Modello di Organizzazione, Gestione e Controllo ai sensi del d.lgs. 231/2001

Iter di emissione			
Redatto da	**Ruolo**	**Data**	**Firma**
Verificato da	**Ruolo**	**Data**	**Firma**
Approvato da	**Ruolo**	**Data**	**Firma**

Storia del documento

Aggiornamenti e Revisioni		
	Oggetto	**Data**
1	Prima edizione del documento	15/02/2018
2	Revisione per introduzione processi e procedura Whistleblowing	02/01/2024
3	Revisione per aggiornamenti normativi e organizzativi	30/06/2025

Sommario

1. Finalità del documento

Le finalità del documento sono:

- Definire il Modello di Organizzazione, Gestione e Controllo (di seguito il "Modello") adottato dalla Mizar International Insurance Brokers S.r.l. (di seguito "Mizar") al fine di garantire condizioni di legalità, correttezza e trasparenza nello svolgimento della propria attività. Il Modello si affianca al Codice Etico e di Comportamento di Mizar ed ha la funzione di prevedere un sistema di procedure per prevenire la commissione dei reati previsti nel D. Lgs. 231/01.
- Definire le competenze e le procedure per l'attuazione del Modello.

2. Definizioni

Modello di Organizzazione, Gestione e Controllo	Sistema organizzativo di procedure e protocolli volti a prevenire comportamenti costituenti rischio di commissione dei reati delle specie previste dal D.Lgs. 231/01 (vedi [RIF1]). Tale modello prevede misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio. Il Modello adottato da Mizar è stato approvato dall'Amministratore Unico Mizar protempore in data 15/06/2017. La presente versione è stata confermata dal Consiglio di amministrazione in data 30/06/2025.
Reati presupposto	Sono i reati la cui commissione può comportare la responsabilità amministrativa a carico della Mizar, per effetto del D. Lgs. 231/01 e s.m.i. (vedi [RIF1]). Nella redazione del Modello, fra quelli previsti dal D. Lgs. 231/01, sono state identificate le seguenti principali categorie di reati, così come aggiornati dalle modifiche legislative fino al mese di giugno 2025: • Reati contro la Pubblica Amministrazione • Reati societari • Reati tributari • Reati commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro • Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio • Reati informatici • Reati commessi con violazione delle norme sul diritto di autore

	anche attraverso l'uso di comunicazioni elettroniche • Reati ambientali
Organismo di Vigilanza	È l'organismo nominato dalla società con il compito di vigilare sul funzionamento e sull'osservanza del Modello e di curarne l'aggiornamento.
Responsabile aziendale per l'applicazione del Modello	Figura aziendale designata dalla Società quale punto di riferimento per l'applicazione del Modello in azienda e con funzione di supporto nell'interpretazione dello stesso.

3. Riferimenti

[RIF1]	D.Lgs. 8/6/2001 n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, della società e delle associazioni anche prive di personalità giuridica"
[RIF2]	Codice Etico e di Comportamento Mizar

4. Lista reati presupposto (al 11 aprile 2025)

Fonte: https://www.reatipresupposto231.it/

Art. 24	Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture [Articolo modificato dalla L. 161/2017 e dal D.Lgs.n.75 del 14 luglio 2020]
Art. 24 - bis	Delitti informatici e trattamento illecito di dati [Articolo aggiunto dalla L. n. 48/2008, modificato dai D.lgs. n.7 e n. 8/2016, dal D.L. n. 105/2019 e da Legge n.90 del 28 giugno 2024]
Art. 24 - ter	Delitti di criminalità organizzata [Articolo aggiunto dalla L. n. 94/2009, modificato dalla L. 69/2015 e da D.Lgs.n.19 del 2 marzo 2023]
Art. 25	Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione [Articolo modificato dalla L. n. 190/2012, dalla Legge n. 3 del 9 gennaio 2019 dal D.Lgs.n.75 del 14 luglio 2020 e dalla Legge n.112 dell'8 agosto 2024]
Art. 25 - bis	Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento [Articolo aggiunto dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001; modificato dalla L. n. 99/2009; modificato dal D.Lgs.n.125/2016]

Art. 25 - bis.1	Delitti contro l'industria e il commercio [Articolo aggiunto dalla L. n. 99/2009]
Art. 25 - ter	Reati societari [Articolo aggiunto dal D.Lgs.n.61/2002, modificato dalla L. n. 190/2012, dalla L. 69/2015 e successivamente dal D.lgs. n.38/2017 e da D.lgs.n.19 del 2 marzo 2023]
Art. 25 - quater	Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal Codice penale e dalle leggi speciali [Articolo aggiunto dalla L. n. 7/2003]
Art. 25 - quater.1	Pratiche di mutilazione degli organi genitali femminili (Art. 583 - bis c.p.) [Articolo aggiunto dalla L. n. 7/2006]
Art. 25 - quinquies	Delitti contro la personalità individuale [Articolo aggiunto dalla L. n. 228/2003 e modificato dalla L. n. 199/2016]
Art. 25 - sexies	Reati di abuso di mercato [Articolo aggiunto dalla L. n. 62/2005] e altre fattispecie in materia di abusi di mercato (Art. 187 - quinquies TUF) [articolo modificato dal D.lgs. n. 107/2018 e dalla Legge n.238 del 23 dicembre 2021]
Art. 25 - septies	Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro [Articolo aggiunto dalla L. n. 123/2007]
Art. 25 - octies	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio [Articolo aggiunto dal D.Lgs.n.231/2007; modificato dalla L. n. 186/2014 e da D.Lgs.n.195 dell'8 novembre 2021]
Art. 25 - octies.1	Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori [Articolo aggiunto dal D.Lgs.n.184 del 18 novembre 2021e modificato da D.L.10 agosto 2023 n.105 coordinato con la Legge di conversione n.137 del 9 ottobre 2023]
Art. 25 - novies	Delitti in materia di violazione del diritto d'autore [Articolo aggiunto dalla L. n. 99/2009]
Art. 25 - decies	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria [Articolo aggiunto dalla L. n. 116/2009]
Art. 25 - undecies	Reati ambientali [Articolo aggiunto dal D.Lgs.n.121/2011, modificato dalla L. n. 68/2015 e da D.lgs. n. 21/2018]
Art. 25 - duodecies	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare [Articolo aggiunto dal D.lgs. n.109/2012 e modificato dalla Legge n. 161/2017]
Art. 25 - terdecies	Razzismo e xenofobia [Articolo aggiunto dalla L. n. 167/ 2017 e modificato dal D.lgs. n.21/2018]

Art. 25 - quater decies	Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati [Articolo aggiunto dall'Art.5 della L.n.39/2019]
Art. 25 - quinquies decies	Reati tributari [Articolo aggiunto dal D.L. n.124/2019 coordinato con Legge di conversione n.157/2019 e modificato dal D.Lgs.n.75/2020)
Art. 25 - sexiesdecies	Contrabbando [Articolo aggiunto dal D.Lgs.n.75/2020 e modificato dal D.lgs. n.141 del 26 settembre 2024]
Art. 25 - septies decies	Disposizioni in materia di reati contro il patrimonio culturale [Articolo aggiunto da L.n.22 del 09 marzo 2022]
Art. 25 - duodevicies	Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici [Articolo aggiunto da L.n.22 del 09 marzo 2022]
Art. 26	Delitti tentati (Art. 56 C.P.)
Art. 12, Legge n. 9/2013	Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato [Costituiscono presupposto per gli enti che operano nell'ambito della filiera degli oli vergini di oliva]
Legge n.146/2006	Reati transnazionali [Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale]

5. Regole

5.1. Premessa: cenni sul Decreto Legislativo

5.1.1. La responsabilità amministrativa degli enti per reati commessi nel loro interesse e/o a loro vantaggio

In data 8 giugno 2001 è stato emanato il Decreto Legislativo n. 231, entrato in vigore il 4 luglio 2001 (qui di seguito denominato "il Decreto"), dal titolo "*Disciplina della responsabilità amministrativa delle persone giuridiche, della società e delle associazioni anche prive di personalità giuridica*".

Con il Decreto, che ha subito negli anni numerosi aggiornamenti e modifiche, è stato introdotto nell'ordinamento italiano un regime di responsabilità a carico degli enti (ad es. società, associazioni, consorzi, ecc., qui di seguito denominati "gli Enti") per alcuni reati commessi, nell'interesse o a vantaggio degli Enti stessi, dai seguenti soggetti:

i) persone fisiche che hanno funzioni di rappresentanza, di amministrazione o di direzione degli Enti o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale (ad es. amministratori, direttori, ecc.), nonché persone fisiche che esercitano, anche di fatto, la gestione ed il controllo degli Enti;

ii) persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti indicati al precedente punto (ad es. dipendenti, agenti, collaboratori, ecc.).

Tale responsabilità si aggiunge a quella della persona fisica che ha commesso - materialmente - il reato e si può configurare anche per reati commessi all'estero.

I tipi di reato la cui commissione può comportare la responsabilità amministrativa a carico degli Enti sono in sostanza - allo stato - i seguenti (qui di seguito denominati "i Reati"):

i) reati contro la Pubblica Amministrazione (ad es. corruzione, concussione, truffa ai danni dello stato, turbata libertà degli incanti, turbata libertà del procedimento di scelta del contraente ecc.);

ii) reati contro la fede pubblica (ad es. falsificazione e/o alterazione di monete, ecc.);

iii) reati societari (ad es. corruzione tra privati, ecc.);

iv) reati tributari (ad es. Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, ecc.);

v) reati con finalità di terrorismo o di eversione dell'ordine democratico (ad es. associazioni sovversive, ecc.);

vi) reati concernenti il riciclaggio, incluso il trasferimento fraudolento di valori ;

vii) reati contro la personalità individuale;

viii) reati concernenti intralcio alla giustizia;

ix) reati concernenti pratiche di mutilazione degli organi genitali femminili;

x) reati concernenti l'abuso di informazioni privilegiate e di manipolazione del mercato;

xi) delitti transnazionali come definiti dalla legge 16/3/2006 n. 146 "Ratifica ed esecuzione

della Convenzione e dei Protocolli della Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea Generale il 15/11/2000 ed il 31/5/2001"

xii) reati commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul

lavoro;

xiii) reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio;

xiv) delitti informatici e trattamento illecito di dati;

xv) delitti in materia di violazione del diritto d'autore anche attraverso l'uso di comunicazioni elettroniche;

xvi) induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;

xvii) reati ambientali, incluso abbandono di rifiuti, inquinamento ambientale, disastro ambientale;

xviii) impiego di cittadini di paesi terzi il cui soggiorno è irregolare e relative sanzioni accessorie;

Tra le sanzioni previste a carico degli Enti, le più gravi sono rappresentate da misure interdittive quali la sospensione o la revoca di licenze e concessioni, il divieto di contrarre con la Pubblica Amministrazione, l'interdizione dall'esercizio dell'attività, l'esclusione o la revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi, oltre alle sanzioni pecuniarie sino ad un importo massimo di euro 1.549.370,70.

5.1.2.Presupposti per l'esclusione della responsabilità amministrativa degli enti

La responsabilità dell'Ente è esclusa nel caso in cui ricorrano tutti i seguenti presupposti (v. art. 6 comma primo del Decreto):

- l'organo dirigente dell'Ente ha adottato ed efficacemente attuato, prima della commissione dei Reati, un modello di organizzazione e di gestione idoneo a prevenire i Reati (qui di seguito denominato "il Modello");
- le persone fisiche che hanno commesso i Reati hanno agito eludendo fraudolentemente il Modello;
- il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento, è stato affidato ad un organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo (qui di seguito "l'Organismo di Vigilanza");
- non vi è stato omesso o insufficiente controllo da parte dell'Organismo di Vigilanza.

In particolare, il Modello deve avere il seguente contenuto (v. art. 6 comma secondo del Decreto):

- individuare le attività in cui esiste il rischio che vengano commessi i Reati;
- prevedere specifici protocolli (qui di seguito "i Protocolli") per la formazione e l'attuazione delle decisioni dell'Ente al fine di prevenire la commissione dei Reati;
- individuare modalità di gestione delle risorse finanziarie al fine di prevenire la commissione dei Reati;

- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto del Modello.

La responsabilità dell'Ente è esclusa nel caso in cui ricorrano tutti i seguenti presupposti (v. art. 6 comma primo del Decreto):

a) l'organo dirigente dell'Ente ha adottato ed efficacemente attuato, prima della commissione dei Reati, un modello di organizzazione e di gestione idoneo a prevenire i Reati (qui di seguito denominato "il Modello");

b) le persone fisiche che hanno commesso i Reati hanno agito eludendo fraudolentemente il Modello;

c) il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento, è stato affidato ad un organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo (qui di seguito "l'Organismo di Vigilanza");

d) non vi è stato omesso o insufficiente controllo da parte dell'Organismo di Vigilanza.

In particolare, il Modello deve avere il seguente contenuto (v. art. 6 comma secondo del Decreto):

- individuare le attività in cui esiste il rischio che vengano commessi i Reati;
- prevedere specifici protocolli (qui di seguito "i Protocolli") per la formazione e l'attuazione delle decisioni dell'Ente al fine di prevenire la commissione dei Reati;
- individuare modalità di gestione delle risorse finanziarie al fine di prevenire la commissione dei Reati;
- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto del Modello.

5.2. Modalità di prevenzione dei reati

5.2.1. Modalità di prevenzione dei reati contro la Pubblica Amministrazione

5.2.1.1. La tipologia dei Reati contro la Pubblica Amministrazione

I Reati contro la Pubblica Amministrazione la cui commissione può comportare la responsabilità amministrativa a carico di Mizar sono i seguenti (cfr. artt. 24 e 25 del Decreto):

- Malversazione a danno dello Stato (art. 316 - bis Codice penale);
- Indebita percezione di erogazioni a danno dello Stato (art. 316 - ter Codice penale);
- Concussione (art. 317 Codice penale);
- Corruzione per l' esercizio della funzione (art. 318 Codice penale);
- Corruzione per un atto contrario ai doveri d' ufficio (art. 319 Codice penale);
- Corruzione in atti giudiziari (art. 319 - ter Codice penale);

- Induzione indebita a dare o promettere utilità (art. 319 ‑ quater Codice penale
- Corruzione di persona incaricata di un pubblico servizio (art. 320 Codice penale);
- Pene per il corruttore (art. 321 Codice penale);
- Istigazione alla corruzione (art. 322 Codice penale);
- 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 Codice penale);
- Traffico di influenze illecite (art.346 ‑ bis Codice penale)
- Truffa (in danno dello Stato) (art. 640, comma 2 n. 1 Codice penale);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 ‑ bis Codice penale);
- Frode informatica (art. 640 ‑ ter Codice penale).

Per quanto riguarda il testo integrale delle fattispecie di reato, si rinvia all'Allegato n. 3.

5.2.1.2. Le aree a rischio

I Reati elencati al precedente paragrafo presuppongono l'instaurazione di rapporti con la Pubblica Amministrazione, anche estera.

