali o speculative il denaro, i beni o le altre utilità derivanti da delitto non colposo (nel seguito, anche il "reato-base") che lo stesso soggetto ha commesso o concorso a commettere.

Ciò a condizione che la condotta sia idonea a ostacolare concretamente l'identificazione della provenienza illecita della provvista reperita con il reato-base.

Al contempo, il precetto penale stabilisce la non punibilità delle condotte di mero utilizzo o godimento personale della provvista illecita, in linea con l'assunto per cui tali ipotesi costituiscono la naturale prosecuzione del reato-base (il c.d. *post factum* non punibile).

L'inserimento, nell'elenco dei reati presupposto, del reato di *autoriciclaggio* comporta la necessità di verificare se le procedure ed i protocolli comportamentali individuati ed adottati nel Modello Organizzativo possono ritenersi idonei a prevenire il rischio di commissione del suddetto reato presupposto e, in caso negativo, di attuare una revisione del modello stesso.

Tale operazione coinvolge necessariamente:

- l'identificazione, da parte dell'ente, delle aree di rischio ai fini della commissione del reato di *autoriciclaggio*;
- la ricostruzione del sistema dei processi aziendali nel cui ambito è più probabile che venga commesso il reato in questione;
- l'impatto che può avere l'evento stesso;
- il piano di risposta al rischio adottato dall'ente.

A riguardo, deve peraltro tenersi in considerazione che:

a) la Legge 186/2014 richiede espressamente che la condotta – per essere rilevante ai fini della commissione del reato di *autoriciclaggio* – sia posta in essere "*in modo da ostacolare concretamente l'identificazione*" della provenienza illecita della provvista, evidenziando come la *ratio* della norma è pertanto diretta a punire soltanto quelle condotte che sono state poste in essere per ostacolare, in concreto, l'identificazione della provenienza delittuosa delle utilità. L'utilizzo di questa espressione evidenzia dunque una precisa scelta del legislatore, soprattutto alla luce della comparazione con l'analoga fattispecie di riciclaggio (art. 648*ter*, c.p.), che ha rappresentato il termine di paragone per la definizione dell'autoriciclaggio e non contiene l'avverbio sopra richiamato.

b) l'art. 25-*octies* punisce l'organizzazione che:

(i) ha tratto un interesse o vantaggio dall'attività di riciclaggio tenuta da soggetti ad essa facenti capo e

(ii) ha agevolato la condotta di costoro non avendo saputo impedire – per carenze organizzative interne – che il suo patrimonio venisse utilizzato per occultare la provenienza illecita dei capitali ivi investiti.

Sulla scorta di quanto sopra ed anche alla luce delle indicazioni fornite dall'Associazione Bancaria Italiana con circolare n. 6 del 1° dicembre 2015 "*Autoriciclaggio e responsabilità degli enti*", si ritiene che le procedure da individuarsi ed adottarsi al fine di eliminare il rischio di commissione del reato di *autoriciclaggio* e di conseguenti sanzioni *ex* art. 25 *octies* D.Lgs. 231/01 comminate a carico della Società debbano concentrarsi in particolar modo sul controllo della movimentazione dei flussi finanziari e di altri beni ed utilità che arrivano alla Società, in modo tale che la stessa sia in grado di accertare adeguatamente la lecita o illecita provenienza dei flussi stessi che si chiede che siano investiti nel patrimonio societario.

In tale quadro, possono pertanto configurarsi due differenti scenari:

1) <u>provenienza dall'esterno delle risorse reinvestite</u>:
   con riferimento a tale scenario ed in considerazione delle indicazioni fornite dall'ABI con la circ. n. 6 del 1° dicembre 2015, si ritiene che le procedure e i princìpi di comportamento individuati dalla Società per prevenire il rischio di commissione degli altri reati inseriti nell'elenco dei reati presupposto di cui al D.Lgs. 231/01, possono risultare efficaci anche per la prevenzione "a monte" dell'attività di autoriciclaggio dei relativi proventi illeciti.
   Pertanto, si rinvia ai principi di comportamento e ai presidi già implementati dalla Società per la prevenzione delle suddette fattispecie criminose, nonché alle procedure specificatamente individuate nel presente Allegato finalizzate, in particolare, a prevenire il rischio di incorrere in responsabilità per la commissione dei reati di "*Ricettazione*" (art. 648 c.p.), "*Riciclaggio*" (art. 648-*bis* c.p.) e "*Impiego di denaro, beni o utilità di provenienza illecita*" (art. 648-*ter* c.p.) e che verranno dettagliatamente affrontate nel prosieguo del presente

Allegato;

2) provviste illecite derivanti da attività interne:
anche con riferimento a tale ipotesi, il Modello adottato dalla Società risulta adeguatamente strutturato e dimensionato in modo tale da prevedere un sistema di protocolli e procedure finalizzate a prevenire la commissione da parte dei soggetti di cui agli artt. 5 e 6 del D.Lgs. 231/01 dei reati presupposto trattati in ciascuna Parte Speciale allegata al Modello stesso, eliminando così il rischio che si verifichi attività di autoriciclaggio degli eventuali proventi di tali reati-base.

A riguardo, il presente Allegato prevede specifici protocolli comportamentali e presidi di controllo incentrati alla verifica ed al controllo del denaro o delle utilità, sia in termini di "tracciabilità" delle suddette risorse, sia in ordine alle modalità di utilizzo delle stesse, limitando concretamente le probabilità di ricorso a comportamenti e tecniche idonei ad ostacolare in concreto l'individuazione della provenienza illecita delle provviste.

Quanto sopra premesso, in relazione ai reati di cui alla presente sezione, nell'ambito di attività finanziarie o di acquisto o cessione di beni che potenzialmente possano avere ad oggetto denaro, beni o altre utilità di provenienza illecita sono individuate, presso la Società le operazioni a rischio indicate nella *Check List* allegata al Modello.

Le aree sensibili sono quelle in cui incorre la normale operatività di un'azienda industriale.

Alla luce dell'esame di tale operatività, si è ritenuto di predisporre procedure per:

- la gestione della liquidità;
- la predisposizione dell'anagrafica clienti;
- l'individuazione di comportamenti sospetti con riferimento ai reati di cui alla presente Parte Speciale.

3. PROCEDURE GENERALI

Per ciascuna delle operazioni di carattere significativo individuate nell'articolo che precede sono previste specifiche procedure, in forza delle quali:

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

2. non vi sia identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;

3. i documenti riguardanti l'attività di impresa siano archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;

4. l'accesso ai documenti, di cui al punto precedente, già archiviati sia sempre motivato e consentito solo al soggetto competente in base alle norme interne, o a suo delegato, al Collegio Sindacale o organo equivalente, alla società di revisione, se nominata, e all'Organismo di Vigilanza;

5. non siano corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, agenti o a soggetti pubblici in misura non congrua rispetto alle prestazioni rese alla Società e non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;

6. eventuali sistemi di remunerazione premianti ai dipendenti e collaboratori rispondano a obiettivi realistici e coerenti con le mansioni e l'attività svolta e con le responsabilità affidate;

7. i flussi finanziari della Società, sia in entrata sia in uscita, siano costantemente monitorati e sempre tracciabili;

8. la Società, ai fini dell'attuazione delle decisioni di impiego delle risorse finanziarie, si avvalga di intermediari finanziari e bancari sottoposti a una

regolamentazione di trasparenza e correttezza conformi alla disciplina dell'Unione Europea;

9. venga effettuata un'adeguata verifica dell'identità dei clienti;
10. in caso di profili di anomalia nei rapporti finanziari con il fornitore o con il cliente - in relazione alle modalità, al luogo o al destinatario del pagamento – sia tempestivamente informato l'Organismo di Vigilanza;
11. le condizioni commerciali siano fissate da processi decisionali trasparenti e ricostruibili nel tempo, e siano autorizzate esclusivamente da soggetti dotati di idonei poteri secondo un sistema di deleghe e procure coerente con le responsabilità organizzative e gestionali;
12. le condizioni commerciali ed i rapporti con i clienti siano integralmente documentati in forma cartacea e/o elettronica;
13. i dati e le informazioni su clienti e fornitori siano completi e aggiornati, in modo da garantire la corretta e tempestiva individuazione dei medesimi e una puntuale valutazione e verifica del loro profilo;
14. siano effettuate con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche anche di Vigilanza e controllo, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate;
15. sia data piena attuazione, in quanto applicabili alla Società, alle prescrizioni contenute nel D.Lgs. 231/2007 volte alla prevenzione delle operazione di riciclaggio o impiego di denaro, beni o utilità di provenienza illecita;
16. siano adottati adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.

Nell'ambito di detti comportamenti, è inoltre fatto esplicito divieto, in particolare, di:

- omettere dati ed informazioni imposti dalla legge sulla normativa

antiriciclaggio, ove applicabile ad eventuali operazioni ritenute sospette;

- 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 da chiunque preposto a tale ruolo;

- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni previste dalle leggi, dalla normativa anche sul riciclaggio cui è eventualmente soggetta la Società;

- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità Pubbliche.

4. PROCEDURE SPECIFICHE

A) Gestione della liquidità

Le procedure adottate dalla Società devono prevedere il rispetto della normativa *pro tempore* in vigore in materia di antiriciclaggio e dei relativi limiti di utilizzo del contante e dei titoli al portatore.

Viene pertanto stabilito che, salvo che si tratti di piccole somme di servizio per le quali valgono comunque le disposizioni della sopra indicata normativa vigente in materia di antiriciclaggio, tutti i pagamenti devono essere effettuati o ricevuti dalla Società esclusivamente con bonifico bancario o con assegni bancari o postali che rechino l'indicazione del beneficiario e la clausola di non trasferibilità.

B) Gestione della contabilità e dell'amministrazione

Con riferimento all'area in esame, è necessario:

- identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da fonte affidabile ed indipendente;

- creare uno specifico dossier clienti e fornitori onde raccogliere e censire le informazioni critiche e significative degli stessi, ovvero a titolo di esempio: il legale rappresentante, la nazione di residenza, il tipo di attività economica svolta, la compagine societaria, eventuali precedenti penali ecc., al fine di poter desumere i requisiti di onorabilità e professionalità delle controparti con le quali la Società opera;

- verificare l'attendibilità commerciale e professionale di fornitori e partner commerciali;

- verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti e controparti effettivamente coinvolte

C) Individuazione di comportamenti sospetti

La Società adotta adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.

Segnala a tale personale i principali indici di anomalia connessi all'attività di riciclaggio desumibili dal profilo soggettivo, dal comportamento e dalla dislocazione territoriale del cliente, dal profilo economico – patrimoniale e dalle caratteristiche e finalità dell'operazione richiesta.

Gli indici di anomalia devono essere desunti dalle periodiche Delibere della Banca d'Italia sugli indicatori di anomalia relativi al profilo soggettivo, oggettivo, alle modalità di pagamento utilizzate, alle operazioni contabili e finanziarie.

In particolare, debbono essere considerati indici di anomalia i casi in cui:

- un cliente, in assenza di plausibili giustificazioni, richiede lo svolgimento di operazioni palesemente non abituali, non giustificati ovvero non proporzionate all'esercizio normale della sua professione o attività;

- un cliente richiede l'esecuzione di operazioni che impiegano disponibilità che appaiono eccessive rispetto al suo profilo economico – patrimoniale;

- un cliente richiede l'esecuzione di operazioni che non sembrano avere giustificazioni economiche e finanziarie;
- il cliente si rifiuta o si mostra ingiustificatamente riluttante a fornire le informazioni occorrenti a dichiarare l'attività esercitata, a presentare documentazione contabile o di altro genere, a segnalare rapporti intrattenuti con altri professionisti, a fornire ogni altra informazione che, in circostanze normali viene acquisita nello svolgimento delle normali attività aziendali;
- il cliente fornisce informazioni palesemente inesatte o incomplete, tali da manifestare l'intento di occultare informazioni essenziali;
- il cliente usa documenti identificativi che sembrano contraffatti;
- il cliente rifiuta di o solleva obiezioni a pagare il prezzo della prestazione con bonifico o assegno bancario;
- le dichiarazioni del cliente in relazione all'operazione del cliente appaiono incongruenti;
- il cliente effettua transazioni con controparti in località inusuali per lo stesso;
- l'operazione appare non economicamente conveniente per il cliente e/o manca un'apparente ragione per utilizzare i servizi dell'operatore;
- l'operazione appare eccessivamente complessa o insolita per lo scopo dichiarato;
- il cliente intende regolare il pagamento dell'operazione con una somma notevole di denaro contanti.

