CRÉDIT AGRICOLE ASSICURAZIONI

# Modello di organizzazione, gestione e controllo *ex* D.Lgs. 231/2001

FEBBRAIO 2026

# Indice


**PARTE GENERALE** ..... **8**
**DEFINIZIONI** ..... 9
**CAPITOLO 1** ..... 12
**IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO A CARICO DELLE PERSONE GIURIDICHE, SOCIETÀ E ASSOCIAZIONI** ..... 12
**1.1 Il Decreto Legislativo n. 231/2001 e la normativa di riferimento** ..... **12**
**1.2 L'adozione del "modello di organizzazione, gestione e controllo" quale possibile esimente dalla responsabilità amministrativa** ..... **14**
**CAPITOLO 2** ..... 16
**ADOZIONE DEL MODELLO DA PARTE DI CAA** ..... 16
**2.1 La Società e l'adozione del Modello** ..... **16**
**2.1.1 Le Linee Guida ANIA** ..... 16
**2.2 Funzione e scopo del Modello** ..... **18**
**2.3 La costruzione del Modello e la sua struttura** ..... **19**
**2.4 Principi ed elementi ispiratori del Modello** ..... **22**
**2.5. Il sistema di organizzazione, gestione e controllo in linea generale** ..... **24**
**2.5.1. Il sistema di organizzazione e gestione** ..... **25**
**2.5.1.1. Gli strumenti organizzativi aziendali** ..... **25**
**2.5.1.2. Il sistema di deleghe e procure** ..... **25**
**2.5.2 Il sistema dei controlli interni** ..... **27**
**2.6 La procedura di adozione del Modello** ..... **34**
**2.7 Destinatari del Modello** ..... **34**
**CAPITOLO 3** ..... 35
**L'ORGANISMO DI VIGILANZA** ..... 35
**3.1 Identificazione dell'organismo di vigilanza** ..... **35**
**3.2 Durata in carica** ..... **38**
**3.3 Funzione e poteri dell'organo di controllo interno** ..... **39**
**3.4 Poteri dell'Organismo di Vigilanza** ..... **42**
**3.5 Regole di convocazione e di funzionamento** ..... **43**
**3.6 Flussi informativi dell'OdV verso il vertice aziendale e il Collegio Sindacale e coordinamento con le funzioni aziendali** ..... **44**
**3.7 Flussi informativi verso l'OdV: informazioni di carattere generale e informazioni specifiche obbligatorie** ..... **46**
**3.7.1. Raccolta e conservazione delle informazioni dell'OdV** ..... **47**
**3.8 Il sistema di *whistleblowing*** ..... **48**
**LA FORMAZIONE DELLE RISORSE E LA DIFFUSIONE DEL MODELLO** 50
**4.1 Premessa** ..... **50**
**4.2 Dipendenti e componenti degli organi sociali** ..... **50**
**4.3 Altri destinatari** ..... **51**
**CAPITOLO 5** ..... 52
**SISTEMA SANZIONATORIO** ..... 52
**5.1 Funzione del sistema sanzionatorio** ..... **52**
**5.2 Dipendenti soggetti al CCNL** ..... **53**
**5.2.1 Sistema sanzionatorio** ..... 53
**5.2.2 Violazioni del Modello e relative sanzioni** ..... 53

**5.3 Misure nei confronti dei dirigenti** ..... **55**
**5.4 Misure nei confronti degli Amministratori** ..... **56**
**5.5 Misure nei confronti dei Sindaci** ..... **56**
**5.6 Misure nei confronti dei membri dell'OdV** ..... **56**
**5.7 Misure nei confronti della Rete Distributiva, dei Consulenti, dei Fornitori e dei *Partner*** ..... **57**
**CAPITOLO 6** ..... 58
**VERIFICHE SULL'ADEGUATEZZA DEL MODELLO** ..... 58
**PARTI SPECIALI** ..... 59
**PARTE SPECIALE – A –** ..... 60
**Reati nei rapporti con la Pubblica Amministrazione e induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** ..... 60
**CAPITOLO A.1** ..... 61
**A.1.1 Enti della Pubblica Amministrazione** ..... **61**
**A.1.2 Pubblici Ufficiali** ..... **62**
**A.1.3 Incaricati di un pubblico servizio** ..... **63**
**CAPITOLO A.2** ..... 65
**Le fattispecie dei reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/2001)** ..... 65
**A.2.1 Reati di tipo corruttivo** ..... **65**
**A.2.2 La concussione, il peculato e l'indebita destinazione di denaro o cose mobili** ..... **70**
**A.2.3 Le ipotesi di truffa** ..... **71**
**A.2.4 Le ipotesi di malversazione e di indebita percezione di erogazioni** ..... **73**
**CAPITOLO A.3** ..... 75
**Attività Sensibili nei rapporti con la P.A.** ..... 75
**Principi generali di comportamento** ..... **79**
**Principi procedurali specifici** ..... 82
**A.5.1 Principi procedurali specifici generalmente applicabili** ..... **82**
**CAPITOLO A.6** ..... 91
**I controlli dell'OdV e flussi informativi** ..... 91
**A.6.1 Il controllo in generale** ..... **91**
**PARTE SPECIALE – B –** ..... 93
**Reati Societari** ..... 93
**CAPITOLO B.1** ..... 94
**Le fattispecie dei reati societari (art. 25-*ter* del D.Lgs. 231/2001)** ..... 94
**B.1.2 La tutela del capitale sociale** ..... **95**
**B.1.3 La tutela del corretto funzionamento della società** ..... **97**
**B.1.4 La tutela penale contro le frodi** ..... **97**
**B.1.5 La tutela delle funzioni di vigilanza** ..... **98**
**CAPITOLO B.2** ..... 99
**Attività Sensibili nell'ambito dei reati societari** ..... 99
**CAPITOLO B.3** ..... 101
**Regole e principi generali** ..... 101
**B.3.1 Principi generali di comportamento** ..... **101**
**Principi procedurali specifici** ..... 105
**I controlli dell'OdV e i flussi informativi** ..... 110
**B. 5.1 Il controllo in generale** ..... **110**
**PARTE SPECIALE – C –** ..... 112

**Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio, reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori e reati di finanziamento del terrorismo, reati con finalità di terrorismo o eversione dell'ordine democratico** ..112
**CAPITOLO C.1** ..113
**C.1.1. Le fattispecie dei reati di Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio (Art. 25-*octies*, D.Lgs. 231/2001)** 113
**C.1.2 Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (Art. 25-*octies*.1, D.Lgs. 231/2001)** ..118
**C.1.3 Delitti con finalità di terrorismo o eversione dell'ordine democratico ("Reati di Terrorismo")** ..119
**C.1.4 La normativa di prevenzione del Reato di Finanziamento del Terrorismo**..122
**CAPITOLO C.2** ..124
**C.2.1 Attività Sensibili nell'ambito dei Reati di Riciclaggio, dei Reati di Terrorismo e dei Reati in materia di strumenti di pagamento diversi dal contante e trasferimento fraudolento di valori** ..124
**C.2.2 Principi generali di comportamento in relazione ai Reati di Riciclaggio, ai Reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori e ai Reati di Terrorismo** ..125
**I controlli dell'OdV in relazione ai Reati di Riciclaggio, ai Reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori e ai Reati di Terrorismo** ..136
PARTE SPECIALE – D – ..137
**Delitti contro la personalità individuale e impiego di cittadini di paesi terzi il cui soggiorno è irregolare** ..137
CAPITOLO D.1 ..138
D.1.1 Le fattispecie dei delitti contro la personalità individuale (art. 25-*quinquies*, D.Lgs. 231/2001) ..138
D.1.2. Le fattispecie di delitto di impiego di cittadini terzi il cui soggiorno è irregolare, procurato ingresso illecito di stranieri nel territorio dello Stato e favoreggiamento dell'immigrazione clandestina (art. 25-*duodecies*, D.Lgs. 231/2001) ..140
Attività Sensibili ..142
D.2.1. Attività Sensibili in relazione ai delitti contro la personalità individuale ..142
D.2.2. Attività Sensibili in relazione alle fattispecie di delitto di impiego di cittadini terzi il cui soggiorno è irregolare, procurato ingresso illecito di stranieri nel territorio dello Stato e favoreggiamento dell'immigrazione clandestina ..142
CAPITOLO D.3 ..144
Principi generali di comportamento ..144
D.3.1 Principi di comportamento ..144
Principi procedurali specifici ..146
D.4.1. Principi procedurali specifici relativi ai reati contro la personalità individuale ..146
D.4.2. Principi di comportamento in relazione al delitto di impiego di cittadini terzi il cui soggiorno è irregolare ..147
CAPITOLO D.5 ..150
I controlli dell'OdV e i flussi informativi ..150
D.5.1 Il controllo in generale ..150
PARTE SPECIALE – E – ..151
Reati e illeciti amministrativi di abuso di mercato ..151
CAPITOLO E.1 ..152

Le fattispecie dei reati e di illeciti amministrativi di abuso di mercato (Art. 25-*sexies*, D.Lgs. 231/2001 e Art. 187-*quinquies* TUF) ..... 152
E.1.1 La definizione di "informazione privilegiata" ..... 152
E.1.2 I reati di abuso di mercato ..... 156
E.1.3 Gli illeciti amministrativi *ex* art. 187-*quinquies* del TUF ..... 157
CAPITOLO E.2 ..... 159
Attività Sensibili nell'ambito dei reati di abuso di mercato ..... 159
CAPITOLO E.3 ..... 160
Regole e principi procedurali specifici ..... 160
E.3.1 Principi di comportamento ..... 160
E.3.2 Regole comportamentali ..... 160
CAPITOLO E.4 ..... 164
I controlli dell'OdV e i flussi informativi ..... 164
E.4.1 Il controllo in generale ..... 164
PARTE SPECIALE – F – ..... 165
Reati di omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro ..... 165
Definizioni ..... 166
**CAPITOLO F.1** ..... 168
**Le fattispecie dei reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (Art. 25-*septies*, D.Lgs. 231/2001)** ..... 168
**Attività Sensibili nell'ambito dei reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro** ..... 170
**CAPITOLO F.3** ..... 171
**Regole e principi procedurali specifici** ..... 171
**F.3.1 Principi di comportamento nell'ambito dei reati in materia di salute e sicurezza nei luoghi di lavoro** ..... 171
F.3.2 La politica per la sicurezza sul lavoro ..... 171
F.3.3 Il processo di pianificazione ..... 173
F.3.2 Compiti e responsabilità ..... 173
**F.3.4.2 Informazione e formazione** ..... 179
F.3.4.3 Comunicazione, flusso informativo e cooperazione ..... 181
F.3.5 Integrazione nei processi aziendali e gestione operativa ..... 185
F.3.6 L'attività di controllo – monitoraggio. ..... 185
F.3.7 Gli interventi successivi alle attività di controllo ..... 186
**CAPITOLO F.4** ..... 188
**I contratti di appalto** ..... 188
**CAPITOLO F.5** ..... 190
**I controlli dell'OdV e i flussi informativi** ..... 190
PARTE SPECIALE – G – ..... 191
Delitti informatici e in materia di violazione del diritto d'autore ..... 191
**CAPITOLO G.1** ..... 192
**G.1.1. Le fattispecie dei delitti informatici e (art. 24-*bis* del Decreto 231) e dei delitti in materia di violazione del diritto d'autore (art. 25-*novies* del Decreto 231)** ..... 192
**G.1.2.Delitti informatici** ..... 192
**G.1.3. Delitti in materia di violazione del diritto d'autore** ..... 200
**CAPITOLO G.2** ..... 203
**G.2.1 Attività Sensibili nell'ambito dei delitti informatici** ..... 203
**G.2.2. Attività Sensibili nell'ambito dei delitti in violazione del diritto d'autore** ..... 203