Pertanto, sulla base della attività di Mizar, sono considerate come "aree a rischio":

i) i rapporti commerciali con Enti Pubblici;

ii) la negoziazione e la stipulazione, diretta o indiretta, di contratti di consulenza e altri rapporti di collaborazione con pubblici ufficiali e/o incaricati di pubblico servizio;

iii) la partecipazione a procedure per ottenere finanziamenti, erogazioni, contributi o altre operazioni similari da parte di Enti Pubblici italiani od esteri, nonché l'impiego concreto e la destinazione di tali somme.

In relazione al punto i) si evidenzia che hanno rapporti commerciali con Enti pubblici e/o loro dipendenti i venditori, gli agenti e i distributori, nonché il Servizio Clienti e la Direzione Amministrazione e Finanza. Analogamente, in relazione ai punti ii) si evidenzia che contratti di consulenza sono assunti principalmente Direzione Amministrazione e Finanza.

In relazione al punto iii) si evidenzia che il soggetto eventualmente coinvolto nella richiesta e nell'utilizzo di Finanziamenti Pubblici è principalmente la direzione Amministrazione e Finanza per quanto riguarda finanziamenti finalizzati alla realizzazione di corsi di formazione e/o ad investimenti.

Si riporta in Allegato n. 2 l'organigramma aziendale.

5.2.1.3. Principi generali di condotta all'interno delle aree a rischio

I principi generali di condotta all'interno delle "aree a rischio" indicate al precedente paragrafo sono i seguenti:

- divieto di adottare comportamenti tali da integrare i Reati contro la Pubblica

Amministrazione;

- divieto di adottare comportamenti che, sebbene non integrino di per sé Reati contro la Pubblica Amministrazione, potrebbero potenzialmente diventare tali;
- divieto di adottare comportamenti in conflitto di interesse con la Pubblica Amministrazione;
- divieto di adottare i comportamenti indicati ai precedenti punti sia direttamente, sia per interposta persona;
- obbligo di osservare il Codice Etico e di Comportamento Mizar;
- obbligo di osservare i Protocolli (vedi par. 4.1.4);
- divieto assoluto di richiedere, sollecitare, suggerire ad agenti, distributori, collaboratori od altri partner commerciali (broker) comportamenti vietati dal Modello;
- obbligo di documentare in modo chiaro e trasparente tutti i passaggi della attività svolte;
- obbligo di consultare il Responsabile aziendale per l'applicazione del Modello prima di adottare un determinato comportamento, in caso di incertezza sulla liceità dello stesso;
- nel caso in cui non sia possibile osservare i Protocolli, preventivi obblighi:
  - di illustrare per iscritto gli specifici motivi di tale inosservanza;
  - di ottenere l'autorizzazione scritta del soggetto di vertice della propria linea gerarchica.

I principi sopra elencati devono essere rispettati anche quando l'attività è svolta congiuntamente con altre società o comunque con terzi.

5.2.1.4. I Protocolli per la formazione e l'attuazione delle decisioni all'interno delle aree a rischio

Per la formazione e l'attuazione delle decisioni all'interno della "aree a rischio" devono essere osservati i seguenti protocolli:

- Per quanto riguarda le forniture di prodotti e servizi, si rinvia all'Allegato n. 4;
- Per quanto riguarda le donazioni di beni o di denaro, si rinvia all'Allegato n. 5;
- Per quanto riguarda i contratti di consulenza, si rinvia all'Allegato n. 6;
- Per quanto riguarda l'erogazione e l'utilizzo di finanziamenti, si rinvia all'Allegato n. 7;
- Per quanto riguarda l'acquisto di beni e di servizi, si rinvia all'Allegato n. 8;

5.2.2. Modalità di prevenzione dei reati societari

I reati societari la cui commissione può comportare la responsabilità amministrativa a carico di Mizar sono i seguenti (cfr. art. 25-*ter* del Decreto):

- *False comunicazioni sociali* (art. 2621 Codice civile);
- *False comunicazione sociali in danno della società, dei soci o dei creditori* (art. 2622 Codice civile);
- *Impedito controllo* (art. 2625 Codice civile);
- *Indebita restituzione dei conferimenti* (art. 2626 Codice civile);
- *Illegale ripartizione degli utili e delle riserve* (art. 2627 Codice civile);
- *Illecite operazioni sulle azioni o quote sociali o della società controllante* (art. 2628 Codice civile);

- *Operazioni in pregiudizio dei creditori* (art. 2629 Codice civile);
- *Formazione fittizia del capitale* (art. 2632 Codice civile);
- *Indebita ripartizione dei beni sociali da parte dei liquidatori* (art. 2633 Codice civile);
- *Corruzione tra privati* (art. 2635 Codice civile)
- *Illecita influenza sull'assemblea* (art. 2636 Codice civile);
- *Aggiotaggio* (art. 2637 Codice civile);
- *Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza* (art. 2638 cCdice civile).

Per quanto riguarda il testo integrale delle fattispecie di reato, si rinvia all'Allegato n.9.

5.2.2.1. Le aree a rischio

I reati elencati al precedente paragrafo tutelano, fra l'altro, i) la veridicità, la trasparenza e la correttezza delle informazioni relative alla società; ii) l'effettività e l'integrità del capitale e del patrimonio sociale; iii) il regolare e corretto funzionamento della società, iv) la regolarità nei rapporti commerciali fra privati.

Pertanto, sono considerate come "aree a rischio":

- la redazione del bilancio e delle comunicazioni sociali;
- la redazione, la compilazione e la raccolta della documentazione e dei dati necessari per la redazione del bilancio e delle comunicazioni sociali;
- le operazioni straordinarie sul capitale (es. riduzione del capitale, fusioni, ecc.)
- i rapporti commerciali con i privati.

I soggetti a rischio sono il Presidente del Consiglio di amministrazione, la Direzione Amministrazione e Finanza.

5.2.2.2. Principi generali di condotta all'interno delle aree a rischio

I principi generali di condotta all'interno della "aree a rischio" indicate al precedente paragrafo sono i seguenti:

1) divieto di adottare comportamenti tali da integrare i Reati societari;
2) divieto di adottare comportamenti che, sebbene non integrino di per sé i Reati societari, potrebbero potenzialmente diventarlo;
3) divieto di adottare qualsiasi situazione e/o tenere qualsiasi comportamento in conflitto di interessi con la società;
4) divieto di adottare comportamenti che integrino il reato di corruzione fra privati;
5) divieto di adottare comportamenti indicati ai precedenti punti sia direttamente, sia per interposta persona;
6) obbligo di osservare il Codice Etico e di Comportamento Mizar;

7) obbligo di osservare i Protocolli (vedi par. 5.2.1.4);

8) obbligo di documentare in modo chiaro, trasparente e completo tutte le informazioni necessarie per la redazione del bilancio e delle comunicazioni sociali;

9) obbligo di consultare il Responsabile aziendale per l'applicazione del Modello prima di adottare un determinato comportamento, in caso di incertezza sulla liceità dello stesso;

10) nel caso in cui non sia possibile osservare i Protocolli, preventivo obbligo:

   i) di illustrare per iscritto gli specifici motivi di tale inosservanza;

   ii) di ottenere l'autorizzazione scritta del Presidente del Consiglio di amministrazione.

5.2.2.3. I Protocolli per la formazione e l'attuazione delle decisioni all'interno delle aree a rischio

Per la formazione e l'attuazione delle decisioni all'interno della "aree a rischio" devono essere osservati i seguenti Protocolli:

- assicurare che la tenuta della contabilità avvenga in modo trasparente e conforme alle norme vigenti, e che i dati contabili siano validati da adeguata documentazione di supporto e dalla verifica di un controllore (Allegato 10);
- attuare le procedure di controllo volte ad assicurare la correttezza, completezza e accuratezza delle voci di bilancio, attraverso adeguata documentazione di supporto (Allegato 11);

nonché rispettare tutti i protocolli richiamati nel capitolo par. 5.2.1.4per quanto attiene ai rapporti con i privati, al fine di prevenire efficacemente il reato di corruzione fra privati.

Inoltre, è fatto obbligo di segnalare preventivamente all'Organismo di Vigilanza eventuali operazioni straordinarie in programma.

5.2.3. Modalità di prevenzione dei reati commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

5.2.3.1. La tipologia dei reati

I Reati commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro la cui commissione può comportare la responsabilità amministrativa a carico di Mizar sono i seguenti (cfr. art. 25-septies del Decreto):

- Omicidio colposo (art. 589 del Codice penale);

- Lesioni personali colpose gravi o gravissime (art. 590, terzo comma, del Codice penale);

Per quanto riguarda il testo integrale della fattispecie di reato, si rinvia all'Allegato n. 12.

5.2.3.2. Le aree a rischio

Le aree a rischio di commissione dei Reati di cui al precedente paragrafo sono quelle ove possono commettersi violazioni delle norme sulla sicurezza e salute nei luoghi di lavoro (D.Lgs. 81/08).

Pertanto, sono considerate come "aree a rischio":

i) le aree aziendali contenenti attrezzature informatiche;

ii) i magazzini dell'azienda, sia interni che esterni;

iii) i viaggi di lavoro.

I soggetti a rischio sono il datore di lavoro (ex D.Lgs. n. 81/2008), della società, il Responsabile del Servizio di Prevenzione e Protezione, i preposti e i lavoratori tutti, tenuti ciascuno individualmente al rispetto della normativa di cui sopra. Sono pertanto da considerarsi "aree a rischio" tutte le aree aziendali.

5.2.3.3. Principi generali di condotta all'interno delle aree a rischio.

I principi generali di condotta all'interno delle "aree a rischio" indicate al precedente paragrafo 4.3.2 sono i seguenti:

1) in ossequio all'art.20 D. Lgs 81/08, ogni lavoratore deve prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal datore di lavoro. In particolare, i lavoratori devono:

   a. contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;

   b. osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;

   c. utilizzare correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi, i mezzi di trasporto, nonché i dispositivi di sicurezza;

   d. utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;

   e. segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi di cui alle lettere c) e d), nonché qualsiasi eventuale condizione di

      pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;

   f. non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;

   g. non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;

   h. partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro;

   i. sottoporsi ai controlli sanitari previsti dal presente decreto legislativo o comunque

disposti dal medico competente;

j. fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione e il medico competente, ove presente;

k. prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico;

l. richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione;

m. richiedere al medico competente l'osservanza degli obblighi previsti a suo carico dal D. Lgs 81/08;

n. adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;

o. informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;

p. adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, nonché per il caso di pericolo grave e immediato;

q. aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;

r. vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità.

2) i preposti, secondo le loro attribuzioni e competenze, così come stabilito dall'art. 19 del D. Lgs 81/08, hanno l'obbligo di:

a. sovrintendere e vigilare sulla osservanza da parte dei singoli lavoratori dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione e, in caso di persistenza della inosservanza, informare i loro superiori diretti;

b. verificare affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;

c. richiedere l'osservanza delle misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa;

d. informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;

e. astenersi, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave ed immediato;

f. segnalare tempestivamente al datore di lavoro o al dirigente sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro, delle quali venga a conoscenza sulla base della formazione ricevuta;

g. frequentare appositi corsi di formazione secondo quanto previsto dall'articolo 37 del D. Lgs 81/08;

3) ai sensi dell'art. 33 del D. Lgs 81/08, il Responsabile del servizio di prevenzione e protezione deve provvedere:

a. all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;

b. ad elaborare, per quanto di competenza, le misure preventive e protettive di cui all'articolo 28, comma 2, e i sistemi di controllo di tali misure;

c. ad elaborare le procedure di sicurezza per le varie attività aziendali;

d. a proporre i programmi di informazione e formazione dei lavoratori;

e. ad adempiere agli altri compiti consultativi e informativi previsti dagli articoli 35 e 36 del D. Lgs 81/08;

4) in virtù dell'art. 17 del D. Lgs 81/08 il datore di lavoro ha i seguenti obblighi non delegabili:

a. valutazione di tutti i rischi con la conseguente elaborazione del documento richiesto dall'art. 28 del D. Lgs 81/08;

b. designazione del Responsabile del servizio di prevenzione e protezione dai rischi;

5) agli obblighi non delegabili di cui al punto precedente, si aggiungono, per il datore di lavoro e per i dirigenti, tutti gli obblighi elencati dall'art. 18 del D. Lgs 81/08, tra i quali quelli di:

a. nominare il medico competente per l'effettuazione della sorveglianza sanitaria nei casi previsti dal D. Lgs 81/08;

b. designare preventivamente i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza;

c. nell'affidare i compiti ai lavoratori, tenere conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute e alla sicurezza.

d. fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione e il medico competente, ove presente;

e. prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico;

f. richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione;

g. richiedere al medico competente l'osservanza degli obblighi previsti a suo carico dal D. Lgs 81/08;

h. adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;

i. informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;

j. adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, nonché per il caso di pericolo grave e immediato;

k. aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;

l. vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità.

5.2.3.4. I Protocolli per la formazione e l'attuazione delle decisioni all'interno delle aree a rischio

L'azienda ha in atto fin dal momento della sua costituzione un sistema di gestione della sicurezza conforme alle linee guida del D. Lgs. 626/94, e che allo stato attuale ha adeguato il proprio sistema di gestione della sicurezza a quanto previsto dalla normativa in vigore (D. Lgs 81/08).

Si rimanda in proposito all'Allegato n. 13.

5.2.4. Modalità di prevenzione dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

5.2.4.1. La tipologia dei reati

I reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché

autoriclaggio la cui commissione può comportare la responsabilità amministrativa a carico di Mizar sono i seguenti (cfr. art. 25-*octies* del Decreto):

- *Ricettazione (Art. 648 c.p.)*
- *Riciclaggio (Art. 648-bis c.p.)*
- *Impiego di denaro, beni o utilita' di provenienza illecita. (Art. 648-ter c.p.)*
- *Autoriciclaggio (Art. 648-ter.1 c.p.)*

5.2.4.2. Principi generali di condotta all'interno delle aree a rischio.

I principi sono fondamentalmente costituiti dal rigoroso rispetto delle leggi finanziarie esistenti in materia.

5.2.5. Modalità di prevenzione dei reati commessi con violazione delle norme in materia di reati informatici

5.2.5.1. La tipologia dei reati

I reati commessi in violazione delle norme in materia di reati informatici la cui commissione può comportare la responsabilità amministrativa a carico di Mizar sono i seguenti (cfr. art. 24-*bis* del Decreto):

- *Documenti informatici (Art. 491-bis c.p.)*
- *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 o 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.)*
- *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640- quinquies c.p.).*

Per quanto riguarda il testo integrale delle fattispecie di reato, si rinvia all'Allegato n. 16.

5.2.5.2. Principi generali di condotta all'interno delle aree a rischio.

I principi sono fondamentalmente costituiti dal rispetto delle procedure di Accesso al Sistema Informativo e di Gestione Personal Computer Individuali e del Regolamento per l'uso delle risorse informatiche.

Si rimanda per il dettaglio all'Allegato 15.

5.2.5.3. I Protocolli per la formazione e l'attuazione delle decisioni all'interno delle aree a rischio

Si rimanda in proposito all'Allegato 15.