Ove alcuni di tali indici di anomalia vengano riscontrati, si dovrà procedere alla tempestiva segnalazione all'Organismo di Vigilanza.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nel presente Allegato.

Il presente Allegato e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale del Modello, al fine di garantire il raggiungimento delle finalità dallo stesso preposte.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO J

DELITTI DI CRIMINALITÀ ORGANIZZATA

(Art. 24-ter)

DELITTO DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA

(Art. 25-decies)

REATI TRANSNAZIONALI

EX ART. 10 DELLA LEGGE 16 MARZO 2006, N. 146

1. REATI PRSUPPOSTO

Si riportano, di seguito, le rubriche dei reati transnazionali presi in considerazione dall'art. 10 della legge 16 marzo 2006, n. 146:

- *Associazione per delinquere* (art. 416 c.p.);
- *Associazione di tipo mafioso* (art. 416-*bis* c.p.);
- *Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri* (art. 291- *quater* D.P.R. 43/1973);
- *Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope* (art. 74 D.P.R. 309/1990);
- *Disposizioni contro le immigrazioni clandestine* (art. 12, commi 3, 3-*bis*, 3-*ter*, 5 D.Lgs. 286/1998);
- *Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria* (art. 377-*bis* c.p.);
- *Favoreggiamento personale* (art. 378 c.p.).

L'articolo 2, comma 29, legge 15 luglio 2009, n. 94 (parte del c.d. "*pacchetto*

sicurezza 2009") ha inserito nel *corpus* del D.Lgs. 231/01 il nuovo articolo 24 *ter* che prevede i seguenti ulteriori reati presupposto:

- *delitti di associazione per delinquere finalizzata alla riduzione o al mantenimento in schiavitù o in servitù, alla tratta di persone, all'acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni contro le immigrazioni clandestine di cui all'art. 12 D.Lgs. 25 luglio 1998 n. 286* (Art. 416, sesto comma c.p.);
- *associazioni di tipo mafioso anche straniere* (Art. 416-*bis* c.p.);
- *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 D.P.R. 309/90);
- *associazione per delinquere* (Art. 416, ad eccezione sesto comma, c.p.);
- *illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo 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 lettera a) c.p.).

L'art. 4, comma 1 della legge 3 agosto 2009, n. 116 ha altresì inserito tra i reati presupposto del D.Lgs. 231/01

- *l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria* (art. 377 *bis* c.p.)[1].

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Nell'ambito delle attività che comportano possibili contatti anche indiretti con

[1] Il reato presupposto in esame è stato inserito dalla norma citata nel D.Lgs. 231/01 come articolo 25 – *nonies*, non tenendo conto dell'inserimento di tale articolo 25 – *nonies* da parte dell'art. 15, comma 7, lettera c) della legge 23 luglio 2009, n. 99. Per tale motivo, nella prassi, si ritiene di rinumerarlo come art. 25 – *decies*.

organizzazioni criminali organizzate, sono individuate presso la Società le operazioni a rischio indicate nella *Check List* allegata al Modello, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati trattati nel presente Allegato.

Per quanto si ritenga che, alla luce dell'attività sociale svolta, il rischio non si presenti particolarmente elevato, la Società ritiene di predisporre idonee procedure per la:

- valutazione e selezione dei fornitori;
- valutazione della clientela, gestione del credito e concessione di affidamenti.

Tali procedure sono volte a prevenire la commissione sia dei c.d. *reati transnazionali* di cui all'art.10 della legge 16 marzo 2006, n. 146, sia di quelli c.d. *di criminalità organizzata* di cui all'articolo 2, comma 29, legge 15 giugno 2009, n. 94.

Con riferimento al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, si rende opportuno adottare la seguente procedura:

- rapporti con soggetti coinvolti in procedimenti giudiziari di cui al paragrafo 4, lettera C del presente Allegato (v. *infra*).

3. PROCEDURE GENERALI

Per ciascuna delle operazioni di carattere significativo individuate nell'articolo che precede sono previste specifiche procedure, in forza delle quali:

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

b) non vi sia identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;

c) i documenti riguardanti l'attività di impresa siano archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;

d) l'accesso ai documenti, di cui al punto precedente, già archiviati sia sempre motivato e consentito solo al soggetto competente in base alle norme interne, o a suo delegato, al Collegio Sindacale o organo equivalente, alla società di revisione, se nominata, e all'Organismo di Vigilanza;

e) la scelta di consulenti tecnici o collaboratori esterni avvenga sulla base di requisiti di professionalità, indipendenza e competenza e in riferimento a essi sia motivata la scelta;

f) non siano corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, agenti o a soggetti pubblici in misura non congrua rispetto alle prestazioni rese alla Società e non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;

g) eventuali sistemi di remunerazione premianti ai dipendenti e collaboratori rispondano a obiettivi realistici e coerenti con le mansioni e l'attività svolta e con le responsabilità affidate;

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

i) le condizioni commerciali siano fissate da processi decisionali trasparenti e ricostruibili nel tempo, e siano autorizzate esclusivamente da soggetti dotati di idonei poteri secondo un sistema di deleghe e procure coerente con le responsabilità organizzative e gestionali;

j) le condizioni commerciali ed i rapporti con i clienti siano integralmente documentati in forma cartacea e/o elettronica;

k) i dati e le informazioni raccolti su clienti e fornitori siano completi e aggiornati, in modo da garantire la corretta e tempestiva individuazione dei medesimi e una puntuale valutazione e verifica del loro profilo.

Ai Destinatari è inoltre fatto divieto di:

- promuovere, costituire od organizzare associazioni con altri soggetti allo scopo di commettere delitti;
- in ogni caso, incoraggiare, sostenere o partecipare ad associazioni per delinquere, in particolare se di stampo mafioso;
- compiere atti diretti a procurare l'ingresso di taluno nel territorio dello Stato in violazione delle disposizioni in materia di immigrazione clandestina, ovvero a procurare l'ingresso illegale in altro Stato del quale la persona non è cittadina o non ha titolo di residenza;
- aiutare taluno ad eludere le investigazioni dell'autorità, o a sottrarsi alle ricerche di questa.

4. PROCEDURE SPECIFICHE

A) Valutazione, qualifica e selezione dei fornitori di beni e servizi

La procedura deve necessariamente prevedere quanto segue:

a) sia formalizzato il processo di selezione e valutazione del fornitore, nonché della gestione del rapporto con il medesimo;

b) sia individuato per ciascuna fase di selezione, valutazione e gestione del fornitore un responsabile interno e i livelli autorizzativi di formazione e attuazione delle decisioni;

c) siano preventivamente identificati e costantemente aggiornati indici di rischio di reato e di possibili anomalie in relazione a ciascuna categoria di fornitori;

d) per le fasi di selezione e di valutazione del fornitore siano individuati idonei criteri e modalità di scelta del fornitore che garantiscano un processo comparativo degli offerenti. Qualora il processo comparativo non sia possibile o sia giudicato non necessario, la funzione competente lo segnali al livello gerarchico superiore, dando adeguata motivazione;

e) siano stabilite idonee modalità di raccolta e conservazione della documentazione relativa al processo di selezione, valutazione e gestione del fornitore;

f) ogni rapporto con i fornitori sia disciplinato da contratto scritto, sottoscritto esclusivamente dal soggetto dotato di idonei poteri secondo il sistema di deleghe e procure vigente, nel quale sia chiaramente prestabilito il prezzo del bene o della prestazione da ricevere o i criteri per determinarlo;

g) i contratti di approvvigionamento che possano presentare carattere inusuale o anomalo per tipologia o oggetto della richiesta, siano sempre preventivamente valutati e autorizzati dalla direzione generale della Società, informato l'Organismo di Vigilanza;

h) in caso di dubbio sulla qualifica o sulla permanenza della qualifica in capo al fornitore oppure in caso di sopravvenienza di profili di anomalia nei rapporti con il fornitore o nella tipologia delle richieste da questi avanzate, la commessa sia assegnata o il rapporto sia mantenuto solo previa espressa autorizzazione della direzione generale, informato l'Organismo di Vigilanza;

i) chiunque ne sia a conoscenza, segnali immediatamente all'Organismo di Vigilanza oppure al proprio superiore gerarchico, che riferirà all'Organismo di Vigilanza, eventuali anomalie nelle prestazioni dovute dal fornitore, discordanze significative o ripetute tra materiale o servizio ricevuto rispetto a quanto concordato o particolari richieste avanzate dal fornitore alla Società;

j) nei contratti che regolano i rapporti con i fornitori sia valutata l'opportunità di prevedere apposite clausole che richiamano gli adempimenti e le responsabilità

derivanti dal D.Lgs. 231/01 e dal rispetto del presente Modello e delle sue parti integranti;

k) nei contratti che regolano i rapporti sia con i clienti che con i fornitori, sia valutata l'opportunità di prevedere l'inserimento di clausole che consentano la risoluzione del contratto da parte della Società nel caso in cui il cliente, ovvero il fornitore, risulti coinvolto in procedimenti giudiziari.

B) Valutazione della clientela, gestione del credito, concessione di affidamenti alla clientela, gestione delle condizioni economico-finanziarie (prezzi e sconti) definite nei contratti con i clienti

La procedura deve prevedere quanto segue:

a) ogni rapporto di cessione di beni o servizi sia disciplinato da contratto scritto, sottoscritto esclusivamente dal soggetto dotato di idonei poteri secondo il sistema di deleghe e procure vigente, nel quale sia chiaramente prestabilito il prezzo del bene o della prestazione da effettuare o i criteri per determinarlo;

b) siano previste modalità e limiti per la concessione di sconti commerciali rispetto al listino prezzi della Società, anche tenendo conto delle oscillazioni dei prezzi di mercato;

c) non vi sia identità soggettiva fra coloro che propongono, coloro che autorizzano la concessione del credito al cliente, coloro che devono dare evidenza contabile dell'operazione e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;

d) siano stabiliti limiti alla concessione di credito alla clientela da parte del responsabile della funzione, mediante la fissazione di soglie quantitative coerenti alle competenze gestionali ed alle responsabilità organizzative affidate; le operazioni che superino la soglia quantitativa siano preventivamente valutate e approvate dall'organismo superiore a quello che cura la funzione;

e) l'affidamento della clientela sia sempre subordinato a una valutazione generale della affidabilità finanziaria e della consistenza patrimoniale del cliente, svolta attraverso la raccolta di informazioni da fonti interne (struttura e organizzazione della Società, protesti, visure ipotecarie e catastali, ecc.) e da fonti esterne, ricorrendo a banche dati ufficiali aggiornate. In caso di rilascio di garanzie personali da parte di terzi a favore dei clienti, siano effettuati accertamenti idonei sul soggetto garante, individuando indici di rischio o anomalia;

f) le operazioni di affidamento della clientela siano documentate a cura della funzione proponente e, una volta approvate, siano registrate nell'anagrafica clienti in conformità ai principi di correttezza professionale;

g) siano effettuati controlli periodici da parte del responsabile della funzione di controllo crediti di sede sugli affidamenti in essere presso la Società, anche in relazione all'esposizione aggiornata del cliente;

h) qualora l'esposizione del cliente superi i parametri indicati dalle procedure interne, la fornitura sia bloccata, salva diversa valutazione responsabile della funzione di controllo crediti, opportunamente motivata;

i) chiunque ne sia a conoscenza segnali immediatamente all'Organismo di Vigilanza oppure al proprio superiore gerarchico, che riferirà all'Organismo di Vigilanza, eventuali anomalie nelle prestazioni dovute al cliente, discordanze significative o ripetute tra materiale ceduto o servizio prestato rispetto a quanto concordato o particolari richieste avanzate dal cliente alla Società.