**CAPITOLO G.3** ..... 204
**Regole e principi generali** ..... 204
**CAPITOLO G.4** ..... 207
**Principi procedurali specifici** ..... 207
G.4.1. Principi procedurali specifici relativi ai Delitti Informatici ..... 207
G.4.2. Principi procedurali specifici relativi ai delitti in materia di violazione del diritto d'autore ..... 214
**CAPITOLO G.5** ..... 216
**I controlli dell'OdV e i flussi informativi** ..... 216
**G.5.1 Il controllo in generale** ..... 216
CAPITOLO H.1 ..... 219
Le fattispecie dei delitti di criminalità organizzata (art. 24-*ter* Decreto 231) ..... 219
CAPITOLO H.2 ..... 222
Attività Sensibili ..... 222
CAPITOLO H.3 ..... 223
Regole e principi generali ..... 223
H.3.1 Il sistema in linea generale ..... 223
H.3.2 Principi generali di comportamento ..... 223
CAPITOLO H.4 ..... 225
Principi procedurali specifici ..... 225
H.4.1 Principi procedurali specifici generalmente applicabili ..... 225
CAPITOLO H.5 ..... 228
I controlli dell'OdV e i flussi informativi ..... 228
H.5.1 Il controllo in generale ..... 228
PARTE SPECIALE – I – ..... 230
Delitti contro l'industria e il commercio e delitti di contraffazione ..... 230
CAPITOLO I.1 ..... 231
CAPITOLO I.2 ..... 235
Attività Sensibili nell'ambito dei delitti contro l'industria e il commercio e dei reati di contraffazione ..... 235
CAPITOLO I.3 ..... 236
Regole e principi generali ..... 236
CAPITOLO I.4 ..... 238
Principi procedurali specifici ..... 238
CAPITOLO I.5 ..... 241
I controlli dell'OdV e i flussi informativi ..... 241
PARTE SPECIALE – L – ..... 242
Fattispecie di corruzione tra privati ..... 242
CAPITOLO L.1 ..... 243
Le fattispecie di reato di corruzione tra privati (Art. 25-*ter*, comma 1, lettera s-*bis*, del D.Lgs. 231/2001) ..... 243
CAPITOLO L.2 ..... 247
Attività Sensibili e Attività Strumentali ..... 247
CAPITOLO L.3 ..... 251
Regole e principi generali ..... 251
L.3.1 Il sistema in linea generale ..... 251
L.3.2 Principi generali di comportamento ..... 251
CAPITOLO L.4 ..... 254
Principi procedurali specifici ..... 254
L.4.1 Principi procedurali specifici generalmente applicabili ..... 254
CAPITOLO L.5 ..... 265

I controlli dell'OdV e i flussi informativi ....265
L.5.1 Il controllo in generale ....265
**CAPITOLO M.1** ....268
**Le fattispecie dei reati tributari** ....268
**CAPITOLO M.2** ....271
**Attività Sensibili nell'ambito dei Reati tributari** ....271
**CAPITOLO M.3** ....272
**Regole e princìpi generali** ....272
**CAPITOLO M.4** ....273
**Principi procedurali specifici** ....273
CAPITOLO M.5 ....276
I controlli dell'OdV e i flussi informativi ....276
PARTE SPECIALE – N – ....278
Reati Ambientali ....278
**CAPITOLO N.1** ....279
**Le fattispecie dei reati ambientali previste dall'art. 25-*undecies* del Decreto 231** ....279
**CAPITOLO N.2** ....282
**Attività Sensibili nell'ambito dei Reati Ambientali** ....282
**CAPITOLO N.3** ....283
**Principi generali di comportamento nell'ambito dei Reati Ambientali** ....283
**CAPITOLO N.4** ....285
**Principi procedurali specifici nell'Ambito dei Reati Ambientali** ....285
**CAPITOLO N.5** ....287
**I controlli dell'OdV e i flussi informativi** ....287

# PARTE GENERALE

**DEFINIZIONI**

- "Attività Sensibili": le attività di Credit Agricole Assicurazioni S.p.A. nel cui ambito sussiste il rischio di commissione dei Reati.

- "CCNL": il Contratto Collettivo Nazionale di Lavoro (contratto delle imprese di assicurazione) attualmente in vigore e applicato da CAA.

- "Codice di Condotta": il codice di comportamento del gruppo che fa capo a Crédit Agricole S.A. che mette in pratica gli impegni indicati nella Carta Etica.

- "Carta Etica": la carta etica del gruppo che fa capo a Crédit Agricole S.A. che indica gli impegni, l'identità e i valori nonché i principi che guidano l'attività delle società del gruppo.

- "Codice Etico": il codice etico del sotto-gruppo assicurativo nazionale "Gruppo Crédit Agricole Assurances Italia" (formato da Crédit Agricole Vita S.p.A., Crédit Agricole Assicurazioni S.p.A. e Stelvio Agenzia Assicurativa S.p.A.) adottato dalla Società.

- "CAA", la "Compagnia" o la "Società": Crédit Agricole Assicurazioni S.p.A. con sede in Corso di Porta Vigentina, 9, 20122, Milano.

- "Responsabile *Area Compliance*": soggetto incaricato di valutare, coerentemente con quanto disposto dalla normativa regolamentare (Regolamento IVASS n. 38 del 3 luglio 2018 recante "*Disposizioni in materia di sistema di controllo societario*"), che l'organizzazione e le procedure interne della Società siano idonee a prevenire il rischio non conformità alle norme.

- "Consulenti": coloro che agiscono in nome e/o per conto di CAA sulla base di un mandato ovvero coloro che collaborano con la Società in forza di un contratto di collaborazione di qualsiasi natura.

- "Crédit Agricole Vita o CA Vita": Crédit Agricole Vita S.p.A., società del Gruppo Crédit Agricole che svolge attività in ambito di servizi amministrativo-contabili, *corporate governance*, legale e reclami, risorse umane, *marketing* e commerciale, finanza, *facility management*, organizzazione e IT, *risk management*, *internal audit* e *compliance* in favore di CAA.

- "Destinatari": i Dipendenti, i Dipendenti di per i servizi prestati a CAA in virtù dei contratti di servizio, i Consulenti, i Fornitori, la Rete Distributiva, i *Partner,* eventuali intermediari e gli Organi Sociali della Società.
- "Decreto *Whistleblowing*": il D.Lgs. 10 marzo 2023, n. 24 di attuazione della Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, "*riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione europea e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*".
- "Dipendenti": tutti i dipendenti di CAA (compresi i dirigenti).
- "D.Lgs. 231/2001" o "Decreto" o "Decreto 231": il Decreto Legislativo 8 giugno 2001, n. 231 e successive modifiche e integrazioni.
- "Esponenti Aziendali": gli Organi Sociali e i Dipendenti della Società.
- "Fornitori": tutti i fornitori di beni e servizi della Società, compresi appaltatori e subappaltatori.
- "Gruppo Crédit Agricole", o "Gruppo": gruppo di società facente capo, a livello italiano, a Crédit Agricole Italia S.p.A.
- "Linee Guida ANIA": le Linee Guida ANIA per la costruzione dei modelli di organizzazione, gestione e controllo *ex* D. Lgs. 231/2001.
- "Modello": il modello di organizzazione, gestione e controllo previsto dal D.Lgs. 231/2001.
- "Operazione Sensibile": operazione o atto che si colloca nell'ambito delle Attività Sensibili.
- "Organi Sociali": i membri del Consiglio di Amministrazione e del Collegio Sindacale di CAA.
- "Organismo di Vigilanza" o "OdV": organismo interno preposto alla vigilanza sul funzionamento e sull'osservanza del Modello (come qui di seguito definito) e al relativo aggiornamento.
- "P.A.": la Pubblica Amministrazione, inclusi i relativi funzionari e i soggetti incaricati di pubblico servizio:

- "*Partner*": le controparti contrattuali di CAA, tra i quali distributori della Rete Distributiva, ecc.; si tratta sia di persone fisiche sia di persone giuridiche, con cui la società addivenga ad una qualunque forma di collaborazione contrattualmente regolata (associazione temporanea d'impresa - ATI, *joint venture*, consorzi, ecc.), ove destinati a cooperare con la società nell'ambito dei Attività Sensibili.
- "Reati": i reati ai quali si applica la disciplina prevista dal D. Lgs. 231/2001.
- "Rete Distributiva": i soggetti con i quali CAA ha stipulato specifici mandati/accordi per la distribuzione dei propri prodotti.

# CAPITOLO 1

# IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO A CARICO DELLE PERSONE GIURIDICHE, SOCIETÀ E ASSOCIAZIONI

## 1.1 Il Decreto Legislativo n. 231/2001 e la normativa di riferimento

In data 4 luglio 2001, in attuazione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300, è entrato in vigore il Decreto Legislativo 8 giugno 2001, n. 231, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*".

Scopo del Decreto era adeguare l'ordinamento giuridico interno ad alcune convenzioni internazionali, cui l'Italia aveva aderito, quali la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione in cui sono coinvolti funzionari della Comunità Europea e degli Stati Membri e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

Esaminando nel dettaglio il contenuto del D.Lgs. 231/2001, l'articolo 5, comma 1, sancisce la responsabilità della società qualora determinati reati (reati cd. presupposto) siano stati commessi nel suo interesse o a suo vantaggio:

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo della stessa (ad esempio, amministratori e direttori generali);

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti indicati alla lettera precedente (ad esempio, dipendenti non dirigenti).

Pertanto, nel caso in cui venga commesso uno dei Reati, alla responsabilità penale della persona fisica che ha materialmente realizzato il fatto si aggiunge – se e in quanto siano integrati tutti gli altri presupposti normativi – anche la responsabilità "amministrativa" della società.

Sotto il profilo sanzionatorio, per tutti gli illeciti commessi è sempre prevista a carico della persona giuridica l'applicazione di una sanzione pecuniaria; per le ipotesi di maggiore gravità è prevista anche l'applicazione di sanzioni interdittive, quali l'interdizione dall'esercizio dell'attività, la sospensione o la revoca di autorizzazioni, licenze o concessioni, il divieto di

contrarre con la P.A., l'esclusione da finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, il divieto di pubblicizzare beni e servizi.

La responsabilità prevista dal suddetto Decreto si configura anche in relazione ai reati commessi all'estero, purché per gli stessi non proceda lo Stato del luogo in cui è stato commesso il reato medesimo.

Ad oggi, le categorie di Reati risultano essere le seguenti:

(i) i reati commessi nei rapporti con la Pubblica Amministrazione (art. 24 e art. 25);

(ii) i reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis*);

(iii) i reati societari (art. 25-*ter*);

(iv) i reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-*quater*);

(v) le pratiche di mutilazione degli organi genitali femminili (art. 25-*quater*.1);

(vi) i reati contro la personalità individuale (art. 25-*quinquies*);

(vii) i reati e gli illeciti amministrativi di abuso di mercato (art. 25-*sexies*);

(viii) i reati transnazionali (Legge 16 marzo 2006, n. 146);

(ix) i reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-*septies*);

(x) i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-*octies*);

(xi) i delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-*octies*.1);

(xii) i reati in materia di violazione di misure restrittive dell'Unione europea (art. 25-*octies*.2);

(xiii) i delitti informatici (art. 24-*bis*);

(xiv) i delitti contro l'industria e il commercio (art. 25-*bis*.1);

(xv) i delitti in materia di violazione del diritto d'autore (art. 25-*novies*);

(xvi) i reati di criminalità organizzata (art. 24-*ter*);

(xvii) il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-*decies*);

(xviii) i reati ambientali (art. 25-*undecies*);

(xix) l'impiego di cittadini di paesi terzi il cui permesso di soggiorno è irregolare, procurato ingresso illecito di stranieri nel territorio dello Stato e favoreggiamento dell'immigrazione clandestina (art. 25-*duodecies*);

(xx) i reati di razzismo e xenofobia (art. 25-*terdecies*);

(xxi) i reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-*quaterdecies*);

(xxii) i reati tributari (art. 25-*quinquiesdecies*);

(xxiii) i reati di contrabbando (art. 25-*sexiesdecies*);

(xxiv) reati contro il patrimonio culturale (art. 25-*septiesdecies*);

(xxv) riciclaggio di beni culturali e devastazione e saccheggio di beni culturali paesaggistici (art. 25-*duodevicies*);

(xxvi) delitti contro gli animali (art. 25-*undevicies*).

Altre fattispecie di reato potranno in futuro essere inserite dal legislatore nella disciplina dettata dal D.Lgs. 231/2001.