5.2.6. Modalità di prevenzione dei reati commessi con violazione delle norme in materia di violazione del diritto d'autore

5.2.6.1. La tipologia dei reati

I reati commessi in violazione delle norme in materia di diritto d'autore, la cui commissione può comportare la responsabilità amministrativa a carico di Mizar, sono quelli di cui ai seguenti articoli della legge 633/41 (cfr. art. 25-novies del Decreto):

- Art. 171 L. 633/41
- Art. 171-bis L. 633/41
- Art. 171-ter L. 633/41
- Art. 171-septies L. 633/41
- Art. 171-octies L. 633/41

Per quanto riguarda il testo integrale delle fattispecie di reato, si rinvia all'Allegato n. 16.

5.2.6.2. Principi generali di condotta all'interno delle aree a rischio. I principi sono fondamentalmente costituiti dal rispetto del Codice Etico e di Comportamento Mizar e del Regolamento per l'uso delle risorse informatiche.

Si rimanda per il dettaglio all'Allegato 17.

5.2.6.3. I Protocolli per la formazione e l'attuazione delle decisioni all'interno delle aree a rischio

Si rimanda all'Allegato 17.

5.2.7. Modalità di prevenzione dei reati in materia ambientale

5.2.7.1. La tipologia dei reati

I Reati commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro la cui commissione può comportare la responsabilità amministrativa a carico di Mizar sono i seguenti (cfr. art. 25-septies del Decreto):

- Omicidio colposo (art. 589 del Codice penale);
- Lesioni personali colpose gravi o gravissime (art. 590, terzo comma, del Codice penale).

5.2.7.2. Le aree a rischio.

Le aree a rischio di commissione dei Reati di cui al precedente paragrafo 4.6.1. sono quelle ove possono commettersi violazioni delle norme in materia ambientale.

Pertanto, sono considerate come "aree a rischio":

i) Gli uffici di via Giacomo Peroni 400;

ii) i magazzini dell'azienda, sia interni che esterni;

Il soggetto a rischio è il Presidente del Consiglio di amministrazione tenuto al rispetto della normativa di cui sopra. Sono pertanto da considerarsi "aree a rischio" tutte le aree aziendali.

5.2.7.3. Principi generali di condotta all'interno delle aree a rischio.

I principi generali di condotta all'interno delle "aree a rischio" indicate al precedente paragrafo sono fondamentalmente costituiti dal rispetto del Codice Etico e di Comportamento Mizar.

5.2.7.4. I Protocolli per la formazione e l'attuazione delle decisioni all'interno delle aree a rischio

L'azienda ha in atto fin dal momento della sua costituzione un sistema di gestione della sicurezza conforme alle linee guida del D. Lgs. 626/94, e che allo stato attuale ha adeguato il proprio sistema di gestione della sicurezza a quanto previsto dalla normativa in vigore (D. Lgs 81/08)

Si rimanda in proposito all'Allegato n. 18.

6. Selezione e formazione del personale e dei collaboratori esterni

6.1. Il personale

6.1.1. Selezione

All'atto dell'assunzione del personale deve essere richiesta al candidato idonea dichiarazione, resa nelle forme di cui al D.P.R. n. 445 del 2000, con la quale lo stesso dichiari:

i) di non avere riportato condanne penali con sentenza passata in giudicato, anche con il beneficio della non menzione nel certificato del casellario giudiziale**;**

ii) se ha avuto precedenti rapporti di dipendenza e/o di collaborazione con pubbliche amministrazioni;

iii) Se ha rapporti di parentela o affinità sino al secondo grado e/o di coniugio con dipendenti e/o collaboratori di pubbliche amministrazioni.

In caso di esistenza di una delle suddette situazioni a rischio, il candidato in esame può essere assunto solo a condizione che:

1) il Responsabile interessato indichi per iscritto gli specifici motivi di tale assunzione;

2) tali motivi siano valutati ragionevoli dal Responsabile Risorse Umane, congiuntamente al Responsabile Amministrativo e Finanziario.

È fatto assoluto divieto di assumere lavoratori extracomunitari non in possesso di regolare permesso di soggiorno.

6.1.2. Formazione ed informativa

La formazione del personale per l'attuazione del Modello è gestita dal Responsabile Risorse Umane, mantenendo costantemente aggiornato sul punto l'Organismo di Vigilanza, con le seguenti modalità:

a) corso introduttivo, anche per i neoassunti;

b) corsi di aggiornamento;

c) *e-mail* informative;

d) informativa nella lettera di assunzione per i neoassunti;

e) verifica annuale della conoscenza delle disposizioni del Modello mediante il superamento di un test basato su un apposito questionario;

f) affissione nella bacheca aziendale del codice disciplinare (vedi capitoli 7 e 8).

6.2. I collaboratori esterni

6.2.1. Selezione

All'atto del conferimento di incarichi a collaboratori esterni (quali ad esempio agenti, consulenti, distributori, ecc.) destinati ad operare in aree a rischio di Reato, deve essere richiesta al collaboratore (nel caso degli agenti o dei distributori persone giuridiche, la verifica deve essere effettuata per il/gli amministratori) idonea dichiarazione, resa nelle forme di cui al d.P.R. n. 445 del 2000, con la quale lo stesso dichiari:

i) di non avere riportato condanne penali con sentenza passata in giudicato, per reati gravi che incidono sulla moralità professionale;

ii) di non avere avuto precedenti rapporti di dipendenza e/o di collaborazione con pubbliche amministrazioni;

iii) di non avere rapporti di parentela o affinità sino al secondo grado e/o di coniugio con dipendenti e/o collaboratori di pubbliche amministrazioni;

In caso di esistenza di una delle suddette situazioni a rischio, l'incarico può essere conferito solo a condizione che:

1) il Responsabile interessato indichi per iscritto gli specifici motivi di tale incarico, mettendo in copia l'Organismo di Vigilanza;

2) tali motivi siano valutati ragionevoli dal Responsabile Risorse Umane, congiuntamente al Responsabile Amministrativo e Finanziario.

In ogni caso non può essere conferito alcun incarico a soggetto extracomunitario privo di regolare permesso di soggiorno.

6.2.2. Formazione, informativa e obblighi in capo ai collaboratori esterni

La formazione dei collaboratori esterni per l'attuazione del Modello è gestita dal Responsabile aziendale per l'applicazione del Modello, previa consultazione con l'Organismo di Vigilanza, con le seguenti modalità:

i) portare a conoscenza del collaboratore esterno il Codice Etico e di Comportamento Mizar e il Modello e fargli sottoscrivere apposita dichiarazione con la quale lo stesso di obbliga al rispetto delle leggi, del Codice Etico e di Comportamento Mizar e del Modello, pena la risoluzione immediata del rapporto.

7. Segnalazione delle violazioni del modello

Chiunque venga a conoscenza di atti o comportamenti posti in essere in violazione del presente Modello, ha l'obbligo di segnalarlo ad uno o più dei seguenti soggetti:

- Responsabile aziendale per l'applicazione del Modello;
- Organismo di Vigilanza all'e-mail org231@mizarbrokers.it;
- Responsabile Risorse Umane.

In aggiunta al canale e-mail sopra indicato, viene istituita una cassetta per segnalazioni riservate in forma cartacee, l'accesso alla quale sarà consentito esclusivamente all'Organismo di Vigilanza.

Tutte le segnalazioni verranno trattate in modo riservato ed il nominativo del segnalante non potrà essere divulgato a soggetti diversi dal Presidente del Consiglio di amministrazione dall'Organismo di Vigilanza.

8. Whistleblowing – Tutela del dipendente o del collaboratore che segnala illeciti – art. 6 comma 2bis del d.lgs. 231/001

8.1. Premessa

La legge n. 179/2017 concernente "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" pubblicata sulla Gazzetta Ufficiale n. 291/2017, ha regolamentato l'istituto del whistleblowing per il settore pubblico e privato.

Con specifico riguardo al settore privato la novella interviene inserendo all'art. 6, del D.Lgs. n. 231/2001, dopo il comma 2 i seguenti:

2-bis. I modelli di cui alla lettera a) del comma 1 prevedono:

a) uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto 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; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della

segnalazione;

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

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

d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

2-ter. L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2-bis può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

2-quater. Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. È onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa".

8.2. Il sistema di whistleblowing Mizar

MIZAR, al fine di garantire una gestione responsabile ed in linea con le prescrizioni legislative, ha implementato diversi Canali di Whistleblowing, attenendosi a quanto disciplinato oltre che dal presente Modello, dal Codice Etico e dalla normativa vigente: Legge 30 novembre 2017, n. 179 "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"

Pertanto, ai sensi dell'art. 6 del D.lgs. 231/01, comma 2-bis, MIZAR:

a) ha istituito più Canali di Whistleblowing dedicati a tutela dell'integrità dell'ente che consentano ai soggetti di cui all'art. 5, comma primo lett. a) e b) del D.lgs. 231/01, di presentare, segnalazioni di condotte illecite rilevanti ai sensi del Decreto 231 o violazioni del presente Modello e del Codice Etico che ne fa parte, di cui siano venuti a conoscenza in ragione delle funzioni svolte;

b) a mezzo di tali Canali di Segnalazione, garantisce la riservatezza dell'identità del segnalante e ammette la possibilità di eseguire segnalazioni anonime;

c) vieta ogni atto di ritorsione o discriminatorio, diretto o indiretto, nei confronti del Segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;

d) tutela, tramite misure ad hoc, sia il Segnalante sia il Segnalato.

Il Sistema di Whislteblowing descritto in maniera dettagliata nella Procedura Whistleblowing.

9. Codice etico e di comportamento

Il Codice Etico e di Comportamento Mizar ([RIF2]) esprime i principi di comportamento, riconosciuti da Mizar Insurance Brokers srl, che ciascun amministratore, dipendente e collaboratore è tenuto ad osservare scrupolosamente nello svolgimento della propria attività.

10. Sanzioni disciplinari

10.1. Principi generali

MIZAR condanna qualsiasi comportamento difforme, oltre che dalla legge, dalle previsioni del Modello e del Codice Etico, anche qualora il comportamento sia realizzato nell'interesse della Società stessa ovvero con l'intenzione di arrecare ad essa un vantaggio.

MIZAR ha predisposto un adeguato sistema sanzionatorio per la violazione del Modello al fine di garantirne l'osservanza e ciò in aggiunta a quanto previsto dal CCNL del settore COMMERCIO.

L'applicazione delle sanzioni disciplinari è indipendente dall'esito di un eventuale procedimento penale.

A titolo esemplificativo, costituiscono comportamenti che possono essere soggetti a procedure disciplinari i seguenti:

- la violazione, anche con condotte omissive e in eventuale concorso con altri, dei principi e delle procedure previste dal Modello o stabilite per la sua attuazione;
- la violazione delle misure poste a tutela dei whistleblower;
- la presentazione di segnalazioni infondate con dolo o colpa grave;
- la redazione, eventualmente in concorso con altri, di documentazione non veritiera;
- l'agevolazione, mediante condotta omissiva, della redazione da parte di altri, di documentazione non veritiera;
- la sottrazione, la distruzione o l'alterazione di documentazione aziendale previste dalle procedure;
- l'ostacolo alla attività di vigilanza dell'Organismo di Vigilanza;
- l'impedimento all'accesso alle informazioni e alla documentazione richiesta dai soggetti preposti ai controlli delle procedure e delle decisioni;
- la realizzazione di qualsiasi altra condotta idonea a eludere il sistema di controllo previsto dal Modello.

10.2. Sanzioni per i dipendenti

Le violazioni da parte dei dipendenti delle previsioni del Modello, anche con riferimento agli obblighi in materia di salute e sicurezza negli ambienti di lavoro, costituiscono illeciti disciplinari.

Le disposizioni del presente capitolo sono da intendersi quale codice disciplinare aziendale e verranno irrogate, a seguito della violazione del Modello, in conformità alle procedure previste dall'art. 7 l. 30 maggio 1970 n. 300 (c.d. Statuto dei Lavoratori), dal CCNL del settoreCommercio e da eventuali

normative speciali applicabili.

Le sanzioni disciplinari applicabili, a seconda della gravità della violazione del Modello, saranno, in conformità a quanto previsto dal CCNL del settore Commercio, le seguenti:

- richiamo verbale;
- ammonizione scritta;
- multa;
- sospensione;
- licenziamento.

A titolo esemplificativo,

1) incorre nel provvedimento dell'ammonizione scritta, della multa non superiore a tre (3) ore di retribuzione oraria o della sospensione dal lavoro sino ad un massimo di tre (3) giorni:

   – il lavoratore che con negligenza commetta una o più violazioni del Modello.

   A mero titolo esemplificativo, ma non limitativo, le sanzioni dell'ammonizione scritta, della multa o della sospensione potranno essere inflitte al dipendente che:

   a) concluda contratti di consulenza con dipendenti pubblici in violazione delle regole e delle procedure previste dall'Allegato n. 6;

   b) assuma iniziative per convegni e/o congressi medico/scientifici in violazione delle regole e delle procedure previste dall'Allegato n. 9;

   c) assuma impegni di spesa eccedenti i propri poteri di spesa, così come previsti dall'Allegato n. 15.

2) incorre nel provvedimento del licenziamento:

   – il lavoratore che intenzionalmente o con grave negligenza commetta gravi infrazioni alla disciplina del Modello che possano costituire Reati o, comunque, aumentino concretamente il rischio della commissione dei Reati.

   A mero titolo esemplificativo, ma non limitativo, la sanzione del licenziamento potrà essere inflitta al dipendente che, da solo o in concorso con altri soggetti, anche esterni alla società:

   a) effettui regalie a favore di pubblici ufficiali o incaricati di pubblico servizio in violazione di quanto previsto dal Codice Etico e di Comportamento (Rif. 2);

   b) effettui pagamenti in contanti al di fuori dei casi tassativamente previsti dall'Allegato n. 16;

   c) falsifichi documenti e/o dichiari il falso al fine di far risultare l'osservanza propria e/o di altri dipendenti delle leggi e/o del Modello;

   d) commetta con recidiva gravi violazioni del Modello di cui ai punti 1a), 1b) e 1c).

10.3. Sanzioni per i dirigenti (ove presenti)

La violazione dei principi e delle regole di comportamento contenute nel presente Modello da parte dei dirigenti, ovvero l'adozione di un comportamento non conforme alle richiamate prescrizioni, così come la violazione delle misure a tutela dei whistleblower o ancora la presentazione di segnalazioni infondate con dolo o colpa grave sarà assoggettata a misura disciplinare modulata a seconda della gravità della

violazione commessa. Per i casi più gravi è prevista la risoluzione del rapporto di lavoro, in considerazione dello speciale vincolo fiduciario che lega il dirigente al datore di lavoro.

In caso di violazione da parte di un dirigente, deve esserne data tempestiva comunicazione al Consiglio Direttivo mediante relazione scritta. I destinatari della comunicazione avviano i procedimenti di loro competenza al fine delle contestazioni e dell'eventuale applicazione delle sanzioni previste dalla legge e dal CCNL applicabile, compresa l'eventuale revoca di procure o deleghe.