C) <u>Rapporti con soggetti coinvolti in procedimenti giudiziari</u>

La procedura deve prevedere quanto segue:

- è fatto assoluto divieto di indurre con qualsiasi modalità soggetti terzi che sono chiamati a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale a non rendere dichiarazioni o a rendere dichiarazioni mendaci;

- ove un dipendente della Società venga indotto da uno dei Destinatari del Modello a non rendere dichiarazioni od a rendere dichiarazioni mendaci, il medesimo dovrà senza indugio riferirne all'Organismo di Vigilanza;

- nei contratti che regolano i rapporti sia con i clienti che con i fornitori, sia valutata l'opportunità di prevedere l'inserimento di clausole che consentano la risoluzione del contratto da parte della Società nel caso in cui il cliente, ovvero il fornitore, risulti coinvolto in procedimenti giudiziari.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nel presente Allegato.

Il presente Allegato e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale del Modello, al fine di garantire il raggiungimento delle finalità dallo stesso preposte.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO K

DELITTI INFORMATICI

E

TRATTAMENTO ILLECITO DI DATI

(Art. 24-bis)

(Articolo aggiunto dall'art. 7 della Legge 18 marzo 2008 n. 48)

1. REATI PRESUPPOSTO

Si riportano, di seguito, le rubriche dei delitti informatici e trattamento illecito di dati presi in considerazione dall'art. 24 *bis* del D.Lgs. 231/01:

- *accesso abusivo ad un sistema informatico o telematico* (art. 615 *ter* c.p.);
- *detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici* (art. 615 *quater* c.p.);
- *diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico* (art. 615 *quinquies* c.p.);
- *intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* (art. 617 *quater* c.p.);
- *installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche* (art. 617 *quinquies* c.p.);
- *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.)
- *falsità in un documento informatico o avente efficacia probatoria* (art. 491 *bis*

c.p.);

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

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Nonostante l'informatica non rivesta una importanza preponderante nell'attività aziendale, la Società ritiene opportuno che tutti i Destinatari prestino la massima attenzione alle disposizioni contenute nel presente Allegato e ritiene ad ogni buon conto opportuno predisporre idonee procedure per:

- il monitoraggio della rete interna con particolare riferimento dei dati ivi contenuti;
- la formazione e la sensibilizzazione del personale tecnico che opera sulle reti telematiche;
- il *tracking* interno ed esterno dei flussi delle informazioni.

In occasione, peraltro, delle precedenti attività preposte alla stesura della *Check List* è emerso che l'attività di manutenzione e gestione dei sistemi informatici e telematici è affidata in appalto ad una società esterna.

3. PROCEDURE GENERALI

La presente sezione prevede che in materia di sicurezza informatica siano garantiti i seguenti requisiti:

- **riservatezza**: intesa come garanzia che i dati informatici siano preservati da accessi impropri e siano utilizzati esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;

- **integrità**: intesa come garanzia che ogni dato informatico sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato

esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;

- **disponibilità**: intesa come garanzia di reperibilità di dati informatici aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Sulla base di tali principi e seppur tenuto conto di quanto evidenziato al paragrafo che precede, le procedure individuate nel presente Allegato prevedono 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. 24-*bis* del D.Lgs. 231/2001);

- violare i principi e le procedure aziendali previste nel presente Allegato.

Nell'ambito delle suddette regole è fatto divieto, in particolare, di:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;

- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;

- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;

- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;

- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;

- svolgere attività di produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;

- installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;

- svolgere attività di modifica illecita e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

I Destinatari debbono pertanto:

1. utilizzare le informazioni, le applicazioni e le apparecchiature informatiche della Società esclusivamente per finalità strettamente attinenti allo svolgimento delle proprie mansioni;

2. non prestare o permettere a terzi l'uso delle apparecchiature informatiche della Società, senza la preventiva autorizzazione del responsabile dei sistemi informativi;

3. in caso di smarrimento o furto, informare tempestivamente il responsabile dei sistemi informativi e gli uffici amministrativi della Società e presentare denuncia all'Autorità Giudiziaria preposta;

4. evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;

5. evitare di utilizzare *password* di altri utenti; qualora un soggetto venga a conoscenza della *password* di altro utente, è tenuto a darne immediata notizia al responsabile dei sistemi informativi;

6. rispettare le procedure e gli standard previsti dalla Società, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;

7. utilizzare ed installare sulle apparecchiature della Società solo prodotti autorizzati dalla Società stessa;

8. astenersi dall'effettuare copie non specificamente autorizzate di dati e di *software* di proprietà della Società;

9. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendale per la protezione e il controllo dei sistemi informatici ed ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;

Per ciascuna delle operazioni di carattere significativo individuate nel presente Allegato sono previste specifiche procedure in forza delle quali:

a) sia previsto (compatibilmente con la normativa vigente in materia di diritto del lavoro e di diritto alla privacy) il costante monitoraggio della rete interna;

b) siano adottati adeguati programmi di formazione del personale ritenuto esposto al rischio relativo ai reati informatici e sia attuata una politica di sensibilizzazione di tutti gli utenti alla sicurezza informatica;

c) sia prevista, ove necessario ai fini dell'attività produttiva, la protezione del trasferimento dei dati, al fine di assicurare riservatezza, integrità e disponibilità

dei canali trasmissivi (sistemi IPS - *intrusion prevention system* / IDS - *intrusion detection system*);

d) sia prevista una procedura periodica (con cadenza almeno annuale) di verifica della vulnerabilità dei sistemi informativi della Società;

e) sia previsto il costante aggiornamento delle componenti antivirus sui sistemi informativi della Società;

f) tutte le richieste di modifica dei flussi informativi trasmessi dai clienti successive alla loro ricezione da parte della Società avvengano con comunicazione scritta e i documenti riguardanti tali attività siano archiviati e conservati, a cura della funzione competente, così che il processo sia sempre tracciabile;

g) sia prevista l'attuazione di un tracciamento delle operazioni che possono influenzare la sicurezza di dati critici;

h) un *server* di dominio garantisca l'accesso ai dati riservati dei singoli clienti esclusivamente ad utenti od applicazioni preventivamente autorizzati dalla Società, tenendo traccia di ogni accesso e dell'attività svolta.

4. PROCEDURE SPECIFICHE

A) Monitoraggio della rete informatica

La Società adotta una procedura che permette il monitoraggio della propria rete informatica.

Il monitoraggio è assicurato attraverso appositi programmi, procedure e strumenti che rilevano e segnalano attività o eventi irregolari o anomali che sono suscettibili di integrare delitti informatici o trattamento illecito di dati.

Detti strumenti segnalano e quindi permettono di individuare il punto di origine del rischio per la sicurezza o del comportamento illecito (strumento od attività) e

eventualmente di ricondurlo ad un utente determinato.

Gli eventi irregolari o anomali che vengono monitorati, rilevati e segnalati sono i seguenti:

- interventi sulle basi di dati (*database* e archivi);
- interventi sulle applicazioni *software*;
- trascrizione dati via posta elettronica o FTP (ove, in quest'ultimo caso, utilizzato);
- monitoraggio dei dati e dei programmi installati su ogni singola postazione di lavoro.

La Società, nel rispetto dell'art. 4 della L. 20 maggio 1970 n. 300 (Statuto dei lavoratori), non utilizza alcuno specifico strumento *hardware* e *software* finalizzato a controllare a distanza il lavoratore e le sue attività, e in particolare:

- alla lettura sistematica dei messaggi di posta elettronica personali;
- al monitoraggio dei siti *web* visitati dal lavoratore;
- alla traccia di altre attività, quali creazione e modifica di *files*.

Esistono alcune forme di registrazione di alcune attività, anche riferibili a singoli lavoratori, le quali o sono necessarie per il corretto funzionamento dei sistemi ed al fine di ottemperare alle previsioni del D.Lgs. 30 giugno 2003, n. 196 nonché del Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati), oppure sono effettuate dagli strumenti informatici utilizzati per loro intrinseca natura.

Nel rispetto dei principi stabiliti dal Garante della Privacy:

- i lavoratori sono preventivamente informati dell'esistenza di tali forme di monitoraggio;

- ogni tipo di registrazione delle attività degli utenti sopra descritta è accessibile solo alla direzione aziendale o a persone appositamente incaricate ed istruite per iscritto di non utilizzarle per finalità diverse da quelle di prevenire o bloccare la commissione di illeciti, con il più rigoroso divieto di monitorare attività dei

singoli lavoratori o estrapolare dati sulle attività dei singoli lavoratori al di fuori di quelli relativi all'illecito stesso.

B) Formazione del personale tecnico

La Società adotta adeguati programmi di formazione e sensibilizzazione del personale ritenuto esposto al rischio di commissione di reati informatici.

Segnala a tale personale la lista dei reati con le relative fattispecie e le sanzioni che possono essere irrogate.

Attua una politica di sensibilizzazione di tutti gli utenti alla sicurezza informatica.

In particolare, il personale viene sensibilizzato ad evitare i seguenti comportamenti:

- utilizzare la rete *internet* esclusivamente per scopi strettamente connessi con l'attività aziendale e le mansioni svolte;
- non accedere a siti diversi da quelli previamente autorizzati dall'azienda;
- non scaricare programmi e/o *files* – anche gratuiti - senza esplicita autorizzazione del proprio Responsabile;
- fermo quanto al precedente punto, non scaricare in ogni caso programmi se non in ambienti autorizzati;
- non visitare siti web diversi da quelli autorizzati dalla Società ovvero dal proprio Responsabile;
- non copiare dati e/o programmi se non specificatamente autorizzati;
- non esportare, con qualsivoglia strumento, i dati aziendali;
- non utilizzare gli strumenti informatici messi a disposizione della Società per fini ed interessi non strettamente coincidenti con quelli dell'azienda e con le mansioni affidate al singolo dipendente;
- non utilizzare la posta elettronica aziendale per scopi privati.

C) *Tracking* interno ed esterno dei flussi delle informazioni

La Società attua un sistema di protezione idoneo a identificare univocamente gli utenti

che accedono al sistema aziendale e che regola l'accesso di ciascun utente sulla base dei privilegi a ciascuno assegnati.

La Società utilizza sistemi informatici che tengono traccia dei *log* di ogni singolo utente così che, in caso di bisogno, l'attività di ogni operatore sui sistemi informativi aziendali possa essere ricostruita con certezza.

Se l'accesso avviene a mezzo di *user id* e *password*, la *password* è personale e non deve essere comunicata a terzi.

Ciascun soggetto è responsabile della segretezza della propria *password* d'accesso al sistema e non possono essere utilizzate *password* di altri utenti.

Qualora un soggetto venga a conoscenza della *password* di altro utente, è tenuto a darne immediata notizia al responsabile dei sistemi informativi ovvero, in assenza di tale figura, al proprio Responsabile di riferimento.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nel presente Allegato.

Il presente Allegato e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale del Modello, al fine di garantire il raggiungimento delle finalità dallo stesso preposte.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO L

DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

(Art. 25-bis.1)

(Articolo aggiunto dall'art. 17, comma 7, lett. b) della Legge 23 luglio 2009 n. 69)

1. REATI PRESUPPOSTO

L'art. 17, comma 7 lettera b) della legge 23 luglio 2009, n. 99 ha inserito tra i reati presupposto del D.Lgs. 231/01 le seguenti fattispecie:

- *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.).

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

La Società, in considerazione dell'attività svolta, non ha rinvenuto rischi specifici di particolare rilevanza con riferimento ai reati previsti nel presente Allegato.

L'unico reato in astratto configurabile sembra essere quello – potenzialmente comune a tutte le realtà imprenditoriali - dell'*illecita concorrenza con minaccia o violenza* di cui all'art. 513–*bis* c.p.

Tuttavia, anche tenuto conto del contenuto del Codice Etico in vigore che già ribadisce l'obbligo di operare nel rispetto delle leggi vigenti e dell'etica professionale, si ritiene

di non dover predisporre una procedura *ad hoc* per prevenire tale rischio e ci si limita a richiamare l'attenzione dei Destinatari sull'opportunità di mantenere in tutte le situazioni un comportamento improntato alla massima correttezza nei rapporti con i *competitors* e con i terzi in generale.