Anticipando quanto si dirà oltre, si specifica che nel presente documento sono stati considerati rilevanti solo gli illeciti (che sono richiamati nell'ambito delle singole Parti Speciali) risultati tali in considerazione dell'analisi del contesto aziendale, dell'attività svolta dalla Società e delle aree potenzialmente soggette al rischio-reato.

### 1.2 L'adozione del "modello di organizzazione, gestione e controllo" quale possibile esimente dalla responsabilità amministrativa

L'articolo 6 del Decreto introduce una particolare forma di esonero dalla responsabilità in oggetto qualora la società dimostri:

a) di aver adottato ed efficacemente attuato attraverso il suo organo dirigente, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi;

b) di aver affidato ad un organismo interno, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curare il loro aggiornamento;

c) che le persone che hanno commesso il reato hanno agito eludendo fraudolentemente il suddetto Modello;

d) che non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lett. b).

Il Decreto prevede, inoltre, che – in relazione all'estensione dei poteri delegati e al rischio di commissione dei Reati – il Modello debba rispondere alle seguenti esigenze:

1. individuare le attività sensibili al rischio di commissione dei reati previsti dal Decreto;
2. predisporre specifici protocolli al fine di programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
3. prevedere modalità di individuazione e di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
4. prescrivere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
5. configurare un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Lo stesso Decreto dispone che il Modello può essere adottato, garantendo le esigenze di cui sopra, sulla base di codici di comportamento (*i.e.* "**Linee Guida**") redatti da associazioni rappresentative di categoria.

# CAPITOLO 2

# ADOZIONE DEL MODELLO DA PARTE DI CAA

## 2.1 La Società e l'adozione del Modello

Il presente Modello è stato adottato, nella sua prima versione, dal Consiglio di Amministrazione di CAA con delibera del 12 marzo 2009 ed è poi stato periodicamente aggiornato nel tempo. Con la medesima delibera è stato istituito l'Organismo di Vigilanza cui è attribuito il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento.

CAA è una compagnia di bancassicurazione che ha per oggetto l'esercizio dell'attività assicurativa, in particolare, la collocazione di prodotti assicurativi, quali ad esempio l'auto, l'abitazione, gli infortuni, attraverso il Gruppo e le relative reti bancarie, con l'obiettivo di ampliare la tradizionale offerta bancaria.

### 2.1.1 Le Linee Guida ANIA

Nella predisposizione del presente Modello CAA si è ispirata alle Linee Guida ANIA per il settore assicurativo quale utile strumento di orientamento per l'interpretazione e l'analisi delle implicazioni giuridiche ed organizzative derivanti dall'introduzione del D.Lgs. 231/2001.

I punti fondamentali individuati dalle Linee Guida ANIA per la costruzione dei Modelli possono essere così sintetizzati:

- individuazione delle **aree di rischio**, volta a verificare in quale area/settore aziendale sia possibile la realizzazione dei Reati;
- previsione di obblighi di **informazione** dell'organismo di vigilanza, volti a soddisfare l'attività di controllo sul funzionamento, l'efficacia e l'osservanza del Modello;
- predisposizione di un **sistema di controllo** ragionevolmente in grado di prevenire o ridurre il rischio di commissione dei Reati attraverso l'adozione di appositi protocolli/procedure. A tal fine soccorre l'insieme ben coordinato di strutture organizzative, attività e regole attuate – su impulso dell'organo decisionale – dal management e dal personale aziendale, volto a fornire una ragionevole sicurezza in merito al raggiungimento delle finalità rientranti nelle seguenti categorie:
  - efficacia ed efficienza delle operazioni gestionali;
  - adeguato controllo dei rischi;

- attendibilità delle informazioni aziendali, sia verso terzi sia all'interno;
- salvaguardia del patrimonio;
- conformità alle leggi, regolamenti, norme e politiche interne.

In particolare, le componenti più rilevanti del sistema di controllo possono essere individuate nei seguenti elementi:

- codice etico e codici di comportamento,
- sistema organizzativo, procedure manuali e informatiche;
- poteri autorizzativi e di firma;
- sistemi di controllo e gestione;
- comunicazione al personale;
- formazione del personale;
- meccanismi disciplinari.

Le componenti del sistema di controllo devono essere informate ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo);
- applicazione di regole e criteri improntate a principi di trasparenza;
- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio per la violazione delle regole e delle procedure previste dal Modello;
- individuazione dei requisiti dell'organismo di vigilanza, riassumibili come segue (e come sarà meglio specificato al Capitolo 3 della presente Parte Generale del Modello):
  - autonomia e indipendenza;
  - professionalità;
  - continuità di azione;

- assenza di cause di incompatibilità, di conflitti di interesse o rapporti di parentela con gli organi di vertice.

Va comunque considerato che, essendo il settore assicurativo soggetto a specifica e capillare vigilanza, l'attenta applicazione della normativa di settore costituisce già un primo strumento di salvaguardia della Società.

Inoltre, nell'ambito dei gruppi assicurativi, rimangono fermi i principi dell'autonomia e delle responsabilità proprie di qualunque società. Conseguentemente ciascuna di esse sarà tenuta ad adottare un proprio Modello e ad individuare un proprio Organismo di Vigilanza. È possibile tuttavia che, all'interno del gruppo, vengano adottate forme di comportamento sostanzialmente univoche, pur nel rispetto delle peculiarità connesse ai diversi settori merceologici di appartenenza dei singoli enti.

### 2.2 Funzione e scopo del Modello

CAA è sensibile alle aspettative dei propri azionisti e degli *stakeholders* ed è altresì consapevole del valore che agli stessi può derivare da un sistema di controllo interno idoneo a prevenire la commissione di reati da parte dei propri Dipendenti, Organi Sociali, Rete Distributiva, Consulenti e *Partner*.

L'adozione e l'efficace attuazione del Modello migliorano il sistema di *Corporate Governance* della Società in quanto limitano il rischio di commissione dei reati e consentono di beneficiare dell'esimente prevista dal D.Lgs. 231/2001, pertanto, scopo del presente Modello è la predisposizione di un sistema strutturato ed organico di prevenzione, dissuasione e controllo finalizzato alla riduzione del rischio di commissione dei Reati mediante l'individuazione di attività sensibili e dei principi di comportamento che devono essere rispettati dai Destinatari. A tal fine viene individuata e descritta la costante attività dell'Organismo di Vigilanza finalizzata a garantire il rispetto del sistema organizzativo adottato e la vigilanza sull'operato dei Destinatari, anche attraverso il ricorso ad idonei strumenti sanzionatori, sia disciplinari che contrattuali.

I principi contenuti nel presente Modello sono volti, da un lato, a determinare una piena consapevolezza del potenziale autore del Reato di commettere un illecito (la cui commissione è fortemente condannata da CAA perché contraria alle norme di deontologia cui essa di ispira e ai suoi interessi, anche quando apparentemente la Società potrebbe trarne

un vantaggio), dall'altro, grazie ad un monitoraggio costante dell'attività, a consentire a CAA di reagire tempestivamente nel prevenire o impedire la commissione del Reato stesso.

Tra le finalità del Modello vi è, quindi, quella di sviluppare nei Dipendenti, negli Organi Sociali, nella Rete Distributiva, nei Consulenti, nei Fornitori e nei *Partner* che operano nell'ambito delle Attività Sensibili e, pertanto, dei Destinatari in generale, la consapevolezza di poter determinare – in caso di comportamenti non conformi alle prescrizioni del Modello e alle altre norme e procedure aziendali (oltre che alla legge) – illeciti passibili di conseguenze penalmente rilevanti non solo per se stessi, ma anche per la Società.

A tal riguardo, le procedure aziendali già adottate e quelle di futura emanazione, così come i principi procedurali indicati nel presente Modello (come meglio indicato di seguito), si caratterizzano per:

- separazione all'interno di ciascun processo tra il soggetto che lo inizia, e/o lo esegue e il soggetto che lo controlla;
- traccia scritta di ciascun passaggio rilevante del processo;
- adeguato livello di formalizzazione.

**2.3 La costruzione del Modello e la sua struttura**

La predisposizione del presente Modello è stata preceduta da una serie di attività preparatorie, suddivise in differenti fasi, tutte finalizzate alla costruzione di un sistema di prevenzione e gestione dei rischi in linea e ispirato, oltre che alle norme contenute nel D.Lgs. 231/2001, anche ai contenuti e suggerimenti dettati dalle Linee Guida ANIA e dalle Linee Guida emanate da Confindustria (aggiornate, da ultimo, nel 2021) nonché alla *best practice* italiana esistente.

Si riporta qui di seguito una breve descrizione delle fasi in cui si è articolato il lavoro di individuazione delle attività potenzialmente a rischio di commissione di Reati, a seguito delle quali si è poi giunti alla predisposizione (e aggiornamento) del presente Modello:

*1. Identificazione delle Attività Sensibili ("*as-is analysis*")*

Tale fase di identificazione delle Attività Sensibili è stata attuata attraverso due distinte attività:

a) esame preliminare della documentazione aziendale, tra cui a titolo esemplificativo: organigramma societario, statuto sociale, verbali di consiglio del amministrazione (in particolare, relativi al conferimento di deleghe e procure), procedure aziendali su tematiche sensibili in relazione ai reati previsti dal Decreto, quali – a titolo esemplificativo – redazione del bilancio, gestione dei rapporti commerciali, rapporti con i Fornitori, documentazione in tema di sicurezza sul lavoro (ad esempio, nomina del RSPP, DVR, procedure di sicurezza, verbali di riunione periodica sulla sicurezza), Codice Etico, Carta Etica, Codice di Condotta, ecc.;

b) interviste ai soggetti chiave della struttura aziendale mirate all'approfondimento dei processi sensibili e dei presidi di controllo esistenti in riferimento agli stessi (procedure esistenti, verificabilità, documentabilità, congruenza e coerenza delle operazioni, separazione delle responsabilità, documentabilità dei controlli, ecc.) tra cui, a titolo esemplificativo: Presidente, Amministratore Delegato, Direttori delle principali funzioni aziendali (e, in particolare, i responsabili delle funzioni di controllo, affari legali, funzioni coinvolte nella redazione di scritture contabili, ecc.).

È stata, inoltre, portata a termine una ricognizione sulla passata attività della Società allo scopo di verificare l'esistenza di eventuali situazioni a rischio e le relative cause. Sono state altresì esaminate le procedure aziendali già adottate e attuate dalla Società.

*2. Effettuazione della "*Gap Analysis*"*

Sulla base della situazione aziendale esistente nella Società a seguito della "as-is analysis" (Attività Sensibili individuate e descrizione delle criticità in esse riscontrate) e alla luce delle previsioni e finalità del D.Lgs. 231/2001, sono state individuate le azioni di miglioramento da attuare nell'ambito delle Attività Sensibili a livello di approntamento sia di procedure interne sia di requisiti organizzativi.

I risultati dell'analisi svolta sia nella fase di "Identificazione delle Attività Sensibili" che in quella di "Effettuazione della *Gap Analysis*" sono stati riassunti in un documento all'uopo predisposto.

*3. Predisposizione del Modello*

Il presente Modello è costituito dai seguenti documenti:

i. una "Parte Generale", contenente l'insieme delle regole e dei principi generali dettati dal Modello;

ii. n. 12 "Parti Speciali" predisposte per alcune categorie di reato contemplate nel D.Lgs. 231/2001, ritenute astrattamente rilevanti in relazione all'attività svolta dalla Società, ossia:

- "Parte Speciale A", denominata "*Reati commessi nei rapporti con la Pubblica Amministrazione e induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*", la quale riguarda le tipologie specifiche di Reati previste ai sensi degli artt. 24, 25 e 25-*decies* del D.Lgs. 231/2001.

- "Parte Speciale B", denominata "*Reati Societari*", la quale è dedicata alle tipologie specifiche di Reati previste ai sensi dell'art. 25-*ter* del D.Lgs. 231/2001.

- "Parte Speciale C", denominata "*Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio, reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori, reati di finanziamento del terrorismo e reati con finalità di terrorismo e di eversione dell'ordine democratico*" la quale è dedicata alle tipologie specifiche di Reati previste ai sensi degli artt. 25-*quater,* 25-*octies,* 25-*octies.*1 del D.Lgs. 231/2001.