Costituiscono illecito disciplinare, tra l'altro:

a) la mancata vigilanza da parte del personale dirigente sulla corretta applicazione, da parte dei lavoratori gerarchicamente subordinati, delle regole previste dal Modello;

b) la violazione degli obblighi di informazione nei confronti dell'Organismo di Vigilanza in ordine alla commissione dei reati rilevanti, ancorché tentata;

c) la violazione delle regole di condotta contenute nel Modello da parte dei dirigenti stessi;

d) l'assunzione, nell'espletamento delle rispettive mansioni, di comportamenti che non siano conformi a condotte ragionevolmente attese da parte di un dirigente, in relazione al ruolo rivestito ed al grado di autonomia riconosciuto.

e) la violazione delle misure poste a tutela dei whistleblower;

f) la presentazione di segnalazioni infondate con dolo o colpa grave

10.4. Sanzioni nei confronti dei Componenti del Consiglio di amministrazione e dei membri del Collegio sindacale

Nei confronti dei componenti del Consiglio di amministrazione non dipendenti della Società che abbiano:

a) commesso una violazione del presente Modello;

b) violato le misure poste a tutela dei whistleblower;

c) presentato, con dolo o colpa grave, segnalazioni infondate

Il Consiglio di amministrazione, prontamente informato dall'Organismo di Vigilanza, può applicare ogni idoneo provvedimento consentito dalla legge. Il Consiglio di amministrazione, qualora si tratti di violazioni tali da integrare giusta causa di revoca, propone all'Assemblea l'adozione dei provvedimenti di competenza e provvede agli ulteriori incombenti previsti dalla legge.

Nel caso di componenti del Consiglio di amministrazione che risultano essere anche dipendenti della Società, si applicano le sanzioni previste ai paragrafi precedenti.

In caso di violazione da parte di un componente del Collegio Sindacale, l'Organismo di Vigilanza deve darne immediata comunicazione al Presidente del Consiglio di amministrazione, mediante relazione scritta. Il Presidente del Consiglio di amministrazione, qualora si tratti di violazioni tali da integrare giusta causa di revoca, convoca l'Assemblea inoltrando preventivamente ai soci la relazione dell'Organismo di Vigilanza. L'adozione del provvedimento conseguente la già menzionata violazione spetta comunque all'Assemblea.

10.5. Sanzioni nei confronti dei "terzi destinatari"

a) I rapporti con le terze parti sono regolati da adeguati contratti formali che devono prevedere clausole di rispetto dei principi fondamentali del Modello e del Codice Etico da parte di tali soggetti esterni. In particolare, il mancato rispetto degli stessi deve comportare la risoluzione di diritto dei medesimi rapporti (ai sensi dell'art. 1456 c.c.), fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti per la Società.

b) L'eventuale mancata inclusione di tali clausole deve essere comunicata dalla funzione nel cui ambito opera il contratto, con le debite motivazioni, all'Organismo di Vigilanza.

11. Compiti

11.1. Presidente del Consiglio di amministrazione

- Applica le misure previste dal Modello nei riguardi dei dirigenti.
- Approva le modifiche e/o integrazioni dei Protocolli allegati al Modello su proposta dell'Organismo di Vigilanza.

11.2. Organismo di Vigilanza

- Si riunisce almeno tre volte all'anno e comunque ogni qualvolta sia ritenuto necessario da parte dell'Organismo stesso o del Presidente del Consiglio di amministrazione.
- Per i problemi operativi, riferisce al Presidente del Consiglio di amministrazione.
- Ha le seguenti funzioni:
  - vigilare sull'osservanza del Modello;
  - vigilare sulla effettiva capacità del Modello, in relazione alla struttura aziendale, di prevenire la commissione dei Reati;
  - curare l'aggiornamento del Modello e proporre le relative modifiche all'Amministratore Unico;
  - gestire le segnalazioni di Whistleblowing;
- Ha i seguenti poteri:
  - richiedere alle direzioni aziendali informazioni e documentazione in merito alle operazioni ed agli atti compiuti nelle "aree a rischio" di commissione dei Reati;
  - adottare e/o attivare procedure di controllo al fine di verificare l'osservanza del Modello;
  - effettuare verifiche a campione su determinate operazioni e/o atti specifici compiuti nelle "aree a rischio" di commissione dei Reati;
  - compiere indagini conoscitive al fine di individuare e/o aggiornare le "aree a rischio" di commissione dei Reati;
  - promuovere idonee iniziative per la diffusione, la conoscenza e la comprensione

del Modello;

- fornire chiarimenti ed istruzioni per l'osservanza del Modello;
- consultarsi con altre funzioni aziendali e/o consulenti esterni al fine di garantire l'efficacia del Modello;
- raccogliere, elaborare e custodire le informazioni relative al Modello;
- valutare e proporre al Consiglio di amministrazione le modifiche e/o gli aggiornamenti da apportare al Modello.

11.3. Responsabili aziendali

Considerata la struttura di Mizar, la dizione "Responsabile" non si riferisce ad una posizione organizzativa ma ad una funzione che può essere accorpata assieme ad altre anche in un solo Dipendente.

11.3.1. Responsabile aziendale per l'applicazione del Modello

- Costituisce il punto di riferimento in Azienda per l'applicazione del Modello.
- Svolge funzione di supporto nell'interpretazione e nell'applicazione del Modello.
- Informa l'Organismo di Vigilanza delle segnalazioni e/o notizie relative alla violazione del Modello.

11.3.2. Responsabile Risorse Umane

- Informa l'Organismo di Vigilanza delle segnalazioni e/o notizie relative alla violazione del Modello.
- Informa l'Organismo di Vigilanza dei procedimenti e/o provvedimenti disciplinari aziendali avviati/adottati a seguito della violazione del Modello.
- Nell'ambito della procedura di selezione del personale deve verificare che il candidato:
  - qualora cittadino di un paese extracomunitario, sia in regola con il permesso di soggiorno (questa condizione non può essere derogata in nessun caso);
  - non abbia precedenti penali;
  - non abbia avuto precedenti rapporti di dipendenza e/o di collaborazione con pubbliche amministrazioni;
  - non abbia rapporti di parentela o affinità sino al secondo grado e/o di coniugio con dipendenti e/o collaboratori di pubbliche amministrazioni.
- Approva, congiuntamente con il Responsabile Amministrazione e Finanza, l'assunzione di personale che si trovi in una o più delle situazioni a rischio indicate nel Modello (vedi punto 5.2.1)
- Previa consultazione con l'Organismo di Vigilanza, organizza e sovrintende alla formazione del personale, attraverso le funzioni deputate a questi compiti, per l'attuazione del Modello, articolata nei seguenti elementi:

- corso introduttivo, anche per i neoassunti;
- corsi di aggiornamento;
- *e-mail* informative;
- informativa nella lettera di assunzione per i neoassunti;
- verifica annuale della conoscenza delle disposizioni del Modello mediante il superamento di un test basato su un apposito questionario.

- Provvede all'affissione del codice disciplinare nella bacheca aziendale
- Applica le sanzioni disciplinari previste dal Modello nei riguardi dei dipendenti
- Applica congiuntamente con l'Amministratore Unico le sanzioni disciplinari previste dal Modello nei riguardi dei dirigenti.

11.3.3. Responsabile Amministrativo e Finanziario

- Informa l'Organismo di Vigilanza sul sistema delle deleghe degli amministratori e di ogni sua successiva modifica e/o integrazione.
- Informa l'Organismo di Vigilanza sul sistema di autorizzazione di spesa e di ogni sua successiva modifica e/o integrazione.
- Sulla base di motivata richiesta scritta del Responsabile di Unità Organizzativa interessato, approva, congiuntamente con il Responsabile Risorse Umane, l'assunzione di personale che si trovi in una o più delle situazioni a rischio indicate nel Modello (vedi punto 5.2.1)
- Sulla base di motivata richiesta scritta del Responsabile di Unità Organizzativa interessato, approva, il conferimento di incarichi a collaboratori esterni che si trovino in una o più delle situazioni a rischio indicate nel Modello (vedi punto 5.2.2)

11.3.4. Responsabile di Unità Organizzativa

- Qualora intenda procedere con l'assunzione di personale che si trovi in una o più delle situazioni a rischio indicate nel Modello, indica per iscritto gli specifici motivi di tale assunzione e richiede l'approvazione del Responsabile Risorse Umane e del Responsabile Amministrativo e Finanziario.
- All'atto del conferimento di incarichi a collaboratori esterni destinati ad operare in aree a rischio di Reato, richiede al collaboratore (nel caso degli agenti o dei distributori persone giuridiche, la verifica deve essere effettuata per il/gli amministratori) idonea dichiarazione, resa nelle forme di cui al D.P.R. n. 445 del 2000, con la quale lo stesso dichiari:
  - di non avere precedenti penali;
  - di non avere avuto precedenti rapporti di dipendenza e/o di collaborazione con pubbliche amministrazioni;
  - di non avere rapporti di parentela o affinità sino al secondo grado e/o di coniugio

con dipendenti e/o collaboratori di pubbliche amministrazioni.

- Qualora intenda procedere con il conferimento di un incarico a un collaboratore esterno che si trovi in una o più delle situazioni a rischio indicate nel Modello, indica per iscritto gli specifici motivi di tale incarico e richiede l'approvazione del Responsabile Amministrativo e Finanziario.
- Previa consultazione con l'Organismo di Vigilanza, è responsabile del rapporto con i collaboratori esterni operanti per conto dell'Unità Organizzativa per tutti gli aspetti relativi all'attuazione del Modello, e in particolare:
  - porta a conoscenza del collaboratore esterno il Codice Etico e di Comportamento Mizar e il Modello;
  - fa sottoscrivere apposita dichiarazione con la quale lo stesso di obbliga al rispetto delle leggi, del Codice Etico e di Comportamento Mizar e del Modello, pena la risoluzione immediata del rapporto.

11.3.5. Dipendente

- Non deve adottare comportamenti tali da integrare i Reati contro la Pubblica Amministrazione o i Reati Societari o i Reati commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
- Non deve adottare comportamenti che, sebbene non integrino di per sé Reati contro la Pubblica Amministrazione o Reati Societari o i Reati commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, potrebbero potenzialmente diventarlo.
- Non deve adottare comportamenti in conflitto di interesse con la Pubblica Amministrazione o con la Società.
- Non deve adottare i comportamenti indicati ai precedenti punti sia direttamente, sia per interposta persona.
- Non deve richiedere, sollecitare, suggerire ad agenti, distributori, collaboratori od altri partner commerciali comportamenti vietati dal Modello.
- Ha l'obbligo di osservare il Codice Etico e di Comportamento (RIF. 2). In particolare, nel corso della sua attività per Mizar, si impegna a non indurre a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.
- Qualora ne venga a conoscenza, informa l'Organismo di Vigilanza dei procedimenti e/o provvedimenti provenienti da organi di polizia giudiziaria, o da qualsiasi autorità, dai quali risulti la commissione da parte di dipendenti e/o dirigenti e/o collaboratori esterni dei Reati e comunque la violazione del Modello.

11.3.6. Dipendente assegnato a mansioni nell'ambito delle aree a rischio per reati contro la Pubblica Amministrazione e per il reato di corruzione fra privati

- In aggiunta agli obblighi ed ai compiti indicati per tutti i dipendenti, deve osservare i protocolli seguenti:
  - per quanto riguarda le forniture, vedi allegato 4;
  - per quanto riguarda le donazioni di beni o di denaro, vedi allegato 5;
  - per quanto riguarda i contratti di consulenza, vedi allegato 6;
  - per quanto riguarda il finanziamento di borse di studio, vedi allegato 7;
  - per quanto riguarda i contratti di sponsorizzazione, vedi allegato 8;
  - per quanto riguarda l'erogazione ed utilizzo di finanziamenti, vedi allegato 14;
  - per quanto riguarda i pagamenti e le autorizzazioni di spesa, vedi allegato 15;
  - per quanto riguarda l'acquisto di beni e servizi, vedi allegato 16.
- prendere conoscenza degli eventuali codici di comportamento anticorruzione adottati dagli enti pubblici con cui il dipendente intrattiene rapporti e conformarsi agli stessi;
- consultare il Responsabile aziendale per l'applicazione del Modello prima di adottare un determinato comportamento, in caso di incertezza sulla liceità dello stesso;
- nel caso in cui non sia possibile osservare i Protocolli, preventivamente:
  - illustrare per iscritto gli specifici motivi di tale inosservanza;
  - ottenere l'autorizzazione scritta del soggetto di vertice della propria linea gerarchica;
- documentare in modo chiaro e trasparente tutti i passaggi della attività svolte.

I principi sopra elencati devono essere rispettati anche quando l'attività è svolta congiuntamente con altre società o comunque con terzi.

11.3.7. Dipendente assegnato a mansioni nell'ambito delle aree a rischio per reati societari

In aggiunta agli obblighi ed ai compiti indicati per tutti i dipendenti, deve:

- assicurare che la tenuta della contabilità avvenga in modo trasparente e conforme alle norme vigenti, e che i dati contabili siano validati da adeguata documentazione di supporto e dalla verifica di un controllore (Allegato 18);
- rispettare il calendario aziendale per la formazione del bilancio, della nota integrativa e della relazione sulla gestione (vedi Allegato 19);
- attuare le procedure periodiche di controllo volte ad assicurare la correttezza, completezza e accuratezza delle voci di bilancio, attraverso adeguata documentazione di supporto (Allegato 20)

- sottoporre al Collegio Sindacale la contabilità aziendale ed il bilancio ai fini della verifica della loro correttezza e regolarità;
- segnalare preventivamente all'Organismo di Vigilanza eventuali operazioni straordinarie in programma;
- documentare in modo chiaro, trasparente e completo tutte le informazioni necessarie per la redazione del bilancio e delle comunicazioni sociali;
- consultare il Responsabile aziendale per l'applicazione del Modello prima di adottare un determinato comportamento, in caso di incertezza sulla liceità dello stesso;
- nel caso in cui non sia possibile osservare i Protocolli, preventivo obbligo:
  - di illustrare per iscritto gli specifici motivi di tale inosservanza;
  - di ottenere l'autorizzazione scritta dell'Amministratore Unico.

11.3.8. Dipendente assegnato a mansioni nell'ambito delle aree a rischio per reati commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

In aggiunta agli obblighi ed ai compiti indicati per tutti i dipendenti, deve:

a) partecipare alla formazione periodica sui rischi per la salute e la sicurezza, le relative procedure e disposizioni aziendali e la normativa vigente in materia;

b) rispettare le procedure e le disposizioni aziendali in materia di prevenzione antinfortunistica ed igiene;

c) segnalare tutte le situazioni di rischio, anche al di fuori della propria area di competenza;

d) evitare comportamenti che possano porre a rischio la propria sicurezza e salute e quella dei colleghi;

e) sottoporsi alle visite di sorveglianza sanitaria previste dal piano di sorveglianza redatto dal medico competente.