A tal fine, il responsabile della funzione commerciale aziendale impartisce ai dipendenti che svolgono mansioni a rischio di commissione dei reati presupposto di cui al presente Allegato istruzioni specifiche con l'invito a prestare particolare attenzione al rispetto di tutti gli obblighi di correttezza nelle relazioni commerciali con i *competitors* e con i terzi.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO M

DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

(Art. 25 nonies)

(Articolo inserito dall'art. 15, comma 7, lett. c) della Legge 23 luglio 2009 n. 99)

1. REATI PRESUPPOSTO

L'art. 15, comma 7 lettera c) della legge 23 luglio 2009, n. 99 ha esteso la responsabilità amministrativa degli enti ai seguenti delitti in materia di violazione del diritto d'autore:

- *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*, Legge 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, Legge 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, Legge 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, Legge 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*, Legge n. 633/1941);

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

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Nell'ambito delle attività sociali che possono comportare la commissione di uno dei delitti in materia di diritto d'autore di cui all'art. 25-*nonies* del D.Lgs. 231/01 sono state individuate le operazioni a rischio specificate nella *Check List* prodotta dalla Direzione Aziendale e messa a disposizione dell'Organismo di Vigilanza.

La Società – richiamato quanto già esposto nell'Allegato che tratta i "*Delitti Informatici e trattamento illecito di dati*" – ritiene opportuno regolamentare l'utilizzo delle proprie risorse informatiche per assicurare che non vengano poste in essere condotte in violazione delle norme sul diritto d'autore.

Alla luce dell'esame dell'operatività della Società, si è quindi ritenuto di predisporre procedure per:

- acquisto e sottoscrizione nuove licenze da parte della Società di *software* e banche dati;
- controllo della validità delle licenze e *sub*-licenze dei *software* e delle banche dati in essere;
- monitoraggio e controllo della rete informatica interna;
- formazione del personale;
- gestione di opere dell'ingegno protette che si trovano nella disponibilità della Società.

3. PROCEDURE GENERALI

Per ciascuna delle operazioni di carattere significativo individuate nella *Check List* allegata al Modello sono previste specifiche procedure in forza delle quali siano garantiti i seguenti requisiti:

- i *software* e le banche dati installati sui personal computer della Società siano sempre muniti di valida licenza di utilizzo;

- la rete informatica della Società ed i dati presenti nella stessa siano preservati da accessi ed utilizzi impropri;

- sia fornito accesso da e verso l'esterno a mezzo di connessione internet esclusivamente ai sistemi informatici dei soggetti che ne abbiano effettiva necessità ai fini lavorativi;

- i *files* relativi alle eventuali opere protette da diritto d'autore detenute dalla Società in formato elettronico siano accessibili, in conformità con la vigente normativa in materia di norme a tutela del diritto d'autore, esclusivamente al personale autorizzato e non possano essere diffusi o divulgati illegittimamente;

- il personale ritenuto esposto al rischio di commissione dei reati in materia di diritto d'autore sia sempre adeguatamente formato e sensibilizzato a tenere

comportamenti corretti.

Sulla base di tali principi, il presente Allegato 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-*nonies* del D.Lgs. 231/2001);

- detenere programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE);

- mettere a disposizione di terzi, riprodurre, divulgare, trasmettere o diffondere, in tutto o in parte, opere dell'ingegno tutelate dal diritto d'autore e dai diritti connessi;

- violare i principi e le procedure aziendali previste nel presente Allegato.

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

- installare sui sistemi informativi della Società programmi per elaboratore non assistiti da valida licenza d'utilizzo;

- installare sui sistemi informatici della Società *software* mediante i quali è possibile scambiare con altri soggetti all'interno della rete internet ogni tipologia di *files*, quali filmati, documenti, canzoni, opere letterarie (c.d. P2P, di *files sharing* o *instant messaging*);

- scaricare sui *personal computer* della Società programmi prelevati da internet o da sistemi *peer to peer*, anche qualora trattasi di *software* gratuiti (c.d. *freeware*) o *shareware*, salvo espressa autorizzazione del responsabile dei sistemi informativi ove presente, ovvero del proprio Responsabile di riferimento;

- installare sui *personal computer* della Società apparati di comunicazione propri (ad esempio *modem*);

- ascoltare sui *personal computer* della Società *files* audio o musicali, nonché visionare video e/o immagini, su qualsiasi supporto essi siano memorizzati, se non a fini prettamente lavorativi.

I Destinatari debbono pertanto:

1. utilizzare esclusivamente i *software*, le applicazioni, i *files* e le apparecchiature informatiche fornite dalla Società e farlo esclusivamente per finalità strettamente attinenti allo svolgimento delle proprie mansioni;

2. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendale per la protezione e il controllo dei sistemi informatici ed ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;

3. rispettare le *policy* interne in merito ai dispositivi antintrusione e antivirus;

4. custodire le *password* di accesso alla rete aziendale ed alle diverse applicazioni e le chiavi personali secondo criteri idonei a impedirne una facile individuazione ed un uso improprio;

5. non prestare o permettere a terzi l'uso delle apparecchiature informatiche della Società o dell'archivio informatico della stessa, senza la preventiva autorizzazione del responsabile dei sistemi informativi;

6. astenersi dall'effettuare copie non specificamente autorizzate dal responsabile dei sistemi informativi ovvero al proprio Responsabile di riferimento di dati e di *software* di proprietà della Società;

7. evitare di trasferire all'esterno della Società e/o trasmettere *files*, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;

8. qualora per la connessione alla rete internet si utilizzino collegamenti *wireless*, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete

internet tramite i *routers* della stessa e compiere illeciti ascrivibili ai dipendenti.

Per ciascuna delle operazioni di carattere significativo individuate nel presente Allegato sono previste specifiche procedure in forza delle quali:

a) sia previsto (compatibilmente con la normativa vigente in materia di diritto del lavoro e di diritto alla *privacy*) il costante monitoraggio della rete informatica interna;

b) siano adottati adeguati programmi di formazione del personale ritenuto esposto al rischio relativo ai reati informatici e sia attuata una politica di sensibilizzazione di tutti gli utenti alla sicurezza informatica;

c) la rete informatica della Società sia dotata di adeguate protezioni, così da evitare la non corretta duplicazione, riproduzione, trasmissione o divulgazione di opere dell'ingegno protette, ed in particolare delle opere letterarie nella disponibilità della Società;

d) sia prevista l'attuazione di un tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici contenuti nel sistema informativo della Società;

e) sia assicurato che tutti i supporti informatici alienati o smaltiti (*personal computer*, *floppy disc*, CD o DVD) siano resi illeggibili prima della loro vendita o distruzione, così da evitare l'involontaria diffusione di programmi e/o contenuti protetti.

4. PROCEDURE SPECIFICHE

A) Installazione ed utilizzo dei programmi per elaboratore

La Società adotta una procedura che assicuri che su tutti i suoi *personal computer* possano essere installati esclusivamente programmi per elaboratore muniti di valida licenza di utilizzo ed approvati dalla Società.

In primo luogo – come sopra già segnalato - la Società vieta ai propri dipendenti di modificare il contenuto del pacchetto *software* installato sui pc aziendali, installandovi programmi ed applicativi non autorizzati, ancorché muniti di regolare licenza per il loro utilizzo.

Il contenuto *software* dei personal computer concessi in uso ai dipendenti viene stabilito dalla Direzione della Società, anche sulla base delle informazioni e delle relazioni tecniche periodicamente ricevute dai responsabili addetti alla manutenzione dell'infrastruttura IT aziendale, autorizzandone a tal fine l'eventuale modifica.

L'intervento sul *software* utilizzato è, pertanto, consentito (e concretamente realizzabile) esclusivamente da parte degli addetti alla manutenzione del sistema informatico aziendale, i quali sono gli unici soggetti che dispongono delle credenziali e delle chiavi di accesso al sistema stesso per apportarvi le modifiche stabilite dalla Società.

B) Controllo della validità delle licenze e *sub*-licenze dei *software* e delle banche dati in essere

La manutenzione del *software* installato sui personal computer aziendali viene affidata contrattualmente dalla Società ad una terza società specializzata nel settore informatico, la quale ultima cura l'aggiornamento dei programmi *software* di ciascuna macchina (inclusi anche i *software antivirus* e *firewall*) e monitora anche le scadenze delle licenze *software* provvedendo, quando necessario - e sempre su autorizzazione della Società - al rinnovo delle stesse.

C) Monitoraggio e controllo della rete informatica interna

Periodicamente la Società provvede ad effettuare verifiche a campione finalizzate ad accertare il contenuto dei personal computer aziendali, con le seguenti modalità:

(i) i controlli vengono svolti dall'addetto alle funzionalità informatiche della Società, alla presenza del Responsabile delle Risorse Umane;
(ii) le verifiche avvengono in ogni caso alla presenza del lavoratore interessato, a

ciò previamente avvisato del controllo in corso;

(iii) chiedendo al lavoratore di accedere al pc per il tramite della *password* in dotazione, nonché alle singole *directory* contenute nel disco rigido ed ai relativi *files* ivi salvati, al fine di verificare la presenza di solo materiale *software* regolarmente licenziato ed autorizzato dalla Società e la conseguente assenza di materiale non consentito;

(iv) redigendo, all'esito del controllo, apposito verbale attestante le operazioni di verifica effettuate, da far sottoscrivere al lavoratore per presa visione e conferma del suo contenuto.

D) Utilizzo delle banche dati e norme di limitazione della loro circolazione all'esterno dell'azienda

Nel caso in cui la Società utilizzi proprie demo dimostrative contenenti applicazioni, dati e materiali predisposti dalla Società medesima per altri clienti, la dimostrazione dovrà essere effettuata a mezzo di presentazioni neutre, in alcun modo riconducibili o riferibili per aspetto, fatti e dati a detti clienti o soggetti.

E) Formazione del personale

La Società adotta adeguati programmi di formazione e sensibilizzazione del personale ritenuto esposto al rischio di commissione di delitti in materia di diritto d'autore.

Segnala a tale personale la lista dei reati con le relative fattispecie e le sanzioni che possono essere irrogate.

Attua una politica di sensibilizzazione di tutti gli utenti alla sicurezza informatica.

In particolare, il personale viene sensibilizzato ad evitare i seguenti comportamenti:

- utilizzare *software* senza possedere una valida licenza d'uso;
- copiare dati e/o programmi se non specificatamente autorizzati dal responsabile dei sistemi informativi ove presente o dalla Direzione Aziendale;
- esportare, con qualsivoglia strumento, i dati aziendali contenuti nei sistemi

informativi;

- possedere, duplicare, riprodurre o diffondere illegittimamente con qualsiasi mezzo (anche *software*), opere musicali, cinematografiche, audiovisive o letterarie e comunque opere tutelate dal diritto d'autore;
- scaricare programmi per elaboratore senza esplicita autorizzazione dal responsabile dei sistemi informativi.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nel presente Allegato.

Il presente Allegato e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale del Modello, al fine di garantire il raggiungimento delle finalità dallo stesso preposte.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO N

REATI AMBIENTALI

(Art. 25-undecies)

(Articolo inserito dall'art. 2, comma 2 del D.Lgs. 7 luglio 2011 n. 121)

1. REATI PRESUPPOSTO

Il D.Lgs. 7 luglio 2011, n. 121, "*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 introdotto nel D.Lgs. 231/01 il nuovo art. 25-*undecies* che estende a società ed enti la responsabilità per i reati ambientali.

Il provvedimento è entrato in vigore a far tempo dal 16 agosto 2011.