- "Parte Speciale D", denominata "*Delitti contro la personalità individuale e impiego di cittadini di paesi terzi il cui permesso di soggiorno è irregolare*", la quale è dedicata alle tipologie specifiche di Reati previste ai sensi degli artt. 25-*quinquies* e art. 25-*duodecies* del D.Lgs. 231/2001.

- "Parte Speciale E", denominata "*Reati e illeciti amministrativi di abuso di mercato*", la quale è dedicata alle tipologie specifiche di Reati previste ai sensi dell'art. 25-*sexies* del D.Lgs. 231/2001.

- "Parte Speciale F", denominata "*Reati di Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro*", la quale è dedicata alle tipologie specifiche di Reati previste ai sensi degli artt. 25-*septies* del D.Lgs. 231/2001.

- "Parte Speciale G", denominata "*Delitti informatici e in materia di violazione del diritto d'autore*", la quale è dedicata alle tipologie specifiche di Reati previste ai sensi dell'art. 24-*bis* del D.Lgs. 231/2001.

- "Parte Speciale H", denominata "*Delitti di criminalità organizzata*" la quale è dedicata alle tipologie di reato previste dall'art. 24-*ter* del D.Lgs. 231/2001.

- "Parte Speciale I", denominata "*Delitti contro l'industria e il commercio e reati di contraffazione*" la quale è dedicata alle tipologie di reato previste dall'art. 25-*bis*1 del D.Lgs. 231/2001.

- "Parte Speciale L" denominata " *Fattispecie di corruzione tra privati*" la quale è dedicata alle fattispecie di reato previste dall'art. 25-*ter*, comma 1, lettera s-*bis* del D.Lgs. 231/2001.

- "Parte Speciale M" denominata "*Reati tributari*" la quale è dedicata alle fattispecie di reato previste dall'art. 25-*quinquiesdecies* del D.Lgs. 231/2001.

- "Parte Speciale N" denominata "*Reati Ambientali*" la quale è dedicata alle fattispecie di reato previste dall'art. 25-*undecies* del D.Lgs, 231/2001.

Ciascuna Parte Speciale è strutturata come segue:

1. descrizione delle fattispecie di reato;
2. descrizione delle Attività Sensibili;
3. principi Generali di Comportamento;
4. principi Procedurali Specifici;
5. controlli dell'Organismo di Vigilanza e flussi informativi.

### 2.4 Principi ed elementi ispiratori del Modello

Nella predisposizione del presente Modello si è tenuto conto delle procedure e dei sistemi di controllo (rilevati in fase di "*as-is*") esistenti in azienda, ove giudicati idonei a valere anche come misure di prevenzione dei Reati e controllo sulle Attività Sensibili.

Il presente Modello, fermo restando la sua finalità peculiare descritta al precedente paragrafo e relativa al D.Lgs. 231/2001, si inserisce nel più ampio contesto del sistema di controllo in essere in azienda e nel Gruppo.

In particolare, quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni della Società anche in relazione ai Reati da prevenire, CAA ha individuato i seguenti:

1. i principi di *corporate governance* generalmente seguiti dalla Società;
2. il Codice Etico, la Carta Etica e il Codice di Condotta adottati dalla Società;
3. la documentazione e le disposizioni inerenti alla struttura gerarchico-funzionale aziendale e organizzativa della Società;
4. la normativa aziendale che la Società ha predisposto nell'ambito delle Attività Sensibili (ad esempio, procedure per la gestione dei rapporti con la P.A., procedure per la redazione delle scritture contabili, documentazione aziendale in materia di sicurezza sul lavoro, ecc.);
5. la formazione del personale e della Rete Distributiva;
6. il sistema sanzionatorio;
7. il sistema *whistleblowing*;
8. i contratti di servizio.

Le regole, procedure e principi di cui agli strumenti sopra elencati non vengono riportati dettagliatamente nel presente Modello, ma fanno parte del più ampio sistema di organizzazione e controllo che lo stesso intende integrare.

Principi cardine cui il Modello si ispira, oltre a quanto sopra indicato, sono:

1. le Linee Guida ANIA, le Linee Guida emanate da Confindustria e la *best practice* italiana esistente in materia, in base alle quali è stata predisposta la mappatura delle **Attività Sensibili** di CAA;
2. i requisiti indicati dal D.Lgs. 231/2001 e in particolare:
    - l'attribuzione all'**Organismo di Vigilanza** del compito di attuare in modo efficace e corretto il Modello anche attraverso il monitoraggio dei comportamenti aziendali e il diritto ad una informazione costante sulle attività rilevanti ai fini del D.Lgs. 231/2001;

- la messa a disposizione dell'organismo di vigilanza di **risorse aziendali** di numero e valore ragionevole e proporzionato ai compiti affidati allo stesso e ai risultati attesi e ragionevolmente ottenibili;
- l'attività di **verifica del funzionamento** del Modello con conseguente aggiornamento periodico (controllo *ex post*);
- l'attività di **sensibilizzazione e diffusione** a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;

3. i principi generali di un adeguato sistema di controllo interno e in particolare:
   - la **verificabilità e documentabilità** di ogni operazione rilevante ai fini del D.Lgs. 231/2001 per consentire l'individuazione di precisi "punti" di responsabilità e della "motivazione" delle scelte stesse (la cosiddetta "*tracciabilità delle scelte*");
   - il rispetto del principio della **separazione delle funzioni e segregazione dei ruoli** (la cosiddetta "*segregation of duties*");
   - la previsione che, nell'assumere decisioni, si prescinda da valutazioni meramente soggettive, facendosi invece riferimento, laddove possibile, a **criteri precostituiti** (la cosiddetta "*oggettivazione dei processi decisionali*");
   - la definizione di **poteri autorizzativi** coerenti con le responsabilità assegnate;
   - la previsione di appositi **flussi informativi** nei confronti dell'Organismo di Vigilanza e da parte di questo nei confronti degli Organi Sociali;
4. il sistema dei controlli interni che monitora le aree in cui vi è un'alta probabilità di commissione dei Reati.

### 2.5. Il sistema di organizzazione, gestione e controllo in linea generale

Obiettivo del presente Modello e, in particolare, delle singole Parti Speciali che lo compongono è che, da un lato, i Dipendenti, gli Organi Sociali e i soggetti che operano a livello periferico per la Società (i.e. *outsourcer* di servizi), dall'altro, i Consulenti e i *Partner* Commerciali, nei limiti delle rispettive pattuizioni contrattuali adottino regole di condotta conformi a quanto prescritto dalle medesime Parti Speciali al fine di prevenire il verificarsi dei Reati ivi considerati.

Tutte le Attività Sensibili tracciate in ciascuna Parte Speciale devono essere svolte conformandosi alle leggi vigenti, alle eventuali procedure in vigore nonché alle regole e ai principi comportamentali contenuti nel presente Modello.

### 2.5.1. Il sistema di organizzazione e gestione

In linea generale, il **sistema di organizzazione** della Società rispetta i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli in particolare, per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

#### 2.5.1.1. Gli strumenti organizzativi aziendali

La Società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati a principi generali di:

a) conoscibilità all'interno della Società;

b) chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri;

c) chiara descrizione delle linee di riporto.

Le procedure interne della Società devono essere formalizzate in modo tale che siano rispettate le seguenti regole di carattere generale:

a) separazione, all'interno di ciascun processo, tra il soggetto che lo inizia (impulso decisionale), il soggetto che lo esegue e lo conclude, e il soggetto che lo controlla;

b) traccia scritta di ciascun passaggio rilevante del processo;

c) adeguato livello di formalizzazione;

d) evitare che i sistemi premianti dei soggetti con poteri di spesa o facoltà decisionali a rilevanza esterna siano basati su target di performance sostanzialmente irraggiungibili.

#### 2.5.1.2. Il sistema di deleghe e procure

In linea di principio, il sistema di deleghe e procure deve essere caratterizzato da elementi di "sicurezza" ai fini della prevenzione dei Reati e, al contempo, consentire la gestione efficiente dell'attività aziendale.

Si intende per "**delega**" quell'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative.

Si intende per "**procura**" il negozio giuridico unilaterale con cui la Società attribuisce dei poteri di rappresentanza nei confronti dei terzi.

Ai titolari di una funzione aziendale che necessitano, per lo svolgimento dei loro incarichi, di poteri di rappresentanza viene conferita una "procura" di estensione adeguata e coerente con le funzioni e i poteri di gestione attribuiti al titolare attraverso la "delega".

La Società definisce un sistema di poteri di spesa e di rappresentanza nei rapporti con i soggetti terzi che risponda ai seguenti requisiti:

a. i poteri di rappresentanza e di spesa sono attribuiti con apposita procura scritta a soggetti che ricoprono adeguati ruoli e responsabilità nell'organigramma aziendale e che siano in possesso di adeguati requisiti di onorabilità e professionalità;

b. i poteri di spesa e di rappresentanza conferiti ai Dirigenti e ai Dipendenti sono limitati da sistemi di firme singole e congiunte a seconda della tipologia e dell'importo dell'operazione;

c. le procure devono essere tempestivamente aggiornate in caso di assunzione di nuove responsabilità, trasferimento a diverse mansioni incompatibili con quelle per cui erano state conferite, dimissioni, licenziamento, ecc.

Sono inoltre posti in essere controlli volti ad accertare il corretto esercizio dei poteri di spesa e di rappresentanza, entro i limiti e secondo le modalità prestabilite dalle relative procure.

***a) Requisiti essenziali del sistema di deleghe***

I requisiti essenziali del sistema di **deleghe**, ai fini di un'efficace prevenzione dei Reati sono i seguenti:

a) tutti coloro (Dipendenti e Organi Sociali) che intrattengono per conto della Società rapporti con la P.A. devono essere dotati di delega formale in tal senso (la Rete Distributiva, i Consulenti e i *Partner* devono essere in tal senso incaricati nello specifico mandato-accordo distributivo, contratto di consulenza o *partnership*);

b) le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;

c) ciascuna delega deve definire in modo specifico e inequivoco:

- i poteri del delegato;
- il soggetto (organo o individuo) cui il delegato riporta gerarchicamente o *ex lege* o statutariamente;

d) i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;

e) il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli.

Il sistema di deleghe esistente nella Società è declinato nell'organigramma e funzionigramma aziendale, il quale si ispira ai principi e alle regole sopra indicate.

In caso di assunzione di nuove responsabilità, trasferimento a diverse mansioni incompatibili con quelle per cui la delega è stata conferita ovvero dimissioni, licenziamento o altra causa, tale organigramma e funzionigramma deve essere tempestivamente aggiornato dalle deputate all'aggiornamento dell'organigramma e funzionigramma aziendale, su segnalazione del dirigente responsabile del soggetto interessato e la procura notarile viene revocata in occasione della prima riunione utile del Consiglio di Amministrazione.

Il documento aggiornato sarà successivamente pubblicato sull'intranet aziendale. Su specifica richiesta, l'organigramma aggiornato deve essere trasmesso anche all'Organismo di Vigilanza.

***b) Requisiti essenziali del sistema di procure***

Oltre a quanto anticipato, i requisiti essenziali del sistema di attribuzione delle **procure**, ai fini di un'efficace prevenzione dei Reati sono i seguenti:

a) le procure funzionali sono conferite esclusivamente per il compimento di specifiche attività a soggetti dotati di delega interna che descriva i relativi poteri di gestione;

b) le procure che attribuiscono un potere di firma singola fissano limiti di spesa; sono inoltre accompagnate da apposita disposizione interna che fissa, oltre ai limiti di spesa, l'ambito nel quale può essere esercitato tale potere di rappresentanza.

L'OdV, con il supporto delle funzioni competenti, ha il potere di verificare il rispetto del sistema di deleghe e procure attuato dalla Società e la loro coerenza con i principi e le regole generali sopra indicate, segnalando al vertice aziendale eventuali anomalie riscontrate..