12. Allegati

Allegato 1	Organismo di vigilanza
Allegato 2	Organizzazione interna di Mizar
Allegato 3	Fattispecie di reati contro la Pubblica Amministrazione
Allegato 4	Forniture
Allegato 5	Donazioni di beni o di denaro
Allegato 6	Contratti di consulenza
Allegato 7	Finanziamenti
Allegato 8	Acquisto di beni e di servizi
Allegato 9	Fattispecie di reati societari
Allegato 10	Tenuta della contabilità e documentazione dei dati contabili
Allegato 11	Procedure di controllo e validazione di saldi contabili
Allegato 12	Fattispecie di reati commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro
Allegato 13	Protocollo relativo alla sicurezza sul lavoro
Allegato 14	Fattispecie di reati informatici
Allegato 15	Protocollo prevenzione reati informatici
Allegato 16	Fattispecie di reati in materia di violazione del diritto d'autore
Allegato 17	Protocollo prevenzione reati in materia di violazione del diritto d'autore
Allegato 18	Protocollo prevenzione reati ambientali

Allegato 1

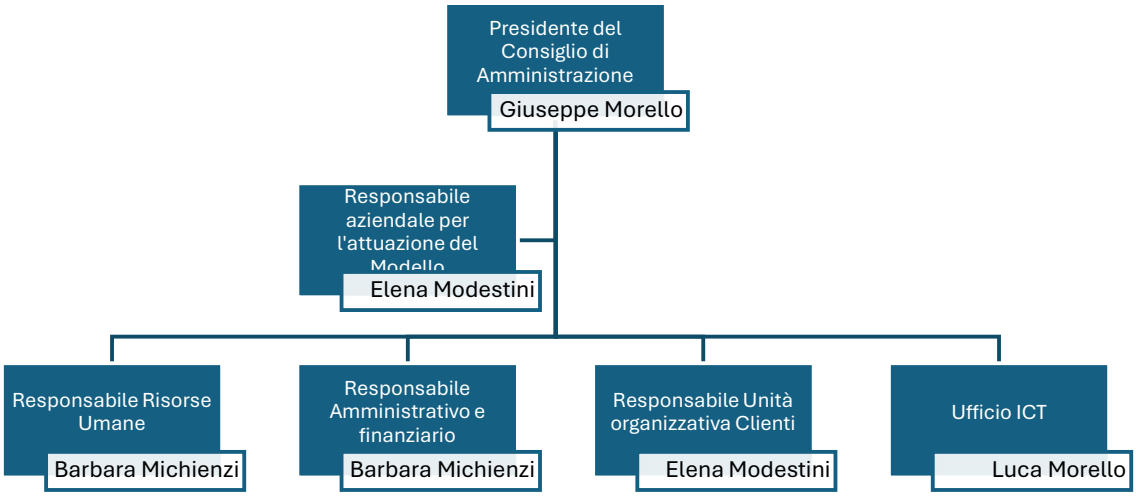
Organismo di Vigilanza

L'Organismo di Vigilanza è costituito in forma monocratica.

Il nominativo della persona incaricata è disponibile in Società.

Allegato 2

Organizzazione interna di Mizar International Insurance Brokers S.r.l. rispetto al MGOC



Allegato 3

Fattispecie di reati contro la Pubblica Amministrazione

Come precisato anche in altra parte del Modello, le fattispecie di reati contro la Pubblcia Amministrazione sono riconducibili alle seguenti:

- malversazione a danno dello Stato (art. 316-bis Codice penale): chiunque, estraneo alla Pubblica Amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee, contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da 6 mesi a 4 anni;
- indebita percezione di erogazioni a danno dello Stato (art. 316-ter, Codice penale): salvo che il fatto costituisca il reato previsto dall'art. 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle comunità europee, è punito con la reclusione da 6 mesi a 3 anni.

  Quando la somma indebitamente percepita è pari o inferiore a euro 3.999,96 si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da euro 5.164 a euro 25.822.

  Tale sanzione non può comunque superare il triplo del beneficio conseguito;
- concussione (art. 317, Codice penale): Il pubblico ufficiale che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro o altra utilità, è punito con la reclusione da 6 a 12 anni.;
- corruzione per l'esercizio della funzione (art. 318, Codice penale): Il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da 1 a 5 anni.

  Se il pubblico ufficiale riceve la retribuzione per un atto d'ufficio da lui già compiuto, la pena è della reclusione fino ad 1 anno;
- corruzione per un atto contrario ai doveri d'ufficio (art. 319, Codice penale): Il pubblico ufficiale, che, per omettere o ritardare o per aver omesso o ritardato, un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da 4 a 8 anni;

  circostanze aggravanti (art. 319bis, Codice penale): la pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei

quali si è interessata l'amministrazione alla quale il pubblico ufficiale appartiene.

- corruzione in atti giudiziari (art. 319-ter, Codice penale): Se i fatti indicati negli art. 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da 4 a 10 anni.

  Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a 5 anni, la pena è della reclusione da 5 a 12 anni; se deriva l'ingiusta condanna alla reclusione superiore a 5 anni o all'ergastolo, la pena è della reclusione da 6 a 20 anni;

- Induzione indebita a dare o promettere utilità (art. 319-quater, Codice penale): Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da tre a otto anni.

  Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni.

- corruzione di persona incaricata di pubblico servizio (art. 320, Codice penale): Le disposizioni degli articoli 318 e 319 si applicano anche all'incaricato di un pubblico servizio.

  In ogni caso, le pene sono ridotte in misura non superiore ad un terzo;

- pene per il corruttore (art. 321, Codice penale): Le pene stabilite nel primo comma dell'art. 318, nell'art. 319, nell'art. 319-bis, nell'art. 319-ter e nell'art. 320 in relazione alle suddette ipotesi degli art. 318 e 319, si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità.

- istigazione alla corruzione (art. 322, Codice penale): Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo.

  Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo.

  La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri.

  La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319.

- 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 Codice penale): Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo

e quarto comma, si applicano anche:

1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;

2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;

3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;

4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;

5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio.

Le disposizioni degli articoli 319-quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:

1) alle persone indicate nel primo comma del presente articolo;

2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali ovvero al fine di ottenere o di mantenere un'attività economica finanziaria.

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

- peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi della Comunità Europee e di funzionari della Comunità Europee e di Stati esteri (art. 322-bis, Codice penale): Le disposizioni degli art. 314, 316, da 317 a 320 e 322, III e IV c., si applicano anche: 1) ai membri della Commissione della Comunità europee, del parlamento europeo, della Corte di Giustizia e della Corte dei Conti della Comunità europee; 2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari della Comunità europee o del regime applicabile agli agenti della Comunità europee; 3) alle persone comandate dagli stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Comunità europee; 4) ai membri e agli addetti a enti costituiti sulla base dei trattati che istituiscono le Comunità europee; 5) a coloro che, nell'ambito di altri stati membri dell'unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali o degli incaricati di un pubblico servizio.

  Le disposizioni degli art. 321 e 322, I e II c., si applicano anche se il denaro o altra utilità è dato, offerto o promesso: 1) alle persone indicate nel I c. del presente art.; 2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali.

Le persone indicate nel I c. sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

- Traffico di influenze illecite (art. 346-bis codice penale): Chiunque, fuori dei casi di concorso nei reati di cui agli articoli 319 e 319-ter, sfruttando relazioni esistenti con un pubblico ufficiale o con un incaricato di un pubblico servizio, indebitamente fa dare o promettere, a sè o ad altri, denaro o altro vantaggio patrimoniale, come prezzo della propria mediazione illecita verso il pubblico ufficiale o l'incaricato di un pubblico servizio ovvero per remunerarlo, in relazione al compimento di un atto contrario ai doveri di ufficio o all'omissione o al ritardo di un atto del suo ufficio, è punito con la reclusione da uno a tre anni.

  La stessa pena si applica a chi indebitamente dà o promette denaro o altro vantaggio patrimoniale.

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

  Le pene sono altresì aumentate se i fatti sono commessi in relazione all'esercizio di attività giudiziarie.

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

- truffa (in danno dello Stato) (art. 640, comma 2, n. 1, Codice penale): chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da Euro 51 a Euro 1.032.

  La pena è della reclusione da uno a cinque anni e della multa da Euro 309 a Euro 1.549:

  1) se il fatto è commesso a danno dello stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare;

- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis, Codice penale): la pena è della reclusione da 1 a 6 mesi e si procede d'ufficio se il fatto di cui all'art. 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o della Comunità europee;

- frode informatica (art. 640-ter, Codice penale): Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da 6 mesi a 3 anni e con la multa da Euro 51 a Euro 1.032.

  La pena è della reclusione da 1 a 5 anni e della multa da Euro 309 a Euro 1.549 se ricorre una delle circostanze prevista dal n. 1) del secondo comma dell'art. 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

  Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

Allegato 4

Forniture

È fatto divieto assoluto di tentare di migliorare o di influenzare in qualsiasi modo, direttamente o indirettamente, con mezzi illeciti o in ogni modo non corretti, l'esito di procedure di gara o negoziazione indette da soggetti pubblici o privati, italiani od esteri in merito all'acquisto di prodotti Mizar.

Nella formulazione dell'offerta la descrizione delle caratteristiche del prodotto o servizio oggetto dell'offerta deve essere coerente con quanto indicato nella documentazione ufficiale delle Società assicurative.

Allegato 5

Donazioni di beni mobili o di denaro

La donazione è un contratto con il quale Mizar può disporre gratuitamente a favore di un terzo di una somma di denaro, di beni mobili o altra utilità. Non si considera donazione l'omaggio di beni di valore trascurabile elargiti a persone fisiche, nel rispetto delle limitazioni previste dal Codice Etico e di Comportamento.

La donazione dovrà essere considerata uno strumento di carattere eccezionale, dovendosi preferire l'utilizzo di altri modelli contrattuali per realizzare l'attribuzione patrimoniale.

Qualora la donazione abbia ad oggetto denaro o altri beni mobili è necessario valutare se la donazione possa essere considerata o meno di modico valore. Questa valutazione andrà effettuata tenuto conto sia del valore del bene, sia delle condizioni economiche di Mizar al momento della donazione. La donazione non potrà essere considerata di modico valore qualora incida in modo apprezzabile sul patrimonio di Mizar (per la procedura vedi Fase Operativa).

Ipotesi in cui è possibile fare ricorso alla donazione

- si deve trattare di un'attribuzione patrimoniale a titolo gratuito. Mizar non dovrà ricevere alcun corrispettivo in relazione alla stessa;
- l'attribuzione patrimoniale deve essere fatta per spirito di liberalità, ovverosia con la consapevolezza di attribuire ad altri un vantaggio patrimoniale senza che ciò comporti a carico dei beneficiari alcun obbligo giuridico o extra giuridico e senza alcun interesse di carattere patrimoniale per Mizar;
- la decisione di donare deve avvenire in maniera spontanea.

In assenza di tali requisiti, non si potrà far ricorso alla donazione, ma occorrerà di volta in volta verificare a quale diversa fattispecie contrattuale l'attribuzione patrimoniale possa essere ricondotta (es. contratti di sponsorizzazione, contratti di consulenza, etc.).

ipotesi in cui non è consentito effettuare donazioni

- Mizar non può effettuare donazioni di beni immobili.
- la donazione di denaro, beni mobili o altra utilità è consentita solo se di modico valore ai sensi dell'articolo 783 c.c. A tal fine è necessario valutare caso per caso se la donazione possa essere considerata o meno di modico valore. Questa valutazione andrà effettuata tenuto conto sia del valore del bene, sia delle condizioni economiche di Mizar al momento della donazione. La donazione non potrà essere considerata di modico valore qualora incida in modo apprezzabile sul patrimonio di Mizar (per la procedura vedi Fase Operativa).
- Il ricorso alla donazione dovrà essere escluso in tutti i casi in cui oggetto della stessa siano prodotti o servizi, che richiedano per il loro utilizzo l'acquisto di prodotti o servizi Mizar. La donazione non può

essere infatti utilizzata come strumento per aggirare l'applicazione delle procedure ad evidenza pubblica per la fornitura di prodotti o servizi.

I destinatari della donazione

Nessuna donazione può essere in ogni caso effettuata a favore di persone fisiche.

In linea generale, non è consentito effettuare donazioni a favore dei seguenti soggetti:

a. strutture pubbliche o private che siano clienti o potenziali clienti di Mizar;

b. società, associazioni, fondazioni ed in ogni caso persone giuridiche i cui membri, soci o amministratori, o parte di essi, siano medici, personale direttivo, personale ausiliario e dipendenti in genere di strutture pubbliche o private che siano clienti o potenziali clienti di Mizar.

In via eccezionale e fermo restando il divieto assoluto di effettuare donazioni a favore di persone fisiche, potranno essere effettuate donazioni a favore dei soggetti di cui ai punti a) e b) solo previa approvazione espressa del Presidente del Consiglio di amministrazione.

In ogni caso è necessario evitare che il destinatario della donazione possa, direttamente o indirettamente, influenzare l'aggiudicazione di forniture di prodotti a favore di Mizar. È pertanto necessario che:

- destinatario della donazione sia l'ente o l'associazione e mai il singolo individuo;
- fermo restando quanto sopra, invitare le persone che beneficiano, anche indirettamente, della donazione e che hanno potere decisorio in merito all'aggiudicazione di forniture, ad evitare qualsiasi comportamento che possa configurare conflitto di interesse.

Procedura aziendale

La richiesta di donazione deve essere approvata dall'Presidente del Consiglio di amministrazione, previo parere dell'Organismo di Vigilanza.

Non potrà essere disposta più di una donazione nei confronti di uno stesso soggetto durante il medesimo anno.

Conservazione della documentazione

Il Servizio Amministrativo e Finanziario conserverà copia della seguente documentazione relativa alla donazione:

1) "PROPOSTA DI DONAZIONE/CONTRIBUTI A ISTITUTI, ENTI, ASSOCIAZIONI, ECC.", sottoscritto dal proponente, dal Direttore dal Servizio Amministrativo e Finanziario e dal Presidente del Consiglio di amministrazione di Mizar;

2) comunicazione sottoscritta dal Presidente del Consiglio di amministrazione, inviata da Mizar al beneficiario, contenente la volontà di donare;

3) lettera di accettazione della donazione da parte del beneficiario;

4) qualora destinatario della donazione sia una società, un'associazione, una fondazione o una persona giuridica i cui membri, soci e/o amministratori, o parte di essi, siano dipendenti di una struttura pubblica o privata, copia della comunicazione di cui al punto 2);

5) se il beneficiario è un ente privato, copia dell'atto costitutivo e dello statuto dell'ente; se il beneficiario è un ente pubblico, copia della delibera di accettazione della donazione e originale della lettera di accompagnamento;

6) se la donazione non è di modico valore, copia dell'atto pubblico con cui è stata disposta la donazione, nonché il successivo atto pubblico con cui il beneficiario ha accettato la donazione (fatta eccezione per il caso in cui l'accettazione sia stata espressa nel medesimo atto con cui è stata disposta).

mizar International Insurance Brokers	Modulo di proposta di donazione/contributi a istituti, enti, associazioni, ecc.
Unità organizzativa richiedente	
Tipo destinatario (*)	
Destinatario della donazione	
Tipo di donazione	( ) denaro ( ) beni materiali
In caso di donazione di beni materiali, descrivere dettagliatamente i beni oggetto della donazione	
Valore della donazione (in euro)	
Motivazioni della donazione	
Qualora la donazione sia effettuata per contribuire alla realizzazione di un progetto e/o di un evento, descriverne le caratteristiche e la tempistica di realizzazione	
Eventuali rapporti esistenti fra Mizar ed il beneficiario	
Eventuali altre donazioni effettuate in passato da Mizar a favore del medesimo beneficiario	
Data e firma del Responsabile della Unità Organizzativa richiedente	
Data e firma del Responsabile Amministrativo e Finanziario	
Date e firma per autorizzazione del Presidente del Consiglio di amministrazione	

Allegato 6

Contratti di consulenza

I contratti di consulenza hanno per oggetto la prestazione di un'attività di consulenza da parte (i) di una struttura pubblica o privata, (ii) di un dipendente di una struttura pubblica o privata, (iii) da parte di società, associazioni, fondazioni o persone giuridiche i cui membri, soci e/o amministratori siano anche dipendenti di strutture pubbliche o private, ovvero (iv) da parte di privati persone fisiche. L'attività di consulenza può avere ad oggetto ad esempio: (i) l'organizzazione e la realizzazione di corsi di formazione; (ii) la realizzazione di video o altro materiale relativo all'utilizzo dei prodotti Mizar; (iii) la redazione di studi o pubblicazioni o di manuali; (iv) quanto altro possa essere considerato prestazione d'opera intellettuale.