Ai sensi della normativa sopra citata, i reati che possono determinare la responsabilità della Società sono i seguenti:

- *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.);
- *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 commi 2, 3, 5, 11, 13 del D.Lgs. 3 aprile 2006, n. 152);
- *attività di gestione di rifiuti non autorizzata* (art. 256 commi 1, 3, 5, 6 del D.Lgs. 3 aprile 2006, n. 152);
- *inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee* (art. 257 commi 1 e 2 del D.Lgs. 3 aprile 2006, n. 152);
- *violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari* (art. 258 del D.Lgs. 3 aprile 2006, n. 152);

- *traffico illecito di rifiuti* (art. 259 del D.Lgs. 3 aprile 2006, n. 152);
- *attività organizzate per il traffico illecito dei rifiuti* (art. 260, commi 1 e 2 del D.Lgs. 3 aprile 2006, n. 152);
- *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 di rifiuti falso; missione o fraudolenta alterazione della copia cartacea della scheda SISTRI – area movimentazione nel trasporto di rifiuti* (art. 260–*bis*, commi 6, 7, 8 del D.Lgs. 3 aprile 2006, n. 152);
- *superamento dei valori limite di emissione che determina anche il superamento dei valori limite di qualità dell'aria* (art. 279, comma 5 del D.Lgs. 3 aprile 2006, n. 152);
- *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, 2, 3–*bis*, 6 della Legge 7 febbraio 1992, n. 150);
- *produzione, consumo, importazione, esportazione, detenzione e commercializzazione di sostanze lesive oltre i limiti previsti dalla normativa vigente* (art. 3 Legge 28 dicembre 1993, n. 549);
- *inquinamento doloso e colposo provocato da navi* (artt. 8 e 9 del D.Lgs. 6 novembre 2007, n. 202).

Successivamente, la Legge 22 maggio 2015 n. 68 recante le "*Disposizioni in materia di delitti contro l'ambiente*" - entrata in vigore il 29 maggio 2015 – oltre ad aver apportato sostanziali modifiche al D.Lgs. 152/2006 (integrandovi, ad esempio un'intera sezione dedicata alla disciplina sanzionatoria), ha inserito nel codice penale il nuovo Titolo VI-*bis* intitolato "*Dei delitti contro l'ambiente*" che prevede un lungo elenco di reati in materia ambientale.

Una buona parte di tali reati viene classificata dalla legge stessa come reati-presupposto atti a far scattare la responsabilità amministrativa dell'impresa, circostanza che ha determinato la conseguente modificazione ed integrazione dell'art. 25-*undecies* del D.Lgs. 231/01.

Il nuovo testo dell'art. 25-*undecies* D.Lgs. 231/01 prevede, pertanto, gli ulteriori seguenti reati-presupposto:

a) *Inquinamento ambientale* (art. 452 *bis* c.p.), che consiste nell'abusiva compromissione o deterioramento significativi e misurabili dello stato preesistente dell'acqua, dell'aria, del suolo e del sottosuolo, dell'ecosistema, della flora e della fauna. Per tale reato sono previste a carico dell'ente sanzioni pecuniarie da 250 a 600 quote;

b) *Disastro ambientale* (art. 452 *quater* c.p.), che si sostanzia:
   (i) nell'alterazione irreversibile dell'equilibrio di un ecosistema
   (ii) nell'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulta particolarmente oberosa e conseguibile solo con provvedimenti eccezionali
   (iii) nell'offesa della pubblica incolumità che viene determinata con riferimento:
   - all'estensione della compromissione o dei suoi efftti lesivi
   - al numero delle persone offese o esposte al pericolo.

   Per tale reato sono previste sanzioni pecuniarie da 400 a 800 quote;

c) *Delitti colposi contro l'ambiente* (art. 452 *quinquies* c.p.) che hanno ad oggetto i reati di cui alle precedenti fattispecie appena esaminate (artt. 452 *bis* e 452 *quater* c.p.), quando vengono commessi per colpa ovvero quando dalla commissione di detti reati deriva il pericolo di inquinamento ambientale o di disastro ambientale.
   Sono previste, per tali reati, sanzioni pecuniarie per l'ente da 200 a 500 quote;

d) *Traffico e abbandono di materiale ad alta radioattività* (art. 452 *sexies* c.p.) che consiste nella abusiva cessione, acquisto, ricezione, trasporto, importazione, esportazione, procura ad altri, detenzione, trasferimento, abbandono o nel disfacimento illegittimo di materiale ad alta radioattività. Per tale reato sono previste sanzioni pecuniarie da 250 a 600 quote;

e) *Circostanze aggravanti* (art. 452 *octies* c.p.) che prevedono:
   (i) l'associazione di cui all'art. 416 c.p. diretta, in via esclusiva o concorrente,

allo scopo di commettere taluno dei delitti in materia ambientale;

(ii) l'associazione di cui all'art. 416 *bis* c.p. finalizzata a commettere taluno dei reati in materia ambientale ovvero all'acquisizione della gestione o comunque del controllo di attività economiche, di concessioni, di autorizzazioni, di appalti o di servizi in materia ambientale;

(iii) l'associazione di cui fanno parte pubblici ufficiali o incaricati di un pubblico servizio che esercitano funzioni o svolgono servizi in materia ambientale.

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

I reati considerati nel presente Allegato riguardano attività illecite poste in essere intenzionalmente o con grave negligenza che provochino danni alla salute delle persone ovvero un danno rilevante alle componenti naturali dell'ambiente (ad esempio, un significativo deterioramento della qualità dell'aria, del suolo, delle acque, della fauna e della flora).

I rischi rilevati – tenuto conto anche delle nuove fattispecie di reati presupposto introdotte - sono quelli inerenti:

- allo smaltimento di rifiuti urbani, vale a dire non pericolosi;
- allo smaltimento di toner, stampanti e pc.

Per quanto la Società non svolga attività che hanno attinenza diretta con la gestione dei rifiuti o comporti rischi di inquinamento specifico particolarmente rilevanti, data la sensibilità dell'azienda per la tutela dell'ambiente, si ritiene comunque di prestare la massima attenzione ad adottare tutte le procedure necessarie a limitare i rischi di commissione colposa dei reati presupposto.

3. PROCEDURE GENERALI

Al fine di prevenire e tenere sotto controllo i principali rischi di reato ambientale, la Società effettua le seguenti attività:

1. analisi, con riferimento all'attività aziendale, dei potenziali impatti ambientali, diretti e indiretti, ivi inclusi i rischi in condizioni anomale e di emergenza, della loro significatività e delle misure necessarie al loro contenimento. Tale analisi deve avere cadenza periodica;
2. emanazione di procedure ed istruzioni di lavoro, o adeguamento ed adattamento di quelle esistenti, alle misure adottate all'esito delle predette analisi;
3. predisposizione di un'organizzazione aziendale adeguata a presidiare i rischi di commissione dei reati ambientali;
4. costante informazione e formazione dei lavoratori eventualmente maggiormente interessati dalle condotte di cui al presente Allegato;
5. costante vigilanza circa il rispetto delle procedure e delle istruzioni di lavoro da parte dei lavoratori;
6. costante monitoraggio della normativa applicabile e analisi e valutazione della costante conformità alla stessa dell'attività sociale;
7. riesame periodico delle analisi ambientali e della congruità delle procedure ed istruzioni di lavoro.

Il presente Allegato prevede, altresì, l'obbligo per la Società di:

1. ottenere, ove necessario tutte le eventuali autorizzazioni previste dalla legge in materia ambientale e provvedere al regolare periodico rinnovo delle stesse;
2. conservare la documentazione inerente agli iter autorizzativi, alle autorizzazioni, alle certificazioni e ogni documentazione inerente, nonché gli eventuali atti aggiuntivi o di modifica;
3. verificare la sussistenza dell'obbligo di effettuare le comunicazioni e di tenere i registri sui rifiuti;
4. compilare correttamente dette comunicazioni e registri;
5. provvedere allo smaltimento dei rifiuti ordinari rispettando la differenziazione indicata dalla normativa comunale applicabile;
6. affidare le attività di ritiro e smaltimento dei rifiuti speciali a soggetti di specchiata reputazione, controllandone costantemente l'attività;
7. verificare che le imprese alle quali è affidato lo smaltimento dei rifiuti siano in

possesso delle regolari autorizzazioni, di cui la Società conserverà copia;

8. verificare con cadenza periodica le emissioni in atmosfera e/o negli scarichi idrici da parte dei macchinari della Società che possano comportare un rischio di violazione delle disposizioni in materia ambientale.

4. PROCEDURE SPECIFICHE

A) Controllo delle emissioni in atmosfera

Benché il ciclo produttivo non comporti l'immissione in atmosfera di sostanze inquinanti e la Società effettui già periodici controlli sulle eventuali emissioni, anche in adempimento delle vigenti disposizioni di legge in materia di sicurezza sul lavoro, la Società stessa manifesta la propria sensibilità sulla tematica attinente alla tutela dell'ambiente, individuando a tal riguardo una specifica procedura da adottare nel caso in cui le eventuali emissioni in atmosfera dovessero superare i valori soglia tollerati dalla vigente normativa in materia. Detta procedura prevede in particolare di:

- verificare, in relazione alle disposizioni previste dalla legislazione vigente, la necessità di ottenere l'autorizzazione alle emissioni in atmosfera;
- provvedere all'ottenimento dell'autorizzazione nei tempi previsti dalla legislazione vigente ed attuare i controlli previsti nell'ambito dei disposti legislativi ad essi applicabili;
- mantenere e rinnovare entro i termini previsti dalla legislazione vigente le autorizzazioni alle emissioni;
- presentare una nuova domanda di autorizzazione in caso di modifica sostanziale di un impianto;
- verificare periodicamente la corretta attuazione dei precedenti adempimenti.

B) Attuazione degli adempimenti in merito alla gestione dei rifiuti

La Società adotta una procedura per la gestione dei propri rifiuti che preveda quanto segue:

- l'effettuazione di un'analisi iniziale del processo di produzione dei rifiuti che valuti la tipologia dei rifiuti prodotti, la modalità ed i tempi del loro smaltimento;
- l'effettuazione della caratterizzazione di base dei rifiuti, mediante attribuzione a ciascuno del corretto codice di legge, al fine di eseguire una corretta gestione degli stessi. Nel caso di dubbia attribuzione del codice, soprattutto ai fini dell'attribuzione delle caratteristiche di pericolosità, richiedere il supporto di consulenti o laboratori qualificati;
- il tempestivo aggiornamento dei registri di carico e scarico eventualmente richiesti dalla legge dei rifiuti all'atto della movimentazione e dello smaltimento degli stessi;
- la gestione del deposito temporaneo dei rifiuti in accordo con la legislazione vigente;
- la compilazione ed emissione dei formulari di identificazione dei rifiuti relativi al trasporto al di fuori dai locali della Società;
- la richiesta e la periodica verificazione delle autorizzazioni necessarie a tutti i soggetti coinvolti nelle varie fasi della gestione dei rifiuti (raccolta, trasporto, recupero, smaltimento);
- ove applicabile, la corretta tenuta e compilazione del Sistema di tracciabilità dei rifiuti (SISTRI);
- la verifica periodica della corretta attuazione dei precedenti adempimenti.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nel presente Allegato.

Il presente Allegato e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale del Modello, al fine di garantire il raggiungimento delle finalità dallo stesso preposte.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO O

IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

(Art. 25-duodecies)

(Articolo inserito dall'art. 2, comma 1 del D.Lgs. 16 luglio 2012 n. 109)

1. REATO PRESUPPOSTO

Il D.Lgs. 16 luglio 2012, n. 109 (pubblicato sulla G.U. n. 172 del 25 luglio 2012) ha ampliato il novero c.d. *reati presupposto* del D.Lgs. 231/01 inserendo il nuovo art. 25-*duodecies* sull' "*Impiego di cittadini di paesi terzi il cui soggiorno è irregolare"*.

L'art. 25-*duodecies* del D.Lgs. 231/01 è entrato in vigore il 9 agosto 2012 ed originariamente prevedeva come unica fattispecie di reato rilevante ai fini della responsabilità amministrativa degli enti ai sensi del D.Lgs. 231/01, esclusivamente l'impiego alle proprie dipendenze di lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso fosse scaduto e che non fosse stato rinnovato nei termini di legge o, ancora, che fosse stato revocato o annullato, qualora i lavoratori occupati irregolarmente fossero risultati, alternativamente:

- in numero superiore a tre; ovvero
- minori in età non lavorativa; oppure
- esposti a situazioni di grave pericolo, con riferimento alle prestazioni da svolgere ed alle condizioni di lavoro.

La norma è stata, peraltro, oggetto di recente integrazione ad opera della Legge 17 ottobre 2017 n. 161 (pubblicata in Gazz. Uff. il 4 novembre 2017, n. 258) in tema di "*Modifiche al codice delle leggi antimafia e delle misure di prevenzione, di cui al decreto legislativo 6 settembre 2011, n. 159, al codice penale e alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale e altre disposizioni. Delega al Governo per la tutela del lavoro nelle aziende sequestrate e confiscate*", che ha comportato l'introduzione di ulteriori fattispecie di reato

perseguibili.