### 2.5.2 Il sistema dei controlli interni

Il sistema dei controlli interni, finalizzato alla prevenzione dei Reati, si basa sui seguenti principi:

a) la verificabilità e documentabilità di ogni operazione rilevante ai fini del D.Lgs. 231/2001, comprese le operazioni effettuate nell'ambito di attività esternalizzate;

b) la separazione delle funzioni e l'individuazione specifica dei ruoli e delle responsabilità dei soggetti coinvolti nello svolgimento delle attività, comprese quelle affidate in *outsourcing*;

c) la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;

d) la definizione di flussi informativi tra gli Organi Sociali e le funzioni aziendali, nonché tra questi e l'Organismo di Vigilanza;

In particolare, il sistema di controllo interno in essere presso la Società si caratterizza per la presenza dei seguenti organi e funzioni:

a) Collegio Sindacale;

b) Revisione contabile;

c) Funzione *Compliance*;

d) Funzione *Internal Audit*;

e) Funzione *Risk Management*.

*a) Collegio sindacale*

Il Collegio Sindacale esercita le funzioni previste dall'art. 2403 c.c., e si compone di tre Sindaci Effettivi e due Supplenti nominati dall'assemblea per tre esercizi.

Tutti i componenti il Collegio Sindacale devono possedere i requisiti richiesti dalle vigenti disposizioni di legge e regolamenti.

L'assemblea provvede anche alla designazione del Presidente del Collegio Sindacale e a quant'altro occorra, sempre a termini di legge.

Ai sindaci è attribuito un compenso fissato dall'assemblea.

Le riunioni del Collegio Sindacale possono svolgersi per tele o videoconferenza.

Inoltre, ai sensi del Regolamento IVASS del 3 luglio 2018, n. 38, il Collegio Sindacale verifica l'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dall'impresa e il suo concreto funzionamento, ai fini della normativa applicabile. Per l'espletamento dei

propri compiti, il Collegio Sindacale può richiedere la collaborazione di tutte le strutture che svolgono compiti di controllo. Il Collegio Sindacale:

a) acquisisce, all'inizio del mandato, conoscenze sull'assetto organizzativo aziendale ed esamina i risultati del lavoro della società di revisione per la valutazione del sistema di controllo interno e del sistema amministrativo contabile;

b) verifica l'idoneità della definizione delle deleghe, nonché l'adeguatezza dell'assetto organizzativo, prestando particolare attenzione alla separazione di responsabilità nei compiti e nelle funzioni;

c) valuta l'efficienza e l'efficacia del sistema di governo societario, con particolare riguardo all'operato della funzione di revisione interna della quale deve verificare la sussistenza della necessaria autonomia, indipendenza e funzionalità; nell'ipotesi in cui tale funzione sia stata esternalizzata valuta il contenuto dell'incarico sulla base del relativo contratto;

d) mantiene un adeguato collegamento con la funzione di revisione interna;

e) cura il tempestivo scambio con la società di revisione dei dati e delle informazioni rilevanti per l'espletamento dei propri compiti, esaminando anche le periodiche relazioni della società di revisione;

f) segnala all'organo amministrativo le eventuali anomalie o debolezze dell'assetto organizzativo e del sistema di governo societario, indicando e sollecitando idonee misure correttive; nel corso del mandato pianifica e svolge, anche coordinandosi con la società di revisione, periodici interventi di vigilanza volti ad accertare se le carenze o anomalie segnalate siano state superate e se, rispetto a quanto verificato all'inizio del mandato, siano intervenute significative modifiche dell'operatività della società che impongano un adeguamento dell'assetto organizzativo e del sistema di governo societario;

g) in caso di società appartenenti al medesimo gruppo, assicura i collegamenti funzionali e informativi con gli organi di controllo delle altre società appartenenti al gruppo;

h) conserva una adeguata evidenza delle osservazioni e delle proposte formulate e della successiva attività di verifica dell'attuazione delle eventuali misure correttive.

*b) Revisione contabile*

Tale controllo, ai sensi dello Statuto della Società, è affidato ad una società di revisione ai sensi dell'art. 2409-*bis* c.c.

*c) Funzione di verifica della conformità (o* Compliance*)*

Tale funzione è prevista dagli artt. 33 e 34 del Regolamento IVASS del 3 luglio 2018, n. 38. La Funzione di verifica della conformità è incaricata di valutare che l'organizzazione e le procedure interne dell'impresa siano adeguate a garantire il raggiungimento degli obiettivi di cui all'art. 33 del Regolamento n. 38/2018, il quale prevede: "*Nell'identificazione e valutazione del rischio di non conformità alle norme, l'impresa pone, tra gli altri, attenzione al rispetto delle norme relative alla trasparenza e correttezza dei comportamenti nei confronti degli assicurati e danneggiati, all'informativa precontrattuale e contrattuale, alla corretta esecuzione dei contratti, con specifico riferimento alla gestione dei sinistri e, più in generale, alla tutela degli assicurati e degli altri aventi diritto a prestazioni assicurative*".

La Funzione di verifica della conformità svolge i seguenti compiti:

a) identifica in via continuativa le norme applicabili all'impresa, valuta il loro impatto sui processi e le procedure aziendali, prestando attività di supporto e consulenza agli organi sociali e alle altre funzioni aziendali sulle materie per cui assume rilievo il rischio di non conformità, con particolare riferimento alla progettazione dei prodotti;

b) valuta l'adeguatezza e l'efficacia delle misure organizzative adottate per la prevenzione del rischio di non conformità alle norme e propone le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio;

c) valuta l'efficacia degli adeguamenti organizzativi conseguenti alle modifiche suggerite;

d) predispone adeguati flussi informativi diretti agli organi sociali dell'impresa e alle altre strutture coinvolte.

*d) Funzione di revisione interna (o* Internal Audit*)*

Tale funzione è prevista dagli artt. 35, 36 e 37 del Regolamento IVASS del 3 luglio 2018, n. 38. A norma dell'art. 35 del citato regolamento, la Funzione di revisione interna è "*incaricata di valutare e monitorare l'efficacia, l'efficienza e l'adeguatezza del sistema di controllo interno e delle ulteriori componenti del sistema di governo societario e le eventuali necessità di adeguamento, anche attraverso attività di supporto e di consulenza alle altre funzioni aziendali*".

Precisa, poi, l'art. 36 del suddetto regolamento che la funzione di revisione interna uniforma la propria attività agli standard professionali comunemente accettati a livello nazionale e internazionale e verifica:

a) la correttezza dei processi gestionali e l'efficacia e l'efficienza delle procedure organizzative;

b) la regolarità e la funzionalità dei flussi informativi tra settori aziendali;

c) l'adeguatezza dei sistemi informativi e la loro affidabilità affinché non sia inficiata la qualità delle informazioni sulle quali il vertice aziendale basa le proprie decisioni;

d) la rispondenza dei processi amministrativo contabili a criteri di correttezza e di regolare tenuta della contabilità;

e) l'efficacia dei controlli svolti sulle attività esternalizzate.

Durante l'esecuzione dell'attività di revisione e in sede di valutazione e segnalazione delle relative risultanze, la funzione di revisione interna:

a) svolge i compiti ad essa assegnati con autonomia ed obiettività di giudizio, in modo da preservare la propria indipendenza e imparzialità, in coerenza con le direttive a tal fine definite dall'organo amministrativo;

b) instaura collegamenti organici con tutti i centri titolari di funzioni di controllo interno.

A seguito dell'analisi sull'attività oggetto di controllo, il titolare della funzione di revisione interna procede, secondo le modalità e la periodicità fissata dall'organo amministrativo, a comunicare all'organo amministrativo, all'alta direzione e all'organo di controllo, la valutazione delle risultanze e le eventuali disfunzioni e criticità; resta fermo l'obbligo di segnalare con urgenza all'organo amministrativo e a quello di controllo le situazioni di particolare gravità.

L'attività di revisione, con specifica evidenza degli interventi effettuati, è adeguatamente documentata, raccolta e archiviata. I rapporti di revisione sono obiettivi, chiari, concisi e tempestivi, contengono suggerimenti per eliminare le carenze riscontrate, riportando raccomandazioni in ordine ai tempi per la loro rimozione. I rapporti sono conservati presso la sede della società o mediante modalità alternative di assolvimento dell'obbligo di conservazione documentale coerenti con quanto previsto da ulteriori disposizioni attuative emanate dall'IVASS, e sono redatti in modo tale da consentire di effettuare una valutazione

in merito all'efficacia dell'attività svolta dalla funzione stessa e anche di riconsiderare le revisioni effettuate e le risultanze prodotte. Le risultanze della specifica area oggetto di controllo sono altresì comunicate al responsabile della funzione interessata dall'attività di revisione.

La revisione interna si conclude con l'attività di *follow-up*, consistente nella verifica a distanza di tempo dell'efficacia delle correzioni apportate al sistema.

*e) Funzione di gestione dei rischi (*Risk Management*)*

Tale funzione è prevista dall'art. 32 del Regolamento IVASS del 3 luglio 2018, n. 38. A norma di detto articolo, la Funzione di gestione dei rischi:

a) concorre alla definizione della politica di gestione del rischio e, in particolare, alla scelta dei criteri e delle relative metodologie di misurazione dei rischi;

b) concorre alla definizione dei limiti operativi assegnati alle strutture operative e definisce le procedure per la tempestiva verifica dei limiti medesimi;

c) valida i flussi informativi necessari ad assicurare il tempestivo controllo delle esposizioni ai rischi e l'immediata rilevazione delle anomalie riscontrate nell'operatività;

d) almeno:

   i. concorre alla definizione della politica di valutazione dei rischi e della solvibilità;

   ii. contribuisce alla scelta delle metodologie, criteri e ipotesi utilizzate per le valutazioni;

   iii. segnala, se non già inclusi nella relazione sulla valutazione interna del rischio e della solvibilità, all'organo amministrativo i rischi individuati come significativi, anche in termini potenziali e riferisce, altresì, in merito ad ulteriori specifiche aree di rischio, d'iniziativa o su richiesta dell'organo stesso;

e) predispone la reportistica nei confronti dell'organo amministrativo, dell'alta direzione e dei responsabili delle strutture operative circa l'evoluzione dei rischi e la violazione dei limiti operativi fissati;

f) verifica la coerenza dei modelli di misurazione dei rischi con l'operatività dell'impresa e concorre all'effettuazione delle analisi di scenario o di stress test

operati anche nell'ambito della valutazione interna del rischio o della solvibilità o su richiesta di IVASS;

g) nel caso di utilizzo di modelli interni completi o parziali, verifica che il modello interno utilizzato sia e rimanga coerente con il profilo di rischio dell'impresa; a tal fine scambia informazioni e collabora con gli utilizzatori del modello interno, con le altre funzioni fondamentali e in particolare con la funzione attuariale;

h) monitora l'attuazione della politica di gestione del rischio e il profilo generale di rischio dell'impresa nel suo complesso;

i) collabora alla definizione dei meccanismi di incentivazione economica del personale.

Il titolare della funzione di gestione del rischio presenta all'organo amministrativo il piano di attività e riferisce, tra l'altro, sull'adeguatezza ed efficacia del sistema di gestione dei rischi, sulle metodologie e modelli utilizzati, in particolare nell'ambito della valutazione interna del rischio e della solvibilità, per il presidio dei rischi stessi. La funzione cura l'attuazione del sistema di gestione dei rischi, sulla base di una visione organica di tutti i rischi cui l'impresa è esposta, incluso il rischio di riservazione, atta a consentire l'individuazione tempestiva di modifiche al profilo di rischio.

Le funzioni *Compliance*, *Internal Audit* e *Risk Management* sono presenti in CAA a fronte di un contratto di servizi con CA Vita.

Con particolare riferimento alle **attività esternalizzate**, il sistema di organizzazione e controllo aziendale (formalizzato anche all'interno di una Politica di esternalizzazione), in considerazione delle responsabilità che ne possono derivare, s'ispira ai seguenti principi di:

a) individuazione specifica dei ruoli e delle responsabilità dei soggetti coinvolti nello svolgimento delle attività;

b) tracciabilità dei processi aziendali affidati in *outsourcing*;

c) definizione delle modalità e dei livelli di qualità del servizio;

d) istituzione di flussi informativi tra l'outsourcer di servizi e il soggetto esternalizzante.

### 2.6 La procedura di adozione del Modello

Sebbene l'adozione del Modello sia prevista dalla legge come facoltativa e non obbligatoria, CAA ha ritenuto comunque necessario procedere alla predisposizione del presente Modello, la cui adozione è sottoposta a deliberazione del Consiglio di Amministrazione.