Regole generali:

1. *i contratti di consulenza devono essere stipulati solo nel caso in cui vi sia un interesse serio, concreto ed attuale da parte di Mizar;*
2. *l'inizio della prestazione deve essere sempre preceduto dalla stipulazione del relativo contratto secondo la procedura esposta qui di seguito;*
3. *non possono essere trasmesse al Servizio Amministrativo e Finanziario fatture relative a prestazioni eseguite prima della stipulazione del relativo contratto, conformemente alla procedura esposta qui di seguito;*
4. *è necessario verificare sempre la congruità tra corrispettivo pagato e prestazione resa in base ai prezzi di mercato;*
5. *è necessario fornire al Servizio Amministrativo e Finanziario tutte le informazioni utili e/o necessarie per consentire al Servizio Amministrativo e Finanziario di valutare la questione e redigere il relativo testo contrattuale; è necessario altresì rispondere tempestivamente a richieste di informazioni e/o chiarimenti aggiuntivi;*
6. *potrà essere stipulato un solo contratto di consulenza con i soggetti di cui sopra all'anno.*

a) Procedura aziendale per la stipulazione di contratti di consulenza con strutture pubbliche o private

Mizar non stipula di norma contratti di consulenza con i soggetti di cui sopra; ove fosse necessario per ragioni di business, il contratto viene stipulato solo dopo aver consultato l'Organismo di Vigilanza

b) Procedura aziendale per la stipulazione di contratti di consulenza con le società, le associazioni, le fondazioni o le persone giuridiche (qui di seguito "persone giuridiche") i cui membri, soci e/o amministratori siano anche dipendenti di strutture pubbliche o private

Fase Preliminare

1) La struttura interessata inoltra la richiesta di stipulazione del contratto con le Persone Giuridiche al Servizio Amministrativo e Finanziario, con indicazione dei seguenti elementi:
   - statuto e atto costitutivo della Persona Giuridica;
   - partita IVA o codice fiscale della Persona Giuridica;
   - tipologia, oggetto e specifiche finalità del contratto;
   - importo da corrispondere e dichiarazione del Responsabile della Direzione in merito alla congruità del corrispettivo e, ove possibile, criteri per la sua determinazione;
   - nome e cognome del dipendente/dei dipendenti che eventualmente eseguono la prestazione oggetto del contratto, nell'ambito del lavoro svolto presso la Persona Giuridica;
   - nome del Direttore Generale della struttura (da cui i membri, soci e/o amministratori della Persona Giuridica dipendono) con indicazione della relativa sede;
   - ente ospitante e luogo della tenuta dei corsi (ove richiesto);
   - la persona che ha inoltrato la richiesta dovrà ottenere l'autorizzazione da parte dell' Presidente del Consiglio di amministrazione.

Fase Operativa

Il richiedente dovrà verificare che la Persona Giuridica i cui membri, soci e/o amministratori siano anche dipendenti di strutture pubbliche o private non sia uno schermo utilizzato dai dipendenti per conseguire incarichi di consulenza eludendo l'applicazione della relativa normativa o comunque evitando di informare la struttura di appartenenza

c) Procedura aziendale per la stipulazione di contratti di consulenza con i privati

Fase Preliminare

La struttura interessata sottopone la richiesta di stipulazione del contratto con il privato al Servizio Amministrativo e Finanziario, con indicazione dei seguenti elementi:

- nome e cognome del soggetto;
- indirizzo completo di residenza;
- partita IVA o codice fiscale del soggetto;
- oggetto del contratto;

- importo da corrispondere e dichiarazione in merito alla congruità del compenso e, ove possibile, criteri per la sua determinazione;
- ente ospitante e luogo della tenuta dei corsi (ove pertinente).

Fase Operativa

1) Una volta ricevuta la richiesta, il Servizio Amministrativo e Finanziario provvede a predisporre il contratto da stipulare con il privato.
2) Il Servizio Amministrativo e Finanziario trasmette al Presidente del Consiglio di amministrazione il contratto per la firma.
3) Il Servizio Amministrativo e Finanziario dovrà comunicare trimestralmente all'Organismo di Vigilanza l'elenco dei contratti di consulenza stipulati con i privati.

Allegato 7

Finanziamenti

Il Responsabile Amministrativo e Finanziario dovrà verificare almeno ogni 6 (sei) mesi che le somme oggetto di finanziamenti siano state destinate ai fini per i quali sono state erogate.

L'elenco dei finanziamenti erogati, con l'indicazione della relativa destinazione, dovrà essere fornito semestralmente all'Organismo di Vigilanza.

Allegato 8

Acquisto di beni e di servizi

In merito all'acquisto di beni, il pagamento dei beni acquistati può essere effettuato solo previa verifica di quanto segue:

1. della conformità di quanto consegnato a quanto ordinato;
2. della consegna degli stessi;
3. dell'esistenza del relativo documento di trasporto.

In merito all'acquisto di servizi, deve essere osservato quanto segue:

1. redazione dell'elenco dei fornitori abituali;
2. verifica semestrale da parte dal Servizio Amministrativo e Finanziario dei nominativi dei fornitori di servizi;
3. controllo a campione da parte dal Servizio Amministrativo e Finanziario dell'effettività dei servizi forniti da parte fornitori non abituali;
4. il beneficiario del servizio deve dichiarare di aver ricevuto effettivamente il servizio in esame mediante firma della relativa fattura.

Si considerano non abituali i fornitori di servizi che abbiano rapporti con Mizar da meno di tre (3) anni.

Allegato 9

Fattispecie dei reati societari

False comunicazioni sociali, anche se a danno dei soci e creditori (artt. 2621 e 2622 c.c.)

Tale ipotesi di reato si configura nel caso in cui, gli amministratori, i direttori generali, i sindaci e i liquidatori, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, espongano fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero omettano informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale, o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione.

Tale fattispecie può realizzarsi anche nel caso in cui si cagioni un danno patrimoniale agli stessi soci o ai creditori.

La punibilità è esclusa se le falsità o le emissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene.

In concreto, può integrarsi il reato in esame qualora un amministratore delegato, ignorando l'indicazione del responsabile amministrativo, iscriva, ad esempio, un ammontare di crediti superiore al dovuto, al fine di non fare emergere una perdita.

Falso in prospetto (art. 2623 c.c.)

Tale ipotesi di reato si configura nel caso in cui, allo scopo di perseguire per sé o per altri un ingiusto profitto, nei prospetti richiesti ai fini della sollecitazione all'investimento o dell'ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari del prospetto, si espongano false informazioni o si occultino dati o notizie in modo idoneo ad indurre in errore i suddetti destinatari.

In concreto, questi reati sono commessi il più delle volte da chi formalmente è responsabile di questi documenti e cioè il Consiglio di Amministrazione nella sua collegialità. Tuttavia, è altresì possibile che reati di questo genere siano commessi da "sottoposti" dei responsabili di funzione, dotati di un certo potere discrezionale ancorché circoscritto. In tali casi il reato potrà dirsi consumato solo se la falsità sia consapevolmente condivisa dai soggetti "qualificati" che nel recepire il dato falso lo fanno proprio inserendolo nella comunicazione sociale.

Falsità nelle relazioni o comunicazioni delle società di revisione (art. 2624 c.c.)

Tale ipotesi di reato si configura nel caso in cui i responsabili della revisione, al fine di conseguire per sé o per altri un ingiusto profitto, nelle relazioni o in altre comunicazioni, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni, attestino il falso od occultino informazioni concernenti la situazione economica, patrimoniale o finanziaria della società, ente o

soggetto sottoposto a revisione, in modo idoneo ad indurre in errore i destinatari delle comunicazioni sulla predetta situazione.

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

Tale ipotesi di reato si configura nel caso in cui gli amministratori, occultando documenti o con altri idonei artifici, impediscano o comunque ostacolino lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali o alle società di revisione, cagionando in tal modo un danno ai soci.

Si precisa come il fatto debba essere realizzato nell'interesse della società e non, ad esempio, di amministratori e di una parte della compagine sociale.

In concreto, può integrarsi il reato in esame qualora ad esempio un amministratore occulti, anche per mezzo di artifici, documentazione utile a rappresentare i processi applicativi in sede aziendale di una specifica normativa.

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

Tale ipotesi di reato si configura nel caso in cui gli amministratori e i soci conferenti, anche in parte, formino o aumentino fittiziamente il capitale della società mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

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

Tale ipotesi di reato si configura nel caso in cui gli amministratori, fuori dei casi di legittima riduzione del capitale sociale, restituiscano, anche simultaneamente, i conferimenti ai soci o li liberino dall'obbligo di eseguirli.

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

Tale ipotesi di reato si configura nel caso in cui gli amministratori ripartiscano utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartiscano riserve, anche non costituite con utili, che non possono per legge essere distribuite.

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

Illecite operazioni su azioni o quote sociali (art. 2628 c.c.)

Tale ipotesi di reato si configura nel caso in cui gli amministratori, fuori dai casi consentiti dalla legge, acquistino o sottoscrivano azioni o quote sociali cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

Tale reato può essere commesso anche da amministratori che, fuori dei casi consentiti dalla legge, acquistino o sottoscrivano azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del

bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

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

Tale ipotesi di reato si configura nel caso in cui gli amministratori, in violazione delle disposizioni di legge a tutela dei creditori, effettuino riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.

Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

È interessante rilevare come l'attuale formula aperta, usata dalla disposizione novellata, consenta di ipotizzare la concretizzazione di questo reato anche ad esempio nel caso in cui l'amministratore abbia proceduto alle descritte operazioni di riduzione, fusione o scissione in situazione di conflitto di interessi con la società ed in violazione delle disposizioni previste dal novellato art. 2634 c.c.

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

Tale ipotesi di reato si configura nel caso in cui l'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1° settembre 1993, n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998, del decreto legislativo 7 settembre 2005, n. 209, o del decreto legislativo 21 aprile 1993, n. 124, violi gli obblighi previsti dall'art. 2391, primo comma, cagionando danni alla società o a terzi.

L'ipotesi di maggiore rilievo, che richiede quindi una più attenta valutazione ai fini della predisposizione di adeguate misure di controllo idonee a prevenire la commissione del reato di specie, sembra essere quella in cui la condotta omissiva dell'amministratore abbia causato danni non alla società di appartenenza, bensì ai terzi che sono venuti in contatto ed hanno concluso con la società medesima rapporti giuridici di qualsiasi genere.

In concreto, può integrarsi il reato in esame qualora, ad esempio, l'amministratore delegato di una società quotata non dichiari volutamente al CdA il suo interesse personale o di suoi familiari in una determinata operazione all'esame del Consiglio di Amministrazione.

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

Tale ipotesi di reato si configura nel caso in cui i liquidatori, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionino un danno ai creditori.

Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Corruzione e istigazione alla corruzione tra privati (art. 2635, comma 3 e art. 2635-bis, comma 1 c.c.)

Tali ipotesi di reato si configurano qualora un soggetto offra, dia o prometta denaro o altre utilità non dovuta agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci, ai liquidatori e comunque a coloro che siano sottoposti alla direzione o

alla vigilanza di uno di tali soggetti al fine del compimento o dell'omissione di atti in violazione dei doveri d'ufficio o dell'obbligo di fedeltà, cagionando nocumento alla di loro società.

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

Tale ipotesi di reato si configura nel caso in cui, con atti simulati o fraudolenti, si determini la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto.

Si precisa che la responsabilità dell'ente è configurabile solo quando la condotta prevista dall'articolo in esame sia realizzata nell'interesse dell'Ente

In concreto, può integrarsi il reato in esame qualora l'amministratore delegato, ad esempio, predisponga apposita documentazione falsa o comunque alterata ai fini della deliberazione dell'assemblea su uno specifico ordine del giorno.

Aggiotaggio (art. 2637 c.c.)

Tale ipotesi di reato si configura nel caso in cui, diffondendo notizie false, ovvero ponendo in essere operazioni simulate o altri artifici, si provochi una sensibile alterazione del prezzo di strumenti finanziari, quotati o non quotati, ovvero si incida in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.

Si precisa che per l'esistenza del reato è sufficiente una situazione di pericolo, indipendentemente dal verificarsi di una variazione artificiosa dei prezzi.

In concreto, può integrarsi il reato in esame qualora il dipendente di una società diffonda alla stampa notizie false sulla società medesima, in modo da determinare una sensibile alterazione del prezzo riguardante il titolo azionario di detta società.

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

Tale ipotesi di reato si configura nel caso in cui gli amministratori, i direttori generali, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongano fatti materiali non rispondenti al vero sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza, ovvero occultino con altri mezzi fraudolenti, fatti che avrebbero dovuto comunicare, concernenti la situazione medesima.

Tale reato può essere commesso anche da amministratori, direttori generali, sindaci e liquidatori di società, o da enti e soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti a obblighi nei loro confronti che, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolino le funzioni.

In concreto, può integrarsi il reato in esame qualora gli amministratori di società quotata in borsa, ad esempio, trasmettano alla Consob il progetto di bilancio con relazioni e allegati, riportando notizie false relativamente a determinate rilevanti operazioni sociali al fine di evitare possibili controlli da parte della Consob.

Allegato 10

Tenuta della contabilità e documentazione dei dati contabili

Ogni operazione che produca effetto sulla situazione economico patrimoniale dell'azienda deve essere prontamente e sistematicamente annotata secondo i principi contabili di riferimento e le norme di legge in vigore (artt. 2423 e ss del Codice civile).

Le scritture contabili devono essere supportate da idonea documentazione e sottoposte a validazione da parte di un controllore (persona diversa da chi ha redatto la prima nota) prima di essere inserite nel sistema contabile.

Prova del controllo è la sigla del controllore apposta sulla copia cartacea della prima nota, che deve essere archiviata secondo la numerazione attribuita automaticamente dal sistema contabile.