L'articolo, pertanto, attualmente recita:
«*D.Lgs. 231/10, art. 25-duodecies - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare:*

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

1-bis. In relazione alla commissione dei delitti di cui all'articolo 12, commi 3, 3-bis e 3-ter, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni, si applica all'ente la sanzione pecuniaria da quattrocento a mille quote.

1-ter. In relazione alla commissione dei delitti di cui all'articolo 12, comma 5, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni, si applica all'ente la sanzione pecuniaria da cento a duecento quote.

1-quater. Nei casi di condanna per i delitti di cui ai commi 1-bis e 1-ter del presente articolo, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a un anno».

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

I reati considerati nel presente Allegato riguardano pertanto:

a) L'ente che occupa 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, ovvero è stato revocato o annullato.
   In tale ipotesi, l'ente è soggetto, in applicazione del D.Lgs. 231/01, ad una sanzione pecuniaria da 100 a 200 quote, per un massimo di Euro 150.000,00, se i lavoratori occupati sono (circostanze alternative tra di loro):
   - in numero superiore a tre;
   - minori in età non lavorativa;
   - esposti a situazioni di grave pericolo, con riferimento alle prestazioni da

svolgere ed alle condizioni di lavoro.

b) L'ente che promuove, dirige, organizza, finanzia o effettua il trasporto di stranieri nel territorio dello Stato ovvero compie altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente, nel caso in cui:

(i) il fatto riguarda l'ingresso o la permanenza illegale nel territorio dello Stato di cinque o più persone;
(ii) la persona trasportata è stata esposta a pericolo per la sua vita o per la sua incolumità per procurarne l'ingresso o la permanenza illegale;
(iii) la persona trasportata è stata sottoposta a trattamento inumano o degradante per procurarne l'ingresso o la permanenza illegale;
(iv) il fatto è commesso da tre o più persone in concorso tra loro o utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti;
(v) gli autori del fatto hanno la disponibilità di armi o materie esplodenti;
(vi) si ricorre a due o più delle ipotesi di cui ai precedenti punti.

Nelle suddette ipotesi, l'ente è soggetto ad una sanzione pecuniaria da 400 a 1.000 quote, oltre alle sanzioni interdittive previste dall'art. 9, co. 2 D.Lgs. 231/01, per una durata non inferiore a 1 anno.

c) I fatti di cui ai punti a) e b) sopra elencati commessi:

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

In tali ipotesi l'ente è soggetto ad una sanzione pecuniaria da 400 a 1.000 quote, oltre alle sanzioni interdittive previste dall'art. 9, co. 2 D.Lgs. 231/01, per una

durata non inferiore a 1 anno.

d) L'ente infine che, al fine di trarre un ingiusto profitto dalla condizione di illegalità dello straniero, favorisce la permanenza di quest'ultimo nel territorio dello Stato in violazione delle norme previste dal D.Lgs. 25 luglio 1998, n. 286 "*Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero*".
In tal caso, all'ente viene comminata la sanzione pecuniaria da 100 a 200 quote, oltre alle sanzioni interdittive previste dall'art. 9, co. 2 D.Lgs. 231/01, per una durata non inferiore a 1 anno.

Sulla scorta della documentazione raccolta e dell'analisi dei processi correlati allo svolgimento della propria attività, emerge che la Società non impiega cittadini di paesi terzi.

Ad ogni buon conto, si ritiene opportuno individuare già da ora le linee e procedure da adottare nel caso in cui la Società dovesse, in futuro, avvalersi di manodopera straniera.

In merito, la Società ha individuato specifiche procedure di controllo sulla legittimità della eventuale presenza di propri lavoratori stranieri in Italia, che vengono descritte nel paragrafo 4 che segue.

I suddetti controlli dovranno essere, in primo luogo, svolti ad opera di agenzie adeguatamente accreditate e specializzate nel settore della somministrazione di forza lavorativa alle quali la Società dovesse affidarsi per la selezione del personale. Tali attività andranno effettuate in coordinamento con il Responsabile delle Risorse Umane della Società e dovranno coinvolgere anche i dipendenti di aziende terze che operano nell'area dello Statuto della Società in appalto, ovvero in subappalto.

3. PROCEDURE GENERALI

Per quanto, nel caso della Società, il rischio di commissione dei reati presi in considerazione dall'art. 25-*duodecies* D.Lgs. 231/01 sia, pertanto, assolutamente

remoto, è in ogni caso fatto divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato richiamate all'art. 25-*duodecies* del D.Lgs. 231/01;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti i quali, sebbene risultino tali da non costituire di per sé reato, possano tendenzialmente diventarlo.

4. PROCEDURE SPECIFICHE

Al fine di scongiurare la commissione del reato in esame, ad integrazione delle procedure interne già esistenti, la Società adotta una procedura che prevede quanto segue:

- la selezione del personale viene affidata ad agenzie adeguatamente accreditate e specializzate nel settore della somministrazione di forza lavoro;
- all'atto dell'assunzione di soggetti stranieri per i quali sia richiesto, ai fini della permanenza nel territorio italiano, il permesso di soggiorno, viene domandata, acquisita e conservata copia dello stesso permesso, che deve essere esibito in originale;
- nella stessa occasione, l'interessato dichiara per iscritto di essere in possesso di permesso di soggiorno in corso di validità, o per il quale sia stato richiesto, nei termini di legge, il rinnovo (in questa ipotesi esibendo in originale ed allegando in copia tale ultima richiesta);
- la Società si dota di una procedura in grado di avvisare il responsabile se un permesso di soggiorno, in costanza di rapporto lavorativo in essere, viene a scadenza, così che la Società si possa attivare per accertarsi del suo tempestivo rinnovo;

– analoga procedura viene eseguita dalla Società nelle ipotesi in cui la stessa opera quale committente di appaltatori (ed anche nei confronti dei subappaltatori) che non siano in grado di produrre la dichiarazione di regolarità contributiva dei documenti.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nel presente Allegato.

Il presente Allegato e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale del Modello, al fine di garantire il raggiungimento delle finalità dallo stesso preposte.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO P

RAZZISMO E XENOFOBIA

(Art. 25-terdecies)

(Articolo inserito dall'articolo 5, comma 2, della Legge 20 novembre 2017, n. 167)

1. REATO PRESUPPOSTO

La Legge 20 novembre 2017 n. 167 (pubblicata in Gazzetta Ufficiale in data 27 novembre 2017, n. 277 ed entrata in vigore a far data dal 12 dicembre 2017) recante le "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017*", ha ulteriormente ampliato l'elenco dei reati presupposto previsti e disciplinati dal D.Lgs. 231/01, aggiungendo il nuovo art. 25-*terdecies* in materia di reati di "*razzismo e xenofobia*" che, nello specifico, stabilisce quanto segue:

«*1. In relazione alla commissione dei delitti di cui all'articolo 3, comma 3-bis, della legge 13 ottobre 1975, n. 654, si applica all'ente la sanzione pecuniaria da duecento a ottocento quote.*

2. Nei casi di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a un anno.

3. Se l'ente o una sua unità organizzativa è stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei delitti indicati nel comma 1, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'articolo 16, comma 3».

Dall'esame del testo normativo sopra riportato, viene pertanto in evidenza che la condotta penalmente rilevante è da individuarsi nelle attività di "*propaganda, istigazione o incitamento al razzismo*" fondate «*…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» (Art. 3, comma 3-*bis* Legge 654/1975 di "*Ratifica ed esecuzione della convenzione internazionale sull'eliminazione di tutte le forme di discriminazione razziale, aperta alla firma a New York il 7 marzo 1966 - Convenzione di New York - Eliminazione della discriminazione razziale*).

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Data la specificità dei delitti in questione, gli stessi sono astrattamente configurabili in capo a enti che svolgono attività informazione e stampa (ad es. testate editoriali, imprese radiotelevisive, società che gestiscono siti web e blog, etc.).

Fermo che la Società condanna ogni forma di discriminazione per motivi razziali, etnici, nazionali ovvero religiosi, sulla scorta della documentazione raccolta e dell'analisi dei processi correlati allo svolgimento della propria attività, emerge che la Società stessa non svolge attività che prevede la prestazione di servizi al pubblico di natura mediatica e, pertanto, non si ritiene siano ravvisabili rischi specifici con riferimento al reato trattato nel presente Allegato.

Ad ogni buon conto, al fine di eliminare alla fonte ogni eventuale rischio in materia, anche con riferimento all'eventuale organizzazione, associazione, movimento o gruppo finalizzati all'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi, si rimanda espressamente alla procedura individuata dalla Società in materia di "*Reati con finalità di terrorismo o di eversione dell'ordine democratico*" che sono pertanto qui da intendersi integralmente richiamate e trascritte.

A.M.R.A. S.p.A.
Via Sant'Ambrogio, 23/25 - 20846 Macherio (MB) - Italia
Tel. 0039 039.245.75.45 – Fax 0039 039.481.561
E-mail: info@amra-chauvin-arnoux.it Internet: www. amra-chauvin-arnoux.it

ALLEGATO Q

WHISTLEBLOWING

1. INTRODUZIONE

Nel linguaggio dell'economia e del diritto, con il termine "*whistleblowing*" si indica l'iniziativa, da parte di qualsiasi risorsa umana impegnata nell'organizzazione dell'ente, o collettivo, che segnala all'organo dirigente, ovvero a quello di controllo, o addirittura all'autorità giudiziaria, una possibile frode, un pericolo o altro rischio, che è in grado di produrre un danno ai colleghi, agli *stakeholders* (i c.d. portatori di interessi) o allo stesso ente.

Il *whistleblower* (letteralmente, il "soffiatore di fischietto") è, in sostanza colui che denuncia o segnala alle autorità o a specifici soggetti all'interno dell'azienda – deputati a ricevere tali segnalazioni – l'esistenza di attività illecite o fraudolente all'interno della propria sede lavorativa.

L'art. 6, comma 1, lett. d) del D.Lgs. 231/2001 stabilisce che i modelli di organizzazione, gestione e controllo adottati dall'ente ai fini della esenzione dalla responsabilità amministrativa derivante dalla commissione dei reati presupposto da parte dei propri dipendenti, devono «*prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli*».

Ciò si traduce nell'obbligo in capo a ciascun soggetto che opera alle dipendenze dell'ente, di portare a conoscenza dell'Organismo di Vigilanza le eventuali violazioni delle disposizioni e delle procedure contenute nel modello organizzativo che vengano commesse da colleghi di lavoro (ovvero da parte dei propri superiori gerarchici), che possano quindi concretizzarsi nella commissione di un reato presupposto.

Il soggetto che effettua la segnalazione di illeciti perpetrati dai propri colleghi di lavoro, se da un lato ottempera ad un dovere di "collaborazione" con l'Organismo di Vigilanza preposto alla verifica dell'effettivo funzionamento ed osservanza dei

modelli organizzativi, dall'altro lato si espone al rischio di eventuale ritorsione da parte dell'ente stesso, dei colleghi medesimi ovvero anche da altre fonti, spesso accompagnato alla frustrazione nel veder eventualmente vanificata la propria iniziativa.

Sorge, pertanto, il problema di "*come tutelare il soggetto che effettua la segnalazione di illeciti all'interno del contesto lavorativo*".

Il 29 dicembre 2017 è entrata in vigore la Legge 30 novembre 2017 n. 179 (pubblicata in Gazzetta Ufficiale il 14 dicembre 2017, n. 291) recante le "*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*" che ha introdotto, per la prima volta nell'ordinamento italiano, una disciplina organica nazionale in materia di *whistleblowing*.