Essendo il Modello un atto di emanazione dell'organo dirigente (in conformità alle prescrizioni dell'art. 6, comma 1, *lett. a* del D.Lgs. 231/2001) le successive modifiche e integrazioni sono rimesse alla competenza del Consiglio di Amministrazione di CAA, salva la facoltà di quest'ultimo di delegare per le modifiche di minor entità l'Amministratore Delegato, sentito l'Organismo di Vigilanza.

Il Consiglio di Amministrazione delibera annualmente sulla eventuale ratifica di tutte le modifiche e le integrazioni che siano state apportate dall'Amministratore Delegato, sentito l'Organismo di Vigilanza. La pendenza della ratifica da parte del Consiglio di Amministrazione non sospende, tuttavia, l'efficacia provvisoria delle modifiche e delle integrazioni nel frattempo apportate dall'Amministratore Delegato.

### 2.7 Destinatari del Modello

Le regole contenute nel presente Modello si rivolgono:

a) alle persone che rivestono funzioni di rappresentanza, amministrazione o direzione della Società;

b) alle persone che esercitano, anche di fatto, la gestione e il controllo della Società stessa;

c) a tutti i dipendenti della Società sottoposti alla direzione o alla vigilanza dei soggetti di cui sopra;

d) limitatamente a quanto specificamente indicato nei relativi accordi contrattuali, ai Consulenti, *Partner* (commerciali/finanziari), Fornitori, agenti, procuratori e, in genere, ai terzi che operano per conto o comunque nell'interesse della Società.

Il Modello e i contenuti dello stesso sono comunicati ai soggetti interessati con modalità idonee ad assicurarne l'effettiva conoscenza, secondo quanto indicato al successivo Capitolo 5 della presente Parte Generale; pertanto, i Destinatari del Modello sono tenuti a rispettare puntualmente tutte le disposizioni, anche in adempimento dei doveri di correttezza e diligenza derivanti dal rapporto giuridico da essi instaurato con la Società.

# CAPITOLO 3

# L'ORGANISMO DI VIGILANZA

## 3.1 Identificazione dell'organismo di vigilanza

Ai sensi dell'art. 6, lett. b), D.Lgs. 231/2001, condizione indispensabile per la concessione dell'esimente dalla responsabilità amministrativa è l'attribuzione ad un organismo della Società, dotato di autonomi poteri di iniziativa e di controllo, del compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento.

Sul tema le Linee Guida ANIA, interpretando le disposizioni del Decreto, ne suggeriscono l'individuazione in un organismo interno alla struttura della società, caratterizzato da autonomia, indipendenza, efficienza operativa e continuità di azione, nonché in possesso di professionalità ed onorabilità adeguate al ruolo.

I singoli requisiti che devono caratterizzare l'Organismo di Vigilanza sono i seguenti.

*a) Autonomia e indipendenza*

Il requisito di autonomia e indipendenza presuppone che l'OdV risponda, nello svolgimento di questa sua funzione, solo al massimo vertice gerarchico (ad esempio, Amministratore Delegato, Consiglio di Amministrazione e Collegio Sindacale).

In sede di costituzione dell'OdV, la sua autonomia è assicurata dall'obbligo, in capo all'organo dirigente, di approvare una dotazione annua adeguata di risorse finanziarie, anche su proposta dell'Organismo di Vigilanza stesso, della quale quest'ultimo potrà disporre per ogni esigenza necessaria al corretto svolgimento dei propri doveri (ad esempio consulenze specialistiche, trasferte, ecc.).

L'indipendenza, infine, presuppone che i membri dell'Organismo di Vigilanza non si trovino in una posizione, neppure potenziale di conflitto d'interessi con la Società, né siano titolari all'interno della stessa di funzioni di tipo operativo che ne minerebbero l'obiettività di giudizio nel momento delle verifiche sul rispetto del Modello.

*b) Onorabilità e cause di ineleggibilità*

Non possono essere eletti membri dell'Organismo di Vigilanza e, se lo sono, decadono necessariamente e automaticamente dalla carica:

i. coloro che si trovano nelle condizioni previste dall'articolo 2382 c.c., ovverosia gli inabilitati, interdetti, falliti o condannati ad una pena che comporti l'interdizione, anche temporanea, da uffici pubblici o l'incapacità ad esercitare uffici direttivi;

ii. coloro che siano stati sottoposti a misure di prevenzione disposte dall'autorità giudiziaria ai sensi della legge 27 dicembre 1956, n. 1423 (cosiddetta legge sulle misure di prevenzione nei confronti delle persone pericolose per la sicurezza e per la pubblica moralità) o della legge 31 maggio 1965, n. 575 (cosiddetta legge antimafia);

iii. coloro che sono stati condannati a seguito di sentenza ancorché non ancora definitiva, o emessa *ex* artt. 444 e ss. del codice di procedura penale o anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:

1) per uno dei delitti previsti nel titolo XI del libro V del c.c. (Disposizioni penali in materia di società e consorzi) e nel Regio Decreto 16 marzo 1942, n. 267, e sue successive modifiche od integrazioni (disciplina del fallimento, del concordato preventivo, dell'amministrazione controllata e della liquidazione coatta amministrativa);

2) a pena detentiva, non inferiore ad un anno, per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento (tra questi si segnalano, a titolo esemplificativo e non esaustivo, i reati di abusivismo bancario e finanziario di cui agli artt. 130 e seguenti del Testo Unico Bancario, i reati di falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate di cui all'art. 453 c.p., i reati di fraudolento danneggiamento dei beni assicurati e mutilazione fraudolenta della propria persona di cui all'art. 642 c.p.);

3) per un delitto contro la pubblica amministrazione, o alla reclusione per un tempo non inferiore ad un anno per un delitto contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica ovvero per un delitto in materia tributaria;

4) alla reclusione per un tempo non inferiore a due anni per un qualunque delitto non colposo;

5) in ogni caso e a prescindere dall'entità della pena per uno o più illeciti tra quelli tassativamente previsti dal D.Lgs. 231/01;

iv. coloro che hanno rivestito la qualifica di componente dell'OdV in società nei cui confronti siano state applicate le sanzioni previste dall'art. 9, D.Lgs. 231/01, salvo

che siano trascorsi 5 anni dalla inflizione in via definitiva delle sanzioni e il componente non sia incorso in condanna penale ancorché non definitiva;

v. coloro nei cui confronti siano state applicate le sanzioni amministrative accessorie previste dall'art. 187-*quater* TUF (D.lgs. n. 58/1998).

*c) Comprovata professionalità, capacità specifiche in tema di attività ispettiva e consulenziale*

L'Organismo di Vigilanza deve possedere, al suo interno, competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite alla sua indipendenza, ne garantiscono l'obiettività di giudizio; è necessario, pertanto, che all'interno dell'Organismo di Vigilanza siano presenti soggetti con professionalità adeguate in materia economica, di controllo e gestione dei rischi aziendali. L'Organismo di Vigilanza potrà, inoltre, anche avvalendosi di professionisti esterni, dotarsi di risorse competenti in materia giuridica di organizzazione aziendale, revisione, contabilità e finanza.

*d) Continuità d'azione*

L'Organismo di Vigilanza svolge in modo continuativo le attività necessarie per la vigilanza in merito alla corretta applicazione del Modello con adeguato impegno e con i necessari poteri di indagine; è una struttura interna alla società, in modo da garantire la dovuta continuità nell'attività di vigilanza; cura l'attuazione del Modello assicurandone il costante aggiornamento; non svolge mansioni operative che possano condizionare e contaminare quella visione d'insieme sull'attività aziendale che ad esso si richiede.

In ottemperanza a quanto stabilito dal Decreto, e da tutto quanto sopra indicato, il Consiglio di Amministrazione della Società ha ritenuto che la composizione dell'Organismo di Vigilanza che meglio risponde ai requisiti indicati dal Decreto è la seguente:

a) un professionista esterno con comprovata esperienza in ambito giuridico e legale, e, in particolare, di *compliance* al D.Lgs. 231/01;

b) il responsabile della funzione *Internal Audit*;

c) il responsabile dell'Area Compliance.

Tale scelta è stata determinata dal fatto che le suddette figure sono state riconosciute come le più adeguate ad assumere il ruolo dell'OdV in quanto, oltre ai requisiti di autonomia, indipendenza, professionalità, onorabilità e continuità d'azione che si richiedono per tale funzione, e alle capacità specifiche in tema di attività ispettive e consulenziali, possiedono altresì quei requisiti soggettivi formali che garantiscano ulteriormente l'autonomia e

l'indipendenza richiesta dal compito affidato, quali onorabilità, assenza di conflitti di interessi e di relazioni di parentela con gli organi sociali e con il vertice.

### 3.2 Durata in carica

Il Consiglio di Amministrazione provvede alla nomina dell'Organismo di Vigilanza mediante apposita delibera consiliare: a tal riguardo, al momento della nomina devono essere forniti nel corso della riunione consiliare adeguati chiarimenti in merito alla professionalità dei suoi componenti, il cui *curriculum vitae* viene allegato al relativo verbale.

L'OdV viene nominato per un periodo di tre anni, coincidente con quello previsto per la durata del Collegio Sindacale in carica al momento della nomina.

Alla scadenza dell'incarico, l'OdV potrà continuare a svolgere le proprie funzioni e ad esercitare i poteri di propria competenza, come in seguito meglio specificati, sino alla nomina dei nuovi componenti da parte del Consiglio di Amministrazione.

Al fine di garantire i requisiti di indipendenza e di autonomia, dal momento della nomina e per tutta la durata della carica, i componenti dell'Organismo:

a) non devono rivestire incarichi esecutivi o delegati nel Consiglio di Amministrazione della Società;

b) non devono svolgere funzioni operative o di business all'interno della Società;

c) non devono intrattenere significativi rapporti d'affari con la Società, con società da essa controllate o ad essa collegate, salvo il rapporto di lavoro subordinato o l'eventuale appartenenza al Collegio Sindacale, né intrattenere significativi rapporti d'affari con gli amministratori muniti di deleghe (amministratori esecutivi);

d) non devono avere rapporti con o far parte del nucleo familiare degli amministratori esecutivi, dovendosi intendere per nucleo familiare quello costituito dal coniuge non separato legalmente, dai parenti e affini entro il quarto grado;

e) non devono risultare titolari, direttamente o indirettamente, di partecipazioni nel capitale della Società;

f) devono avere e mantenere i requisiti di onorabilità indicati nella lettera b) del paragrafo 3.1 che precede.

I componenti dell'Organismo di Vigilanza sono tenuti a sottoscrivere, all'atto della nomina e poi periodicamente, una dichiarazione attestante l'esistenza e la successiva persistenza dei requisiti di indipendenza di cui sopra e, comunque, a comunicare immediatamente al

Consiglio e agli altri componenti dell'Organismo di Vigilanza l'insorgere di eventuali condizioni ostative.

Rappresentano ipotesi di decadenza automatica le incompatibilità di cui alle precedenti lettere da a) ad e), le circostanze di cui alla lettera f), la sopravvenuta incapacità e la morte; fatte salve le ipotesi di decadenza automatica, i membri dell'Organismo non possono essere revocati dal Consiglio di Amministrazione se non per giusta causa.

Rappresentano ipotesi di giusta causa di revoca:

a) una sentenza di condanna della Società ai sensi del Decreto o una sentenza di patteggiamento, passata in giudicato, ove risulti dagli atti l'omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;

b) la violazione degli obblighi di riservatezza di cui al successivo paragrafo 3.9;

c) la mancata partecipazione a più di tre riunioni consecutive senza giustificato motivo;

d) grave negligenza nell'adempimento dei propri compiti;

e) in caso di soggetti interni alla struttura aziendale, le eventuali dimissioni o licenziamento.

In caso di dimissioni o di decadenza automatica di un membro effettivo dell'Organismo di Vigilanza, quest'ultimo ne darà comunicazione tempestiva al Consiglio di Amministrazione, che prenderà senza indugio le decisioni del caso.

L'Organismo di Vigilanza si intende decaduto se viene a mancare, per dimissioni o altre cause, la maggioranza dei componenti. In tal caso, il Consiglio di Amministrazione provvede a nominare nuovi componenti.