Allegato 11

Procedure di controllo e validazione di saldi contabili

Con cadenza periodica e almeno ogni trimestre, tutti i saldi patrimoniali devono essere oggetto di controllo e validazione attraverso la riconciliazione degli stessi con la documentazione di supporto e attraverso la ricostruzione della movimentazione dei saldi da un periodo a quello successivo.

In particolare:

- i saldi contabili di cassa devono essere corrispondenti alla conta fisica di cassa;
- i saldi bancari devono essere regolarmente sottoposti a riconciliazione bancaria, e le riconciliazioni bancarie devono essere controllate e firmate dal responsabile amministrativo, o comunque da persona diversa da chi ha preparato le riconciliazioni bancarie;
- i saldi relativi ai crediti e ai debiti commerciali devono essere corrispondenti alle risultanze dei relativi partitari;
- i saldi relativi alle partite intra gruppo (crediti, debiti, finanziamenti) devono essere regolarmente riconciliati con i saldi risultanti alla controparte, dalla quale deve essere ottenuta conferma scritta delle risultanze;
- lo scadenziario dei crediti verso clienti e dei debiti verso fornitori deve essere regolarmente sottoposto al responsabile amministrativo per il controllo;
- i saldi relativi alle rimanenze devono essere corrispondenti alla conta fisica delle giacenze e la loro valutazione deve essere documentata e ripercorribile, nonché validata dal responsabile amministrativo, o comunque da persona diversa da chi ha effettuato la valutazione delle giacenze;
- i saldi relativi alle immobilizzazioni devono essere corrispondenti alle risultanze del libro cespiti, e la movimentazione dei saldi deve essere adeguatamente riconciliata e documentata;
- i saldi relativi alle partite aperte nei confronti dei dipendenti devono essere riconciliati con la documentazione di supporto e validati dal responsabile Risorse Umane;
- i saldi relativi ad accantonamenti per fatture e note credito da ricevere da fornitori devono essere documentati da idonea documentazione di supporto e periodicamente controllati dal responsabile amministrativo, o da persona diversa da chi ha determinato gli accantonamenti;
- i saldi relativi ad accantonamenti per fatture e note credito da emettere a clienti devono essere documentati da idonea documentazione di supporto e periodicamente controllati dal responsabile amministrativo, o da persona diversa da chi ha determinato gli accantonamenti;
- i saldi relativi alle imposte correnti e differite devono essere validati da parte del responsabile amministrativo e con riferimento ai saldi di fine anno anche da un consulente esterno fiscalista;
- ogni altro saldo di bilancio deve essere ciclicamente oggetto di controllo da parte del responsabile amministrativo, o da persona diversa da chi ha determinato il saldo stesso.

Allegato 12

Fattispecie di reati commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

- Omicidio colposo (articolo 589 del codice penale)

  1) Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni. Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da uno a cinque anni. Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni dodici.

- Lesioni personali colpose gravi o gravissime (articolo 590, comma 3, del codice penale)

  1) Chiunque cagiona ad altri, per colpa, una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a lire seicentomila.

  2) Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da lire duecentoquarantamila a un milione duecentomila; se è gravissima, della reclusione da tre mesi a due anni o della multa da lire seicentomila a due milioni quattrocentomila.

  3) Se i fatti di cui al precedente capoverso sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro, la pena per le lesioni gravi è della reclusione da due a sei mesi o della multa da lire quattrocentottantamila a un milione duecentomila; e la pena per lesioni gravissime è della reclusione da sei mesi a due anni o della multa da lire un milione duecentomila a due milioni quattrocentomila.

  4) Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque.

  5) Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale.

Allegato 13

Protocollo sulla sicurezza sul lavoro

Mizar adotta una serie di procedure e disposizioni in materia di prevenzione antinfortunistica ed igiene, che, oltre ad essere conformi a quanto previsto dal D. Lgs. 81/2008, pongono vincoli ulteriori al fine di ridurre al minimo i rischi connessi in coerenza con la politica aziendale di salute, sicurezza e ambiente, nel garantire un luogo di lavoro salubre e sicuro per tutti coloro i quali svolgono la loro prestazione, a qualunque titolo, presso le sedi della Società.

Mizar ha in atto un programma di accoglienza per i nuovi assunti che prevede uno specifico addestramento in materia di salute e sicurezza in azienda e comprende anche la consegna di un manuale contenente i necessari riferimenti alla normativa vigente ed alle procedure e disposizioni aziendali.

Allegato 14

Fattispecie dei reati informatici

Con Legge 18 marzo 2008 n. 48 – "Ratifica ed esecuzione della Convenzione del Consiglio d‟Europa sulla criminalità informatica", assunta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno - è stato introdotto, nel D. Lgs 231/2001, l'art. 24 bis con rubrica "Delitti informatici e trattamento illecito di dati."

Art. 24-bis. D. Lgs. nr. 231/01.

Delitti informatici e trattamento illecito di dati

"In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.

In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)".

* * *

Art. 491-bis c.p.

Documenti informatici

"Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private".

Tale ipotesi di reato può configurarsi qualora alcuna delle falsità previste nel Libro II, Titolo VII, Capo III del codice penale (segnatamente i reati di cui agli artt. 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 490 c.p. in tema di falsità in atti pubblici e scrittura privata) riguardi un documento informatico pubblico o privato, avente efficacia probatoria.

Art. 615-ter c.p.

Accesso abusivo ad un sistema informatico o telematico

“Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione t totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio”.

Tale ipotesi di reato può configurarsi in caso di accesso abusivo ad un sistema informatico o telematico o in caso di permanenza all'interno dello stesso contro la volontà espressa o tacita di chi ha il diritto di escluderlo. Pene differenti sono previste qualora il reato sia commesso, abusando della sua posizione, da un pubblico ufficiale o da un incaricato di un pubblico servizio, ovvero nel caso in cui dal fatto sia derivata la distruzione o il danneggiamento del sistema, dei dati, delle informazioni o dei programmi in esso contenuti o l'interruzione totale o parziale del funzionamento.

Art. 615-quater c.p.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

“Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater”.

Tale ipotesi di reato può configurarsi in caso di acquisizione, circolazione abusiva o aggiramento di parole chiave o altri codici di accesso a sistemi informatici o telematici.

Art. 615-quinquies c.p.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

“Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l’interruzione, totale o parziale, o l’alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329”.

Tale ipotesi di reato può configurarsi qualora allo scopo di danneggiare illecitamente un sistema informatico o telematico e i dati, informazioni o programmi in esso contenuti o pertinenti, o al fine di favorirne l'interruzione totale o parziale o la manipolazione del suo funzionamento, ci si procuri o si producano, riproducano, importino, diffondano, comunichino, consegnino o, comunque si mettano a disposizione di terzi apparecchiature, dispositivi o programmi informatici.

Art. 617-quater c.p.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

“Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato”.

Tale ipotesi di reato può configurarsi qualora siano intercettate, impedite o interrotte fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi. Nel caso in cui il reato sia compiuto in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico è prevista una pena più grave. Lo stesso avviene nel caso in cui il fatto sia posto in essere da un pubblico ufficiale o da un incaricato di pubblico servizio o dall'operatore del sistema i quali compiono il reato abusando dei loro poteri.

Art. 617-quinquies c.p.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

“Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più

sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater".

Tale ipotesi di reato può configurarsi qualora vengano installate, fuori dai casi previsti dalla legge, apparecchiature idonee ad intercettare, impedire o interrompere 103 comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

Art. 635-bis c.p.

Danneggiamento di informazioni, dati e programmi informatici

"Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio."

Tale ipotesi di reato può configurarsi qualora siano deteriorati, alterati o cancellati dati, informazioni o programmi informatici altrui. Se il reato è stato compiuto con violenza fisica o psicologica o se a commetterlo sia un operatore del sistema abusando della sua qualità è prevista una pena più grave.

Art. 635-ter c.p.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

"Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

Tale ipotesi di reato può configurarsi qualora siano deteriorati, alterati o cancellati dati, informazioni o programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità. Qualora il deterioramento, l'alterazione o la cancellazione abbiano avuto i loro effetti, la pena è aumentata. Se il reato è stato compiuto con violenza fisica o psicologica o se a commetterlo sia un operatore del sistema abusando della sua qualità è prevista una pena più grave.

Art. 635-quater c.p.

Danneggiamento di sistemi informatici o telematici

"Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all"articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

Tale ipotesi di reato può configurarsi qualora siano distrutti, danneggiati o resi in tutto o in parte inservibili sistemi informatici o telematici altrui attraverso la distruzione, deterioramento, cancellazione, soppressione, introduzione o la trasmissione di dati, informazioni o programmi. Se il reato e' stato compiuto con violenza fisica o psicologica o se a commetterlo è un operatore del sistema abusando della sua qualità è prevista una pena più grave.

Art. 635-quinquies c.p.

Danneggiamento di sistemi informatici o telematici di pubblica utilità

"Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

Tale ipotesi di reato può configurarsi qualora siano distrutti, danneggiati o resi in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità attraverso la distruzione, deterioramento, cancellazione, soppressione, introduzione o la trasmissione di dati, informazioni o programmi. Se il reato è stato compiuto con violenza fisica o psicologica o se a commetterlo sia un operatore del sistema abusando della sua qualità è prevista una pena più grave.

Art. 640-quinquies c.p.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

"Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a se´ o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro".

Tale ipotesi di reato può configurarsi nel caso in cui chi certifica firme elettroniche violi obblighi di legge per il rilascio delle stesse, al fine di procurare a sé od altri un ingiusto profitto o di arrecare ad altri un danno.

La legge n.90 del 2024 ha inasprito le sanzioni per l'accesso abusivo ai sistemi informatici e i reati informatici in generale, come l'estorsione digitale.

Allegato 15

Protocollo prevenzione reati informatici

A. Le aree di rischio e le funzioni aziendali coinvolte con riferimento ai reati di cui all'art. 24- bis del D.Lgs. 231/01

Per le attività svolte dal Servizio Information Technology (di seguito "IT") si possono individuare le seguenti aree a rischio reato, connesse all'utilizzo dei sistemi informativi:

1. creazione account per accesso a sistemi informatici aziendali;
2. attribuzione di password di accesso a sistemi informatici sensibili;
3. utilizzo pc aziendale;
4. immissione/gestione/utilizzo dei dati aziendali nei sistemi informatici aziendali;
5. utilizzo dei pc aziendali per accesso a sistemi esterni;
6. gestione dati e informazioni riservati;
7. manutenzione dei pc (interventi periodici e straordinari);
8. programmazione di sistemi informatici personalizzati;
9. adattamento/aggiornamento di sistemi informatici aziendali;
10. perdita dei dati;
11. utilizzo/gestione telefoni cellulari.

Possibili modalità di commissione dei reati nei confronti dei soggetti pubblici e/o privati

Nel Servizio IT si rendono astrattamente possibili "reati presupposto" di diverso tipo, collegati direttamente o indirettamente con l'uso di strumenti informatici e telematici. Anzitutto possono commettersi reati in tema di falsità documentali (in/con documentazione informatica), frode informatica, ovvero accesso abusivo a sistema informatico o telematico (ad es. del Ministero della Salute o enti ispettivi, con cui la società ha rapporti, od anche di una società concorrente).

Qui di seguito un elenco (non esaustivo) di ipotesi di condotta che possono integrare uno dei reati presupposto di cui all'art. 24-bis D. Lgs. 231/2001:

- falsità di documento informatico privato;
- falsità di documento informatico pubblico;
- abusiva introduzione in un sistema informatico/telematico;

- permanenza all'interno di un sistema informatico/telematico contro la volontà espressa o tacita del titolare dello ius excludendi;
- abusivo procacciamento di codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza;
- abusiva diffusione di codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza;
- abusiva comunicazione di codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza;
- abusiva consegna di codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza;
- comunicazione a terzi di indicazioni o istruzioni atte a accedere illegittimamente ad un sistema informatico o telematico;
- cessione di programma informatico, idoneo al danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- diffusione di programma informatico idoneo al danneggiamento di un sistema informatico o telematico, dei dati o dei programmi un esso contenuti o a esso pertinenti ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- intercettazione fraudolenta di comunicazioni intervenute all'interno di un sistema informatico o telematico o intercorrenti tra più sistemi;
- impedimento fraudolento di comunicazioni svolgentisi all'interno di un sistema informatico o telematico o intercorrenti tra più sistemi;
- interruzione fraudolenta di comunicazioni svolgentisi all'interno di un sistema informatico o telematico o intercorrenti tra più sistemi;
- intercettazione fraudolenta di comunicazioni intervenute all'interno di un sistema informatico o telematico o intercorrenti tra più sistemi utilizzati dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- impedimento fraudolento di comunicazioni svolgentisi all'interno di un sistema informatico o telematico o intercorrenti tra più sistemi utilizzati dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- interruzione di comunicazioni di comunicazioni svolgentisi all'interno di un sistema informatico o telematico o intercorrenti tra più sistemi utilizzati dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi;
- distruzione, in tutto o in parte, di sistemi informatici o telematici altrui;

- deterioramento, in tutto o in parte, di sistemi informatici o telematici altrui;
- rendere inservibili, in tutto o in parte, sistemi informatici o telematici altrui;
- distruzione, in tutto o in parte, di programmi, informazioni o dati altrui;
- deterioramento, in tutto o in parte, di programmi, informazioni o dati altrui;
- rendere, in tutto o in parte, inservibili programmi, informazioni o dati altrui;
- distruzione di informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico ad essi pertinenti, o comunque di pubblica utilità;
- deterioramento di informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità;
- cancellazione di informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità;
- alterazione di informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità;
- soppressione di informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità;
- ostacolo al funzionamento di sistemi informatici o telematici altrui;
- introduzione di dati, informazioni o programmi atti a distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici altrui;
- trasmissione di dati, informazioni o programmi atti a distruggere, danneggiare, r endere in tutto o in parte inservibili sistemi informatici o telematici altrui.

*****

B. Principi generali di comportamento in ordine ai reati di cui all'art. 24-bis del d. lgs. 231/01

(i) Introduzione

Mizar adotta specifiche procedure e istruzioni, in relazione alle attività informatiche svolte in azienda.

Con apposito Regolamento denominato "Regolamento per l'uso delle risorse informatiche" sono definite chiare regole riguardo all'uso del sistema informativo e delle risorse elettroniche, telematiche e telefoniche, al fine di garantire l'utilizzo appropriato degli stessi, in linea con una politica aziendale trasparente. L'utilizzo dello strumento informatico (in primis il PC) è strettamente collegato all'attività svolta dall'utente in ambito aziendale.

Inoltre, apposite procedure e istruzioni stabiliscono le regole da adottare in materia di amministrazione dell'infrastruttura e delle applicazioni, di backup e di restore, nonché di archiviazione e ripristino dei dati.