Il testo normativo ha apportato modifiche sostanziali al sopra citato art. 6 del D.Lgs. 231/2001, prevedendo l'inserimento, dopo il comma 2 della norma di cui sopra, dei seguenti:

a) comma 2-*bis* ove viene stabilito che i modelli organizzativi devono prevedere:

   (i) l'individuazione di uno o più canali che consentano ai soggetti indicati nell'art. 5, comma 1, lettere *a)* e *b)* (e cioè i c.d. "soggetti apicali" e le persone sottoposte alla direzione o alla vigilanza degli stessi) di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del D.Lgs. 231/01 e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; i suddetti canali devono garantire la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;

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

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

(iv) l'adozione di sanzioni disciplinari 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.

b) Comma 2-*ter*, ove viene stabilito che l'eventuale adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2-*bis* sopra descritto, possa essere denunciata all'Ispettorato nazionale del lavoro sia da parte del soggetto segnalante stesso, sia da parte dell'organizzazione sindacale indicata dal medesimo.

c) Comma 2-*quater*, il quale sanziona con la nullità:

(i) il licenziamento ritorsivo o discriminatorio del soggetto segnalante;

(ii) il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante;

ponendo in capo al datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, l'onere di dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

La Società pertanto, nell'obiettivo di dare concreta esecuzione alle tematiche affrontate dal D.Lgs. 231/01, ritiene opportuno e quanto meno doveroso predisporre la presente procedura da adottare al fine di portare a conoscenza della Società medesima, degli Organi di Controllo ovvero dell'autorità giudiziaria competente eventuali segnalazioni di attività illecite o fraudolente commesse da chiunque all'interno ed in occasione dell'attività lavorativa.

2. OBIETTIVI DEL PRESENTE ALLEGATO

Il presente Allegato definisce e regola il processo di ricezione, analisi e trattamento delle Segnalazioni (come nel seguito definite) da chiunque, terzi o dipendenti, inviate o trasmesse, anche in forma confidenziale o anonima.

Il presente allegato risponde agli adempimenti previsti dal Modello di Organizzazione, Gestione e Controllo adottato dalla Società *ex* D.Lgs. 231/01.

3. AMBITO DI APPLICAZIONE

Le disposizioni contenute nel presente allegato si applicano a tutto il personale della Società.

La Società garantisce che verranno soddisfatti gli standard indicati nel presente Allegato, adottando e mantenendo un adeguato sistema di controllo in coerenza con i requisiti stabiliti dalla vigente normativa.

La gestione delle Segnalazioni ed il relativo trattamento dei dati ai fini *privacy* è effettuata nel rispetto delle vigenti disposizioni di legge applicabili, ivi inclusi, in particolare, i principi di necessità, proporzionalità e liceità del trattamento così come previsti dal Decreto Legislativo 30 giugno 2003, n. 196 e sue successive modifiche ed integrazioni, nonché dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati), nonché, in coerenza con quanto previsto al riguardo nell'ambito delle specifiche procedure interne.

La Società garantisce, altresì, che verranno in ogni caso rispettate sempre le istruzioni impartite dal Titolare del trattamento, assicurando le esigenze di riservatezza sottese allo svolgimento delle attività istruttorie.

4. GLOSSARIO

Ai sensi e per gli effetti del presente Allegato, si intende per:

Codice Privacy: il Decreto Legislativo 30 giugno 2003, n. 196 e sue successive modifiche ed integrazioni.

Regolamento Generale sulla Protezione dei Dati: il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE

Collegio Sindacale: il Collegio Sindacale di AMRA S.p.A.

Organismo di Vigilanza: l'Organismo di Vigilanza di cui all'articolo 6 del Decreto Legislativo n. 231 del 2001, istituito presso AMRA S.p.A.

Segnalante: il soggetto che effettua la segnalazione utilizzando la procedura prevista nel presente Allegato

Segnalato/a: il soggetto o l'ente in relazione nei confronti dei quali viene avviata una procedura di segnalazione ai sensi del presente Allegato

Segnalazione/i: qualsiasi comunicazione avente ad oggetto comportamenti (di qualsivoglia natura, anche meramente omissivi) riferibili al personale di AMRA S.p.A. o a Terzi (come nel seguito definiti) posti in essere con violazione: *(i)* del Modello Organizzativo adottato da AMRA S.p.A., *(ii)* del Codice Etico, *(iii)* di leggi o regolamenti o provvedimenti dell'autorità o normative interne o comunque idonei ad arrecare danno o pregiudizio, anche solo d'immagine, a AMRA S.p.A.
Non sono trattate come Segnalazioni ai fini del presente Allegato:

- le carenze già individuate e documentate dalle strutture aziendali nell'ambito dei relativi controlli interni;
- le lamentele relative ad attività di natura commerciale (es. reclami per bollette, fatturazione, ecc.);
- le comunicazioni riguardanti circostanze/fatti già noti e oggetto di contenziosi (giurisdizionali o amministrativi) pendenti tra AMRA S.p.A. e i Terzi.

Segnalazione Anonima: Segnalazione in cui le generalità del segnalante non siano esplicitate, né siano individuabili in maniera univoca.

Segnalazione in Malafede: Segnalazione che dagli esiti della fase istruttoria si rilevi priva di fondamento sulla base di elementi oggettivi comprovanti la malafede del Segnalante, fatta allo scopo di arrecare un danno ingiusto alla persona e/o società segnalata.

Segnalazione/i Circostanziata/e: Segnalazione in cui la narrazione da parte dell'autore, di fatti, eventi o circostanze che costituiscono gli elementi fondanti dell'asserito illecito (ad esempio, tipologia di illecito commesso, periodo di riferimento, valore, cause e finalità dell'illecito, società/aree/persone/unità/enti interessati o coinvolti, anomalia sul sistema di controllo interno, ecc.) è effettuata con un grado di dettaglio sufficiente a consentire, almeno astrattamente, ai competenti organi aziendali di identificare elementi utili o decisivi ai fini della verifica della fondatezza della Segnalazione stessa.
Le Segnalazioni Circostanziate si distinguono a loro volta in:

- *Segnalazioni Circostanziate Verificabili*: qualora, considerati i contenuti della Segnalazione Circostanziata, sia possibile in concreto, sulla base degli strumenti di indagine a disposizione, compiere verifiche sulla fondatezza o meno dei fatti o circostanze segnalati;
- *Segnalazioni Circostanziate Non Verificabili*: qualora, considerati i contenuti della Segnalazione Circostanziata, non sia possibile, sulla base degli strumenti di indagine a disposizione, compiere verifiche sulla fondatezza o meno dei fatti o circostanze segnalati e pertanto procedere alla fase di accertamento disciplinata al successivo cap. 5 "*Modalità Operative*", par. "*B) Istruttoria*", punto "*2) Accertamento*".

Terzi: i soggetti che si trovano in relazioni d'interesse con AMRA S.p.A. (es. *business partner*, clienti, fornitori, società di revisione, consulenti, collaboratori e, in generale, gli *stakeholders*).

5. PRINCIPI GENERALI

I principi generali con riferimento al processo di gestione delle Segnalazioni sono i seguenti:

a) *Indipendenza e professionalità nelle attività di istruzione delle Segnalazioni*: le attività di verifica, istruzione e trattazione delle Segnalazioni verranno svolte dai competenti organi assicurando il mantenimento delle necessarie condizioni di indipendenza e la dovuta obiettività, competenza e diligenza professionali.

b) *Garanzia di riservatezza e anonimato*: i soggetti che, ai sensi del presente documento, ricevano una Segnalazione e/o che siano coinvolte, a qualsivoglia titolo, nell'istruzione e trattazione della stessa, sono tenuti a garantire la massima riservatezza sui soggetti e sui fatti segnalati, utilizzando, a tal fine, criteri e modalità di comunicazione idonei a tutelare l'identità e l'onorabilità delle persone menzionate nelle Segnalazioni, nonché l'anonimato dei Segnalanti, affinché chi effettua la segnalazione non sia soggetto ad alcuna forma di ritorsione, evitando in ogni caso la comunicazione dei dati acquisiti a soggetti estranei al processo di istruzione e trattazione delle Segnalazioni disciplinato nel presente allegato, nei limiti e compatibilmente con le vigenti disposizioni di legge.
   Fermo restando ciò, la comunicazione di tali informazioni ai fini dell'istruzione e trattazione della Segnalazione, è consentita:

   - nei confronti dei seguenti soggetti/enti:
     (i) Organismo di Vigilanza;
     (ii) Collegio Sindacale;

   - nei casi in cui la loro conoscenza sia indispensabile per la comprensione dei fatti segnalati e/o per la conduzione delle relative attività di istruzione e/o trattazione;

   - ai fini del reporting verso i relativi soggetti destinatari.

c) *Protezione dalle Segnalazioni in Malafede*: AMRA S.p.A. auspica che il proprio personale, ad ogni livello, collabori a mantenere in azienda un clima di reciproco rispetto della dignità, dell'onore e della reputazione di ciascuno.

AMRA S.p.A. interverrà per impedire atteggiamenti interpersonali ingiuriosi, discriminatori o diffamatori. Pertanto AMRA S.p.A. garantisce adeguata protezione dalle Segnalazioni in Malafede, censurando simili condotte e informando i soggetti/società oggetto di Segnalazione di cui verrà accertata la "malafede".

6. MODALITÀ OPERATIVE

Le attività del processo di gestione delle Segnalazioni sono le seguenti:

A) RICEZIONE

Le Segnalazioni possono essere inviate all'Organismo di Vigilanza di AMRA S.p.A. a mezzo posta al seguente indirizzo: **Organismo di Vigilanza di AMRA S.p.A. c/o AMRA S.p.A., Via S. Ambrogio n. 23/25, 20050 Bareggia di Macherio (MI)**.

Le ulteriori modalità di invio, anche a mezzo posta elettronica, verranno stabilite di comune accordo con l'ODV e saranno rese note ai dipendenti ed ai terzi interessati a mezzo circolare che l'Azienda curerà di distribuire nei tempi più solleciti e comunque in quelli tecnici strettamente necessari.

Verranno, altresì, messi a disposizione presso i locali della Società strumenti alternativi per la raccolta delle Segnalazioni (ad es. cassette per la posta dedicata), per quei soggetti che non abbiano accesso alle postazioni informatiche aziendali e non dispongano neppure di strumenti informatici propri.

In tal caso, le Segnalazioni dovranno essere previamente inserite in buste bianche opportunamente sigillate, prive di qualsiasi segno distintivo o di riconoscimento dal quale si possa risalire all'identità del soggetto Segnalante.

Le buste verranno recapitate all'Organismo di Vigilanza a cura di AMRA S.p.A.

La Società garantisce che nessuna delle buste di cui sopra verrà aperta e/o ispezionata da AMRA S.p.A. stessa, dal personale incaricato della raccolta e recapito delle Segnalazioni cartacee ovvero da parte di terzi non autorizzati, ad esclusione del solo

Organismo di Vigilanza al quale la stessa è indirizzata e che, pertanto, il contenuto delle Segnalazioni resterà inviolato.

Ricevuta la Segnalazione, l'Organismo di Vigilanza informa il Segnalante, con le modalità da quest'ultimo indicate nella Segnalazione stessa, circa:

(i) l'avvenuta presa in carico della Segnalazione;
(ii) la possibilità che il Segnalante potrà essere ricontattato per l'eventuale acquisizione di elementi utili alla fase istruttoria; nonché
(iii) la possibilità di inviare ulteriori informazioni/elementi di cui verrà a conoscenza, ai fini della integrazione e/o aggiornamento dei fatti oggetto della Segnalazione iniziale;

La Società garantisce che l'identità tanto del Segnalante quanto del Segnalato, il contenuto della Segnalazione e/o ogni altra informazione relativa a fatti connessi, direttamente e/o indirettamente con la Segnalazione stessa, verranno trattati dall'Organismo di Vigilanza ai soli fini della istruzione e trattazione della Segnalazione medesima, con la più assoluta riservatezza, e che le informazioni medesime non verranno in ogni caso trasmesse a terzi senza la preventiva autorizzazione scritta del Segnalante, fatto salvo quando ciò sia richiesto dalla vigente normativa e/o dalle autorità competenti.

Il personale di AMRA S.p.A. che eventualmente riceva una Segnalazione transitata al di fuori dei canali sopra descritti, è tenuto a trasmetterla senza indugio all'Organismo di Vigilanza ovvero a farla in ogni caso recapitare a quest'ultimo con le modalità sopra descritte, nel rispetto dei criteri di massima riservatezza e con modalità idonee a tutelare il Segnalante e l'identità e l'onorabilità dei soggetti segnalati, senza pregiudizio per l'efficacia delle successive attività di accertamento.