### 3.3 Funzione e poteri dell'organo di controllo interno

All'OdV è affidato il compito di vigilare:

a) sull'osservanza del Modello da parte dei Destinatari;

b) sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale e alla effettiva capacità di prevenire la commissione dei Reati;

c) sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative.

Su un piano più operativo, all'OdV è affidato il compito di:

i. *Aggiornamenti, potestà normativa, segnalazioni*:

   a. suggerire e promuovere l'emanazione di disposizioni procedurali attuative dei principi e delle regole contenute nel Modello;

   b. interpretare la normativa rilevante e verificare l'adeguatezza del Modello a tali prescrizioni normative, segnalando al Consiglio di Amministrazione le possibili aree di intervento;

   c. valutare le esigenze di aggiornamento del Modello, segnalando al Consiglio di Amministrazione (o, per le modifiche minori, all'Amministratore Delegato) le possibili aree di intervento;

   d. indicare nelle relazioni semestrali al Consiglio di Amministrazione di cui al paragrafo 3.6 le opportune integrazioni ai sistemi di gestione delle risorse finanziarie (sia in entrata che in uscita), già presenti in CAA, per introdurre alcuni accorgimenti idonei a rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto;

   e. indicare nelle relazioni semestrali al Consiglio di Amministrazione di cui al paragrafo 3.6 l'opportunità di emanare particolari disposizioni procedurali attuative dei principi contenuti nel Modello, che potrebbero non essere coerenti con quelle in vigore attualmente nella Società, curando altresì il coordinamento delle stesse con quanto esistente.

ii. *Verifiche e controlli*:

   a. condurre – attraverso i componenti aziendali interni all'OdV – ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura delle Attività Sensibili;

   b. in ottemperanza a quanto previsto nel calendario annuale delle attività dell'organismo, effettuare – attraverso i componenti aziendali interni all'OdV – periodiche verifiche mirate su determinate operazioni o specifici atti posti in

essere da CAA, soprattutto nell'ambito delle Attività Sensibili, i cui risultati devono essere riassunti in sede di *reporting* agli organi Sociali deputati;

c. raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere ad esso trasmesse o tenute a propria disposizione (vedi in dettaglio il successivo par. 3.7);

d. coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per il miglior monitoraggio delle attività in relazione alle procedure stabilite nel Modello. A tal fine, l'OdV ha libero accesso a tutta la documentazione aziendale (sia cartacea sia informatica) che ritiene rilevante e deve essere costantemente informato dal *management*: a) sugli aspetti dell'attività aziendale che possono esporre CAA al rischio di commissione di uno dei Reati; b) sui rapporti con la Rete Distributiva, i Consulenti e i *Partner* che operano per conto della Società nell'ambito di Operazioni Sensibili;

e. attivare e svolgere le inchieste interne, raccordandosi di volta in volta con le funzioni aziendali interessate per acquisire ulteriori elementi di indagine;

f. sollecitare l'attuazione delle procedure di controllo previste dal Modello anche tramite l'emanazione o proposizione di disposizioni (normative e/o informative) interne;

iii. *Formazione*:

a. coordinarsi con gli incaricati della gestione delle Risorse Umane per la definizione dei programmi di formazione per il personale stesso e del contenuto delle comunicazioni periodiche da farsi ai Dipendenti e agli Organi Sociali, finalizzate a fornire ai medesimi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al D.Lgs. 231/2001;

b. coordinarsi con il responsabile dell'Ufficio del Personale della Rete Distributiva del Gruppo per la definizione dei programmi di formazione della Rete Distributiva e del contenuto delle comunicazioni periodiche da farsi alla medesima, finalizzate a fornire ai medesimi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al D.Lgs. 231/2001;

c. monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione interna necessaria al fine della

sua efficace attuazione, contenente istruzioni d'uso, chiarimenti o aggiornamenti dello stesso;

d. far predisporre e aggiornare con continuità lo spazio nell'Intranet del Gruppo contenente tutte le informazioni relative al D.Lgs. 231/2001 e al Modello.

*iv.* *Sanzioni:*

a. coordinarsi con il *management* aziendale per valutare o proporre l'adozione di eventuali sanzioni o provvedimenti, fermo restando la competenza di quest'ultimo – e, in particolare, degli incaricati della gestione delle Risorse Umane – in merito alla decisione e alla irrogazione dei medesimi (si rinvia in merito a questo punto al successivo Capitolo 5 della presente Parte Generale).

### 3.4 Poteri dell'Organismo di Vigilanza

L'OdV ha, *ex lege*, autonomi poteri di iniziativa e controllo ai fini di vigilare sul funzionamento e l'osservanza del Modello, ma non ha poteri coercitivi o di intervento sulla struttura aziendale o sanzionatori, poteri questi che sono demandati ai competenti Organi Sociali o alle funzioni aziendali competenti.

Tenuto conto delle peculiarità delle attribuzioni e degli specifici contenuti professionali richiesti, nello svolgimento dei compiti di vigilanza e controllo l'OdV sarà costantemente supportato anche da tutti i dirigenti e dal *management* della Società. In capo a questi ultimi, nell'ambito delle rispettive funzioni e nei limiti delle deleghe assegnate, ricade una responsabilità primaria per quanto concerne: (i) il controllo delle attività e delle aree di competenza; (ii) l'osservanza del Modello da parte dei Dipendenti sottoposti alla loro direzione; (iii) la tempestiva e puntuale informazione verso l'OdV su eventuali anomalie, problematiche riscontrate e/o criticità rilevate.

L'OdV potrà richiedere ai dirigenti specifiche attività di controllo sul corretto e preciso funzionamento del Modello.

Tutti i soggetti coinvolti all'interno della struttura aziendale sono tenuti a vigilare e informare l'OdV sulla corretta applicazione del presente Modello, ciascuno nell'ambito delle proprie competenze operative.

L'OdV può avvalersi, ogni qualvolta lo ritiene necessario all'espletamento della propria attività di vigilanza e di tutto quanto previsto nel presente Modello, della collaborazione di

ulteriori risorse, prescelte nell'ambito delle varie funzioni aziendali, senza limitazioni di tempo e di numero.

L'autonomia e l'indipendenza che necessariamente devono connotare le attività dell'OdV hanno reso necessario introdurre alcune forme di tutela in suo favore, al fine di garantire l'efficacia del Modello e di evitare che la sua attività di controllo possa ingenerare forme di ritorsione a suo danno. Pertanto, le decisioni in merito a remunerazione, promozioni, trasferimento o sanzioni relative all'OdV e ai suoi membri, allorquando essi siano dipendenti della Società, sono attribuite alla competenza esclusiva del Consiglio di Amministrazione, sentiti, laddove necessario, gli incaricati della gestione delle Risorse Umane.

Pertanto, il Consiglio di Amministrazione della Società conferisce all'OdV i seguenti poteri:

- potere di accedere a tutti i documenti e a tutte le informazioni relative alla Società;
- potere di avvalersi di tutte le strutture della Società, che sono obbligate a collaborare, dei revisori e di consulenti esterni;
- potere di raccogliere informazioni presso tutti i Dipendenti e i Collaboratori, inclusa la società di revisione, in relazione a tutte le attività della Società;
- potere di richiedere, attraverso i canali e le persone appropriate, la riunione del Consiglio di Amministrazione e del Collegio Sindacale per affrontare questioni urgenti;
- potere di richiedere ai titolari delle funzioni di partecipare, senza potere deliberante, alle sedute dell'Organismo di Vigilanza;
- potere di avvalersi di consulenti esterni ai quali delegare circoscritti ambiti di indagine o attività. A tale proposito, il Consiglio di Amministrazione dovrà approvare ogni anno un budget di spesa per l'OdV, il quale ne potrà disporre liberamente in relazione alle proprie attività, salvo richieste integrazioni per eventuali necessità sopravvenute.

### 3.5 Regole di convocazione e di funzionamento

L'Organismo di Vigilanza disciplina con specifico regolamento le modalità del proprio funzionamento, sulla base dei principi di seguito riportati:

- l'Organismo di Vigilanza si riunisce trimestralmente e la documentazione relativa viene distribuita almeno 3 giorni prima della seduta;
- le sedute si tengono di persona, per video o teleconferenza (o in combinazione);

- il Presidente, l'Amministratore Delegato, il Consiglio di Amministrazione e il Collegio Sindacale possono richiedere che l'Organismo di Vigilanza si riunisca in qualsiasi momento per un incontro con i medesimi;
- per la validità delle sedute è richiesto l'intervento della maggioranza dei membri in carica;
- possono essere effettuate sedute *ad hoc* e tutte le decisioni prese durante queste sedute devono essere riportate nella successiva seduta trimestrale;
- le decisioni vengono assunte sulla base di decisioni unanimi; in caso di mancanza di unanimità, prevale la decisione maggioritaria e ciò viene riportato immediatamente al Consiglio di Amministrazione;
- i verbali delle sedute riportano tutte le decisioni prese dall'organo e riflettono le principali considerazioni effettuate per raggiungere la decisione; tali verbali vengono conservati dall'Organismo di Vigilanza nel proprio archivio.

I suddetti princìpi si integrano con quanto previsto più nel dettaglio dal regolamento adottato dall'OdV.

### 3.6 Flussi informativi dell'OdV verso il vertice aziendale e il Collegio Sindacale e coordinamento con le funzioni aziendali

L'OdV riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità.

L'OdV ha due differenti tipologie di flussi informativi:

- la prima, su base continuativa, non appena ve ne sia la necessità, direttamente verso l'Amministratore Delegato;
- la seconda, su base almeno semestrale, anche tramite apposita relazione scritta, nei confronti del Consiglio di Amministrazione e del Collegio Sindacale.

Tali flussi informativi hanno ad oggetto:

1. l'attività svolta dall'ufficio dell'OdV;
2. le eventuali criticità (e spunti per il miglioramento) emerse sia in termini di comportamenti o eventi interni a CAA, sia in termini di efficacia del Modello. Qualora l'OdV rilevi criticità riferibili a qualcuno dei soggetti referenti, la corrispondente segnalazione è da destinarsi prontamente ad uno degli altri soggetti sopra individuati.

Le sunnominate relazioni semestrali nei confronti del Consiglio di Amministrazione e del Collegio Sindacale contengono:

(a) un'analisi sintetica di tutta l'attività svolta nel periodo di riferimento (indicando, in particolare, i controlli effettuati e l'esito degli stessi, le verifiche specifiche di cui al successivo Capitolo 6 della presente Parte Generale e l'esito delle stesse, l'eventuale aggiornamento della mappatura delle Attività Sensibili, ecc.);

(b) quanto alla relazione relativa al secondo semestre dell'anno, un piano delle attività previste per l'anno successivo.

Gli incontri con gli organi cui l'OdV riferisce vengono debitamente documentati.

Il Consiglio di Amministrazione e il Presidente del Consiglio di Amministrazione hanno la facoltà di convocare in qualsiasi momento l'OdV che, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione dei predetti organi per motivi urgenti.

L'OdV deve, inoltre, coordinarsi con le funzioni competenti presenti in Società per i diversi ambiti di controllo e precisamente:

- con la funzione Legale e Affari Societari per gli adempimenti Sociali che possano avere rilevanza ai fini della commissione dei Reati;
- con gli incaricati della gestione delle Risorse Umane in ordine alla formazione del personale e ai procedimenti disciplinari;
- con il responsabile delle funzioni Commerciale e *Marketing* e della funzione controlli reti distributive in ordine alla formazione della Rete Distributiva e ai relativi provvedimenti;
- con il responsabile dell'Area *Finance & Strategy* in ordine alla gestione dei flussi finanziari;
- con il RSPP per le tematiche relative alla sicurezza sul lavoro;
- con le funzioni di controllo (*Compliance*, *Internal Audit* e *Risk Management*) per il coordinamento dell'attività di verifica e controllo.

### 3.7 Flussi informativi verso l'OdV: informazioni di carattere generale e informazioni specifiche obbligatorie

Fermo restando quanto previsto *infra* in relazione al sistema di *whistleblowing* adottato da CAA, l'OdV deve essere informato, mediante appositi flussi informativi da parte dei Dipendenti, dei Dipendenti di CA Vita per i servizi prestati a CAA, degli Organi Sociali, della Rete Distributiva, dei Consulenti e dei *Partner* in merito ad eventi che assumono rilevanza – ancorché astratta – ai sensi del D.Lgs. 231/2001.