(ii) Procedura accessi al sistema informativo e gestione personal computer individuali

La procedura ha lo scopo di regolamentare le autorizzazioni all'accesso al Sistema Informativo Aziendale e la gestione dei personal computer assegnati ai dipendenti e agli esterni, onde proteggere il patrimonio dei dati aziendali

In particolare, la procedura prevede regole per:

- la creazione di nuove utenze di rete
- l'assegnazione delle credenziali per l'accesso ai sistemi informatici
- la creazione delle password e la loro modifica periodica
- l'accesso ai sistemi informatici in caso di indisponibilità dell'utente autorizzato
- l'assegnazione dei profili di accesso degli utenti in relazione alla mansione svolta in azienda
- la protezione degli strumenti informatici
- il backup e il ripristino delle apparecchiature

(iii) Regolamento per l'uso delle risorse informatiche

Il Regolamento adottato per l'utilizzo del sistema informatico e di comunicazione si applica a tutti i dipendenti Mizar senza distinzione di ruolo e/o di livello e a prescindere dal rapporto contrattuale. In tale contesto, si applica, in via esemplificativa a lavoratori somministrati, collaboratori a progetto, in stage e consulenti.

Esso si applica, altresì, all'utilizzo di PC portatili, laddove la responsabilità della custodia e la cura della rimozione di eventuali file elaborati prima della riconsegna spetta all'utente assegnatario.

Le medesime disposizioni si applicano anche nei confronti di incaricati esterni quali agenti e forza vendita.

Il Regolamento in parola disciplina l'utilizzo dei sistemi informativi con riferimento a:

- utilizzo del personal computer da parte dell'utente;
- utilizzo della rete Mizar;
- uso della posta elettronica;
- navigazione in Internet;
- utilizzo dei telefoni, fax e fotocopiatrici.

Allegato 16

Fattispecie dei reati in materia di violazione del diritto di autore

L'elenco dei reati suscettibili di determinare la responsabilità amministrativa di un ente è stato ampliato con la Legge n. 99 del 23 luglio 2009 recante "Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia" che ha introdotto il nuovo articolo 25-nonies del D. Lgs. 231/01.

Art. 25-nonies D. Lgs. nr. 231/01

Delitti in materia di violazione del diritto d'autore.

"In relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a-bis), e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.

Nel caso 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 superiore ad un anno. Resta fermo quanto previsto dall'articolo 174-quinquies della citata legge n. 633 del 1941".

* * *

Art. 171 L. 633/41

Le parti inserite tra parentesi quadre non sono espressamente richiamate dal D.Lgs. 231/01 ma sono state ugualmente inserite per una migliore comprensione delle condotte delittuose.

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

a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nello Stato esemplari prodotti all'estero contrariamente alla legge italiana;]

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

[b) rappresenta, esegue o recita in pubblico o diffonde, con o senza variazioni od aggiunte, un'opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell'opera cinematografica, l'esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico;

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

d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di riprodurre o di rappresentare;

e) (soppresso); f) in violazione dell'art. 79 ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.

Chiunque commette la violazione di cui al primo comma, lettera a-bis), è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato].

La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.]

[La violazione delle disposizioni di cui al terzo ed al quarto comma dell'articolo 68 comporta la sospensione dell'attività di fotocopia, xerocopia o analogo sistema di riproduzione da sei mesi ad un anno nonché la sanzione amministrativa pecuniaria da euro 1.032 a euro 5.164".

La norma punisce chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma, mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa. Se il reato è commesso con riguardo ad un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore, è prevista una sanzione più grave. La Legge del 22 aprile 1941, n 633 considera "opere dell'ingegno protette" anche le opere scientifiche, i programmi per elaboratore, le banche dati e le opere di disegno industriale.]

Art. 171-bis L. 633/41

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

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

Tale reato può configurarsi quando:

- abusivamente si duplichino, per trarne profitto, programmi per elaboratore ovvero si importino, distribuiscano, vendano, detengano a scopo commerciale o imprenditoriale o si concedano in locazione programmi contenuti in supporti non contrassegnati SIAE (shareware, freeware, demo);
- vengano usati mezzi atti a consentire la rimozione o l'elusione di dispositivi applicati a protezione di un programma per elaboratori;
- si riproduca o diffonda su supporti non contrassegnati SIAE, il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64quinquies e 64sexies della legge in parola;
- si estraggano o si reimpieghino parti di banca dati in violazione delle disposizioni di cui agli articoli 102bis e 102ter del medesimo testo normativo;
- si distribuiscano o si vendano parti di una banca di dati.

Art. 171-ter L. 633/41

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;

b) la pubblicazione della sentenza in uno o più quotidiani, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;

c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

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

Il reato in questione può configurarsi laddove a fini di lucro e per uso non personale, abusivamente si duplichino, riproducano, trasmettano o diffondano in pubblico con qualsiasi procedimento, in tutto o in parte, opere o parti di opere dell'ingegno, letterarie, drammatiche, scientifiche, anche se inserite in opere collettive o composite o in banche dati. È punito, altresì, colui che pur non avendo concorso alla duplicazione o riproduzione, introduca nel territorio dello Stato o detenga per la cessione o la commercializzazione,

proiettando o facendo ascoltare in pubblico, con qualsiasi procedimento, duplicazioni o riproduzioni abusive di opere dell'ingegno.

Art. 171-septies L. 633/41

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

a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;

b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge".

Art. 171-octies L. 633/41

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

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

La trattazione degli artt. 171-septies e 171-octies della l. n. 633/41 viene omessa in quanto, allo stato, la Società non svolge attività a rischio di commissione di tali reati.

Allegato 17

Protocollo prevenzione reati in materia di violazione del diritto di autore

A. Le aree di rischio e le funzioni aziendali coinvolte con riferimento ai reati di cui all'art. 25-nonies del D.Lgs. 231/01

A. Quanto all'immissione di opere altrui in reti telematiche (con eventuali e particolari modalità quali deformazione dell'opera o usurpazione della sua paternità), su un piano teorico, ogni attività aziendale che implichi utilizzo di PC potrebbe essere esposta a rischio;

B1. Quanto alla detenzione, diffusione o duplicazione di programma per elaboratore in supporti senza contrassegno SIAE, su un piano teorico, ogni attività aziendale che implichi utilizzo di PC potrebbe essere esposta a rischio;

B2. Quanto alla duplicazione o diffusione di banche dati o parti di esse su un piano teorico, ogni attività aziendale che implichi utilizzo di PC potrebbe essere esposta a rischio;

In relazione alle attività aziendali che comportano l'utilizzo del PC si possono individuare i seguenti comportamenti a rischio reato, connessi all'utilizzo dei sistemi telematici e informatici:

- accesso (logico) alla rete aziendale;
- immissione nei sistemi telematici di dati scientifici, fotografie, brani musicali, disegni ed altre opere di ingegno di terzi estranei alla Società;
- gestione e utilizzo (con modalità di deformazione, modificazione, usurpazione, etc.) nei sistemi telematici di dati scientifici, fotografie, brani musicali, disegni ed altre opere di ingegno di terzi estranei alla Società;
- detenzione, duplicazione, diffusione di programma per elaboratore senza contrassegno SIAE;
- rimozione o elusione di dispositivi applicati a protezione di programma per elaboratore;
- utilizzo dei PC aziendali per accesso a banche dati;
- gestione (con modalità di deformazione, modificazione, usurpazione, estrazione, reimpiego, duplicazione, riproduzione, diffusione, cessione, etc.) di banca dati;
- gestione (con modalità di deformazione, modificazione, usurpazione, estrazione, reimpiego, duplicazione, riproduzione, diffusione, cessione, etc.) di opera dell'ingegno di terzi;
- manutenzione dei PC (interventi periodici e straordinari);
- adattamento/aggiornamento di sistemi informatici aziendali;
- perdita dei dati nelle reti telematiche.

Qui di seguito un elenco (non esaustivo) di ipotesi di condotta che possono integrare uno dei reati presupposto di cui all'art. 25-nonies D. Lgs. 231/2001:

- diffusione in pubblico, attraverso l'immissione in un sistema di reti telematiche, di un'opera altrui;
- usurpazione della paternità dell'opera, ovvero deformazione, mutilazione o altra modificazione di un'opera altrui;
- immissione in rete telematica di un'opera altrui non destinata alla pubblicazione;
- abusiva duplicazione, per trarne profitto, di programmi per elaboratore;
- distribuzione, vendita, detenzione, concessione in locazione a scopo commerciale di programmi per elaboratore;
- rimozione arbitraria o elusione di dispositivi applicati a protezione di un programma per elaboratori;
- riproduzione, distribuzione, comunicazione, presentazione in pubblico, al fine di trarne profitto, su supporti non contrassegnati SIAE, del contenuto di una banca dati;
- estrazione ovvero trasferimento permanente o temporaneo della totalità o di una parte sostanziale del contenuto di una banca dati su un altro supporto con qualsiasi mezzo
- reimpiego ovvero messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto di una banca dati, mediante distribuzione di copie, noleggio, trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma della banca dati medesima;
- duplicazione, riproduzione, diffusione in pubblico di un'opera altrui con qualsiasi procedimento;
- importazione di duplicazioni o riproduzioni di opera altrui.

*****

B. Principi generali di comportamento in ordine ai reati di cui all'art. 25-nonies del d.lgs. 231/01

(i) Introduzione

Qui di seguito i principi e le relative regole di condotta ritenuti rilevanti rispetto alle fattispecie prese in considerazione:

a) vige il principio secondo cui il patrimonio della Società va tutelato anche nel comportamento quotidiano di ciascun dipendente; costituiscono patrimonio della Società anche i beni immateriali, siano essi oggetto di proprietà intellettuale (opere dell'ingegno, relativo diritto d'autore/copyright), siano essi oggetto di proprietà industriale (nomi, marchi, altri segni distintivi, disegni, modelli, brevetti).

b) allorché la titolarità dei suddetti beni non sia della Società ma di terzi, va comunque rispettata e pertanto deve essere prevenuta in ogni momento la violazione dei relativi diritti dei terzi. Ciò vale sia per i beni dei terzi con cui la Società entri in rapporto (c.d. partners industriali o commerciali, quali i fornitori di beni e servizi), sia per i beni di soggetti concorrenti della Società o di terzi in genere;

c) da quanto sopra, si desume che in ordine ai beni di proprietà intellettuale ogni dato e informazione della Società e dei terzi deve, di norma, essere valutato quanto alla rilevanza e importanza per il titolare e

quindi essere classificato anche ai fini della protezione da rischio di dispersione, manipolazione, usurpazione ed altri illeciti comportamenti. Ciò vale per tutte le opere dell'ingegno, compresi i testi scientifici, disegni, opere cinematografiche nonché le "banche dati". Analogamente, in ordine ai beni di proprietà industriale, la Società mira a proteggere sia quelli di cui essa è titolare, sia quelli che costituiscono patrimonio altrui.

(ii) Codice Etico e di Comportamento Mizar

A tutela dei dati e delle informazioni il "Codice Etico e di Comportamento" di Mizar prevede le seguenti regole di condotta e sistemi di controllo:

- Le informazioni non devono essere divulgate senza preventiva autorizzazione;
- Le informazioni devono essere discusse con altri dipendenti solo se questi necessitano di conoscerle;
- È necessario ricordare ai venditori che possono avvalersi di tali informazioni solo al fine di condurre trattative commerciali con Mizar;
- Occorre fare attenzione a non divulgare inavvertitamente informazioni in nessun momento e in nessun contesto, inclusa l'interazione sociale;
- Occorre fare attenzione quando si trattano argomenti inerenti agli affari della Società fuori dall'ufficio. Inoltre, è necessario assicurare ai partners commerciali dell'azienda che saranno protette le loro informazioni riservate dalla divulgazione inappropriata. Nel ricevere e gestire informazioni riservate di un'altra parte, non si deve accettare l'informazione a meno che non sussista un contratto di riservatezza firmato che contempli lo scambio di informazioni e non si devono acquisire informazioni riservate di un'altra parte in modo illegale o improprio.

La struttura Risorse Umane è responsabile della formazione dei dipendenti sin dalla loro assunzione così da creare consapevolezza nei dipendenti in relazione agli obblighi e modalità di gestione di dati e informazioni riservati.

A tale scopo:

- informa i candidati all'assunzione che Mizar è in possesso di informazioni di natura riservata, ha direttive atte a proteggere tali informazioni e che, in qualità di dipendente, l'aspirante è tenuto a mantenere riservate tali informazioni alle procedure aziendali;
- stipula un accordo di riservatezza con i dipendenti che abbiano funzioni di responsabilità, che deve essere accettato e firmato;
- assicura che nel corso dell'orientamento in fase di assunzione, i neo-dipendenti siano avvertiti della necessità di proteggere le informazioni classificate Riservato (Esclusivo);
- mantiene un programma continuo di consapevolezza della sicurezza al fine di proteggere le informazioni di natura Riservato (Esclusivo).

(iii) Regolamento per l'uso delle risorse informatiche

Con apposito Regolamento denominato "Regolamento per l'uso delle risorse informatiche" sono definite chiare regole riguardo l'uso del sistema informatico e delle risorse elettroniche e telematiche, al fine di garantire l'utilizzo appropriato degli stessi, in linea con una politica aziendale trasparente.

Secondo tale Regolamento vale quanto segue:

i) utilizzo del personal computer:

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del servizio IT per conto della Mizar né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo, infatti, il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la Mizar a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore, vengono sanzionate anche penalmente.

ii) gestione delle informazioni Mizar:

in relazione alla protezione delle informazioni riservate lo "Standard di condotta professionale ed etica" dispone che "sono considerate informazioni riservate quelle informazioni relative ai prodotti, affari o attività della Società non disponibili pubblicamente e che possono avere un valore per la Società, i suoi concorrenti o altre entità. La nostra Società genera una grande quantità di informazioni e i dipendenti sono tenuti a sapere quali informazioni sono riservate e non devono essere divulgate al di fuori della Società. La divulgazione di informazioni riservate può distruggere il valore dell'informazione, danneggiare la posizione competitiva della nostra Società, violare la legge o influire sui nostri obblighi contrattuali. Ognuno di noi è responsabile del trattamento, mantenimento e smaltimento delle informazioni riservate in modo conforme alle procedure aziendali."

Per una completa comprensione dei sistemi di controllo e misure preventive adottate dalla Società a presidio di abusi e operazioni indebite, effettuati mediante o nei sistemi telematici ed informatici si rinvia alla parte del Modello riguardante i reati informatici. Riteniamo in questa sede utile richiamare espressamente sistemi e misure riguardanti l'accesso alle banche dati di tipo informatico.

L'accesso alle banche dati personali di tipo informatico è consentito solamente ai soggetti muniti di apposita abilitazione dai personal computer loro in dotazione per lo svolgimento delle mansioni lavorative. La gestione delle abilitazioni ed l'aggiornamento del pc è compito dell'Amministratore di sistema.

Mizar adotta le seguenti misure di sicurezza:

- per accedere alle banche dati personali trattate su supporto informatico è necessario possedere una password di accesso ed un codice d'identificazione (d'ora in poi denominato "User ID").
- l'accesso alle banche dati è consentito solo ai soggetti in possesso degli strumenti di cui sopra.

Allegato 18

Protocollo di prevenzione dei reati ambientali

Mizar adotta una serie di procedure e disposizioni in materia di prevenzione della commissione dei reati ambientali e di gestione delle eventuali anomalie ed emergenze, al fine di ridurre al minimo i rischi connessi allo svolgimento della propria attività, in coerenza con la politica aziendale in materia di ambiente e di rispetto dell'ecosistema.