Fatto salvo che per l'Organismo di Vigilanza ai soli fini della conduzione delle attività di indagine e controllo in merito alle circostanze segnalate con la Segnalazione, è sempre fatto divieto assoluto a chiunque entri in possesso di una Segnalazione ricevuta da terzi soggetti, di prendere visione del suo contenuto.

L'eventuale violazione delle disposizioni di cui sopra, nonché di quelle contenute nel presente Allegato, comporterà l'irrogazione in capo al soggetto che ha commesso la violazione delle sanzioni previste dal vigente contratto collettivo nazionale di lavoro applicato dalla Società.

B) ISTRUTTORIA

Ricevuta la Segnalazione, l'Organismo di Vigilanza effettuerà tutte le opportune verifiche sui fatti segnalati verificabili, attraverso una o più delle seguenti attività, garantendo che tali fasi verranno svolte nel minor tempo possibile e, comunque, nel rispetto dei principi di obiettività, competenza e diligenza professionale:

1) Verifica preliminare

L'obiettivo della verifica preliminare è di procedere alla classificazione delle comunicazioni ricevute al fine di identificare le Segnalazioni da trattare in applicazione del presente strumento normativo, nonché valutare la presenza dei presupposti necessari all'avvio della successiva fase di accertamento.

A tal fine, l'Organismo di Vigilanza che ha ricevuto e preso in carico la Segnalazione attraverso i canali di comunicazione di cui al precedente paragrafo "*A) Ricezione*":

1) protocolla la Segnalazione ricevuta con le modalità indicate al successivo Cap. 10 "*Controlli, archiviazione e conservazione della documentazione, tracciabilità*";

2) esamina le comunicazioni ricevute per identificare le Segnalazioni rientranti nell'ambito di applicazione del presente Allegato;

3) individua tra le Segnalazioni Circostanziate quelle qualificabili come Segnalazioni Circostanziate Verificabili e Segnalazioni Circostanziate Non Verificabili;

4) qualora ritenuto utile ai fini dell'integrazione delle verifiche preliminari, conduce verifiche anche presso le strutture aziendali interessate o le persone coinvolte;

5) propone l'archiviazione:

(i) delle Segnalazioni non qualificabili come Segnalazioni Circostanziate;

(ii) delle Segnalazioni palesemente infondate e delle Segnalazioni in Malafede;

(iii) delle Segnalazioni contenenti fatti che, in passato, sono già stati oggetto di specifiche attività di istruttoria all'esito delle quali è stata disposta l'archiviazione della pratica, nel caso in cui dalle verifiche preliminari ulteriormente svolte non emergano nuove informazioni tali da rendere necessarie ulteriori attività di verifica;

(iv) delle Segnalazioni Circostanziate Non Verificabili per le quali non ritiene necessario avviare la fase di accertamento di cui al successivo par. "*2) Accertamento*", valutando – ove emergesse la necessità di aggiornare, modificare e/o implementare alcune delle procedure interne della Società riferite alle funzioni e/o reparti interessati dalla segnalazione medesima - l'eventuale invio all'Organo di Amministrazione della Società della Segnalazione stessa unitamente alle raccomandazioni sulle eventuali iniziative da intraprendere;

(v) delle Segnalazioni Circostanziate Verificabili per le quali, alla luce degli esiti delle verifiche preliminari condotte ai sensi del precedente punto 4), non valuta necessario l'avvio della successiva fase di accertamento di cui al par. "*2) Accertamento*" che segue;

6) trasmette le comunicazioni ricevute non identificate come Segnalazioni alle funzioni aziendali di AMRA S.p.A. competenti a riceverle ed a trattarle sulla base delle vigenti normative di riferimento (ad es. segnalazioni relative ad attività di natura commerciale, come eventuali reclami per bollette, fatturazione, ecc.);

7) comunica la proposta di archiviazione di cui al punto 5) che precede al Collegio Sindacale ai fini dell'esame ed approvazione della stessa con le modalità di cui al successivo par. "*3) Archiviazione*";

8) con riferimento alle Segnalazioni Circostanziate Verificabili che residuassero all'esito del precedente punto 5)*(v)*, dà informativa dell'apertura dei fascicoli relativi alle Segnalazioni alle funzioni competenti di AMRA S.p.A.

Le attività istruttorie afferenti a fatti segnalati sui quali sia nota l'esistenza di indagini in corso da parte di pubbliche autorità (ad esempio, autorità giudiziarie, ordinarie e speciali, organi amministrativi ed *authority* indipendenti investiti di funzioni di vigilanza e controllo), nonché la trasmissione alle medesime autorità di rapporti o relazioni di *audit*, sono soggette a previa valutazione da parte dell'Organismo di Vigilanza che potrà disporne l'eventuale sospensione, nei limiti e compatibilmente con la vigente normativa.

2) <u>Accertamento</u>

L'obiettivo delle attività di accertamento sulle Segnalazioni è di procedere ad accertamenti, analisi e valutazioni specifiche circa la fondatezza o meno dei fatti segnalati, nonché di formulare eventuali raccomandazioni in merito all'adozione delle necessarie azioni correttive sulle aree e sui processi aziendali interessati dalla Segnalazione volte a rafforzarne il sistema di controllo interno da parte della Società e la gestione dei relativi rischi, a fronte delle quali i responsabili aziendali a ciò preposti redigono uno specifico piano di azione.

A tal fine, l'Organismo di Vigilanza svolge le necessarie verifiche:

(i) direttamente acquisendo gli elementi informativi necessari alle valutazioni dalle funzioni aziendali interessate; ovvero

(ii) tramite le competenti funzioni direttive di AMRA S.p.A., interessando un livello organizzativo che garantisca in ogni caso indipendenza di giudizio; ovvero

(iii) tramite il Responsabile del Servizio di Prevenzione e Protezione se la Segnalazione attiene a temi di salute, sicurezza, ambiente e incolumità pubblica.

Le verifiche di cui ai precedenti punti *(ii)* e *(iii)* verranno coordinate eventualmente anche avvalendosi delle funzioni/uffici competenti della Società i quali invieranno all'Organismo di Vigilanza una nota conclusiva delle attività svolte, unitamente alla documentazione di supporto.

3) Archiviazione

Al termine della fase di Accertamento, l'Organismo di Vigilanza trasmette la proposta di archiviazione al Collegio Sindacale per l'esame da parte dello stesso e la sua approvazione.

Ricevuta la proposta di archiviazione, il Collegio sindacale:

a) approva la proposta di archiviazione; ovvero
b) ove lo ritenga necessario, richiede all'Organismo di Vigilanza di effettuare ulteriori accertamenti, nel quale ultimo caso si procederà secondo la procedura di "*Accertamento*" di cui al precedente paragrafo 2).

7. MONITORAGGIO AZIONI CORRETTIVE

Nel caso in cui all'esito delle fasi dell'istruttoria emerga la necessità di apportare azioni correttive sul sistema di controllo interno della Società e la gestione dei relativi rischi, è responsabilità della Società redigere un piano delle azioni correttive per la rimozione delle criticità rilevate.
L'Organismo di Vigilanza ne monitora il relativo stato di attuazione.

8. REPORTING

All'esito di ciascun procedimento di istruttoria inerente una Segnalazione ricevuta, L'Organismo di Vigilanza trasmette all'Organo di Amministrazione della Società, un *report* riepilogativo della Segnalazione ricevuta, contenente la descrizione delle attività svolte e delle ragioni che hanno portato allo specifico esito della procedura stessa.

9. SANZIONI DISCIPLINARI E ALTRI PROVVEDIMENTI

Ogni comportamento illecito, ascrivibile al personale di AMRA S.p.A., che dovesse emergere a seguito delle attività di verifica delle Segnalazioni condotte ai sensi del presente Allegato, secondo quanto previsto ai seguenti capoversi del presente paragrafo, verrà sanzionato secondo le disposizioni previste dal vigente contratto collettivo nazionale di lavoro applicato dalla Società.

Nel caso in cui dagli esiti della fase di istruttoria:

a) emergano Segnalazioni in Malafede da parte di propri dipendenti, la Società adotta le opportune azioni disciplinari nei confronti del Segnalante nel rispetto delle disposizioni previste dal vigente CCNL applicato dandone, nel contempo, notizia anche al soggetto e/o alla società Segnalati;

b) si evidenzino possibili gravi inadempimenti o illeciti a carico di fornitori della Società, la stessa ne darà immediata comunicazione agli organi amministrativi e/o di controllo dei suddetti soggetti, riservandosi ogni valutazione in merito ai profili inerenti l'eventuale risoluzione dei rapporti contrattuali in essere con detti soggetti, nonché – ove ne sussistessero i presupposti di legge – di informarne le competenti autorità giurisdizionali;

c) si evidenzino presunti comportamenti illeciti o irregolari da parte di uno o più dipendenti della Società, quest'ultima si riserva di valutare l'eventuale contestabilità sotto il profilo sanzionatorio disciplinare dei suddetti comportamenti in capo ai soggetti Segnalati e di adottare, all'esito dei procedimenti medesimi, le opportune azioni disciplinari nei confronti degli stessi, nel rispetto delle disposizioni previste dal vigente contratto collettivo applicato, nonché – se del caso ed ove vi siano i presupposti di legge – anche le eventuali azioni giudiziarie avanti alle competenti sedi giurisdizionali;

La Società prenderà in ogni caso adeguati provvedimenti disciplinari, secondo quanto disposto dal Modello 231 e dal CCNL applicato o dalle altre norme nazionali applicabili, nei confronti del proprio dipendente che:

(i) all'esito delle attività istruttorie relative alle Segnalazioni, risulti responsabile della violazione di norme di legge, delle disposizioni contenute nel Modello 231 e nel Codice Etico, nonché nel presente Allegato; ovvero

(ii) ometta volutamente di rilevare o riportare eventuali violazioni o minacci o adotti ritorsioni contro altri dipendenti di AMRA S.p.A. che riportano eventuali violazioni.

I provvedimenti disciplinari sono quelli espressamente previsti dal vigente Contratto Collettivo Nazionale di Lavoro applicato dalla Società e descritti nel Capitolo "*Sistema Disciplinare*" di cui al Modello 231 al quale si rimanda.

Le sanzioni saranno in ogni caso proporzionate all'entità ed alla gravità dei comportamenti illeciti che saranno accertati all'esito della procedura istruttoria sopra descritta, potendo giungere, compatibilmente con quanto previsto nel CCNL, sino alla risoluzione del rapporto di lavoro.

10. CONTROLLI, ARCHIVIAZIONE E CONSERVAZIONE DELLA DOCUMENTAZIONE, TRACCIABILITÀ

La Società garantisce che tanto l'Organismo di Vigilanza, quanto il Collegio Sindacale, nonché le unità e funzioni aziendali che verranno eventualmente coinvolte nelle attività disciplinate dal presente Allegato assicurano - ciascuno per quanto di propria competenza - la tracciabilità dei dati e delle informazioni acquisiti nel corso dell'istruttoria e provvedono alla conservazione ed archiviazione della documentazione prodotta, cartacea e/o elettronica, in modo da consentire la ricostruzione delle diverse fasi del processo stesso.

Al fine di garantire la gestione e la tracciabilità delle Segnalazioni e delle relative attività di istruttorie, l'Organismo di Vigilanza predispone e aggiorna un sistema dedicato alla gestione, monitoraggio e *reporting* delle Segnalazioni, nel quale registra i fascicoli relativi a ciascuna Segnalazione, assicurando l'archiviazione di tutta la relativa documentazione di supporto.

A tale scopo, viene garantita la conservazione presso l'Organismo di Vigilanza della documentazione originale delle Segnalazioni in appositi archivi cartacei/informatici, con adeguati standard di sicurezza/riservatezza.

I dati personali raccolti nell'ambito di una Segnalazione vengono conservati per il tempo strettamente necessario al loro trattamento, in coerenza con quanto disciplinato dalla vigente normativa in materia di protezione dei dati personali.

È tutelato, ai sensi della legge vigente e delle procedure aziendali in materia di *privacy*, il trattamento dei dati personali delle persone coinvolte e/o citate nelle Segnalazioni.