In particolare, alcune funzioni aziendali sono tenute all'invio periodico all'OdV di cosiddette "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento). I *format* di dette schede di flusso sono allegati al presente Modello, di cui costituiscono parte integrante.

I flussi informativi nei confronti dell'OdV devono essere inviati tramite e-mail all'indirizzo di posta elettronica

**odv@ca-assicurazioni.it**

Oltre ai flussi informativi sopra descritti, gli Organi Sociali, i Dipendenti, i Dipendenti di CA Vita e, nei modi e nei limiti previsti contrattualmente, la Rete Distributiva, i Consulenti e i *Partner* devono obbligatoriamente e immediatamente trasmettere all'OdV le informazioni concernenti:

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i Reati qualora tali indagini coinvolgano CAA o suoi Dipendenti, Organi Sociali, Rete Distributiva, Consulenti e *Partner*;
- i rapporti preparati dalle funzioni competenti nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D.Lgs. 231/2001;
- le notizie relative ai procedimenti sanzionatori svolti e alle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i Dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora essi siano legati a commissione di Reati o violazione delle regole di comportamento o procedurali del Modello.

Periodicamente l'OdV propone, se del caso, al Consiglio di Amministrazione o all'Amministratore Delegato eventuali modifiche della lista sopra indicata relativa alle informazioni obbligatorie ovvero modifiche o integrazioni alle "schede di flusso".

In ogni caso, qualora un Destinatario non adempia agli obblighi informativi di cui al presente paragrafo (abbiano essi a riguardo le segnalazioni "ad evento", quali, ad esempio, le notizie relative a provvedimenti dell'Autorità circa lo svolgimento di indagini, ovvero le segnalazioni periodiche, quali quelle da effettuarsi tramite le dianzi citate schede di flusso), allo stesso saranno inviati un numero massimo di due solleciti, dopodiché, in caso di mancato riscontro, l'OdV provvederà a richiedere alle funzioni competenti di valutare l'irrogazione di una sanzione disciplinare che varierà a seconda della gravità dell'inottemperanza agli obblighi sopra menzionati e che sarà irrogata secondo le regole indicate nel Capitolo 5 del presente Modello. Parimenti – come meglio spiegato *infra* – sarà punita con idonea sanzione l'effettuazione di segnalazioni con dolo o colpa grave ovvero la violazione delle misure previste a tutela del segnalante.

L'OdV, inoltre, ha il diritto di richiedere informazioni in merito al sistema di deleghe adottato da CAA, secondo modalità dallo stesso stabilite.

### 3.7.1. Raccolta e conservazione delle informazioni dell'OdV

I componenti dell'Organismo di Vigilanza assicurano la riservatezza delle informazioni di cui vengano in possesso, in particolare se relative a segnalazioni che agli stessi dovessero pervenire in ordine a presunte violazioni del Modello (che verranno trattate secondo le indicazioni contenute nel paragrafo 3.8).

I componenti dell'OdV si astengono, altresì, dall'utilizzare informazioni riservate per fini diversi da quelli di cui ai precedenti paragrafi e comunque per scopi non conformi alle funzioni proprie di un organismo di vigilanza.

L'inosservanza di tali obblighi costituisce giusta causa di revoca della carica.

Ogni informazione, segnalazione, *report* previsti nel presente Modello sono conservati dall'OdV in un apposito archivio (informatico o cartaceo) per dieci anni avendo cura di mantenere riservati i documenti e le informazioni acquisite, anche nel rispetto della normativa sulla privacy.

Per la raccolta e la conservazione delle informazioni relative a una segnalazione trasmessa in conformità al Decreto *Whistleblowing* devono essere osservate le regole stabilite da detto decreto e del Regolamento per le Segnalazioni (citati al successivo paragrafo 3.8.).

### 3.8 Il sistema di *whistleblowing*

Con riferimento all'istituto del cosiddetto "*whistleblowing*" previsto dall'art. 6, comma 2-*bis* del Decreto 231, la Società prevede un canale di segnalazione interna, il divieto di ritorsione e un sistema disciplinare conformi al Decreto *Whistleblowing*.

Le violazioni che possono essere segnalate ai sensi del Decreto *Whistleblowing* sono quelle di cui il segnalante sia venuto a conoscenza nell'ambito del proprio contesto lavorativo e che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o della Società; tra queste rientrano anche le segnalazioni di condotte illecite rilevanti ai sensi del Decreto 231 o violazioni del Modello 231, che non rientrano negli illeciti di seguito indicati.

In conformità a quanto previsto dal Decreto *Whistleblowing*, CAA ha istituito un canale interno (*i.e.* piattaforma informatica) che consente l'effettuazione di segnalazioni in forma scritta e in forma orale (garantendo, anche tramite crittografia, la riservatezza del segnalante e della persona coinvolta nonché del contenuto della segnalazione e della relativa documentazione).

La Società, al fine di disciplinare l'utilizzo del canale di segnalazione interno e la gestione delle segnalazioni nonché al fine di fornire informazioni chiare sui gestori delle segnalazioni e sui presupposti per l'effettuazione di una segnalazione, ha adottato un "*Regolamento per le Segnalazioni*" (aggiornato alla luce del Decreto *Whistleblowing* e delle principali linee guida in materia), al quale si fa rimando per l'indicazione dei canali di segnalazione attivati e per ogni ulteriore dettaglio.

Le segnalazioni che riguardano la Società e rientrano nel perimetro di applicazione del Regolamento per le Segnalazioni sono esaminate e gestite dal gestore (individuato nel Responsabile dell'Area *Compliance*) nel rispetto delle condizioni di autonomia e indipendenza previste dalla disciplina in materia di *whistleblowing*.

I soggetti individuati per la gestione delle segnalazioni o per supporto al gestore sono specificamente formati in materia di *whistleblowing* e autorizzati ai sensi del Regolamento UE n. 2016/679 (GDPR).

Il gestore individuato nel Regolamento è competente per ricevere anche tutte le segnalazioni riguardanti violazioni del Modello 231 e fatti idonei a configurare i reati presupposto previsti dal Decreto 231 ovvero situazioni di rischio in tale ambito ("**Segnalazioni 231**").

In caso di Segnalazioni 231, il gestore coinvolge, nel rispetto degli obblighi di riservatezza, l'Organismo di Vigilanza della Società che lo supporta nelle relative valutazioni e, ove necessario, nell'attività istruttoria.

I segnalanti non possono subire alcuna ritorsione e, a tal proposito, il Decreto *Whistleblowing* dispone la previsione di sanzioni pecuniarie e disciplinari a carico di chi realizza atti ritorsivi nonché misure di sostegno per i segnalanti e la possibilità per quest'ultimi di comunicare all'ANAC le ritorsioni che ritengono di aver subito in ragione di una segnalazione.

A tal riguardo, la Società adotta tutte le misure necessarie per garantire che sia assicurato il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante in ragione di una segnalazione.

Si precisa che ai sensi del Decreto *Whistleblowing*, le segnalazioni possono essere effettuate anche da soggetti esterni alla Società (indicati nel Decreto *Whistleblowing* e nel Regolamento per le Segnalazioni) e le tutele riservate al segnalante vengono estese anche a soggetti collegati (indicati nel Decreto *Whistleblowing* e nel Regolamento per le Segnalazioni).

## CAPITOLO 4

## LA FORMAZIONE DELLE RISORSE E LA DIFFUSIONE DEL MODELLO

### 4.1 Premessa

CAA, al fine di dare efficace attuazione al Modello, intende assicurare una corretta divulgazione dei contenuti e dei principi dello stesso all'interno e all'esterno della propria organizzazione.

In particolare, obiettivo di CAA è estendere la comunicazione dei contenuti e dei principi del Modello non solo ai propri dipendenti ma anche ai soggetti che, pur non rivestendo la qualifica formale di dipendente, operano – direttamente o indirettamente, stabilmente o temporaneamente – per il conseguimento degli obiettivi di CAA in forza di rapporti contrattuali.

L'attività di comunicazione e formazione è diversificata a seconda dei destinatari cui essa si rivolge ed è, in ogni caso, improntata a principi di completezza, chiarezza, accessibilità e continuità al fine di consentire ai diversi destinatari la piena consapevolezza di quelle disposizioni aziendali che sono tenuti a rispettare e delle norme etiche che devono ispirare i loro comportamenti.

La comunicazione e la formazione sui princìpi e contenuti del Modello vengono svolte periodicamente e sono garantite dai responsabili delle singole aree aziendali che – con il supporto della funzione aziendale competente – identificano la migliore modalità di fruizione di tali servizi: *staff meeting*, corsi istituzionali (in aula ovvero *web-based*), *induction*, ecc.

L'attività di comunicazione e formazione è supervisionata e monitorata dall'OdV.

### 4.2 Dipendenti e componenti degli organi sociali

Ogni soggetto che opera presso la Compagnia è tenuto a:

- acquisire consapevolezza dei principi e contenuti del Modello;
- conoscere le modalità operative con le quali deve essere realizzata la propria attività;
- contribuire attivamente, in relazione al proprio ruolo e alle proprie responsabilità, all'efficace attuazione del Modello, segnalando eventuali carenze riscontrate nello stesso.

Al fine di garantire un'efficace e razionale attività di comunicazione, CAA intende promuovere e agevolare la conoscenza dei contenuti e dei principi del Modello da parte dei

dipendenti e altri esponenti aziendali con grado di approfondimento diversificato a seconda della posizione e del ruolo dagli stessi ricoperto, nonché delle aree in cui essi operano.

L'adozione del presente Modello (nelle versioni periodicamente aggiornate) è comunicata a tutte le risorse presenti in azienda.

Ai nuovi dipendenti e ai nuovi componenti degli organi sociali viene consegnato un *set* informativo (ad esempio, Modello Organizzativo, Codice Etico, la Carta Etica, Codice di Condotta, ecc.), con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza.

Idonei strumenti di comunicazione saranno adottati per aggiornare il personale circa le eventuali modifiche apportate al Modello, nonché ogni rilevante cambiamento procedurale, normativo o organizzativo.

All'interno dei piani di formazione periodica (verso il personale e verso il *management*) previsti dalla Società, è inserita anche la formazione in materia di *whistleblowing*.

La mancata partecipazione all'attività di formazione senza giustificazione da parte degli Esponenti Aziendali costituisce una violazione dei principi contenuti nel presente Modello e, pertanto, sarà sanzionata ai sensi di quanto indicato nel seguente Capitolo 6.

### 4.3 Altri destinatari

L'attività di comunicazione dei contenuti e dei principi del Modello (e nel Regolamento per le Segnalazioni richiamato dallo stesso) dovrà essere indirizzata anche nei confronti di quei soggetti terzi che intrattengano con CAA rapporti contrattualmente regolati, anche di collaborazione, o che rappresentano la Società senza vincoli di dipendenza (ad esempio, Fornitori, Consulenti e *Partner*).

A tal fine, i Fornitori, i Consulenti e i *Partner* verranno adeguatamente informati, anche tramite apposite clausole negli accordi che regolano i loro rapporti con la Società, delle previsioni di cui al Modello, al Codice Etico, alla Carta Etica e al Codice di Condotta.

CAA, tenuto conto delle finalità del Modello, valuterà l'opportunità di comunicare i contenuti e i principi del Modello stesso a terzi, non riconducibili alle figure sopra indicate a titolo esemplificativo, e più in generale, al mercato.

# CAPITOLO 5

# SISTEMA SANZIONATORIO

## 5.1 Funzione del sistema sanzionatorio

La definizione di un sistema di sanzioni (commisurate alla violazione e dotate di adeguata efficacia deterrente) applicabili in caso di violazione delle regole di cui al presente Modello, rende effettiva l'azione di vigilanza dell'OdV ed ha lo scopo di garantirne l'efficace attuazione.

La definizione di tale sistema sanzionatorio costituisce, infatti, ai sensi dell'art. 6, comma 1, lett. *e)*, D.Lgs. 231/2001, un requisito essenziale del Modello medesimo ai fini dell'esimente rispetto alla responsabilità della Società.

In virtù di quanto previsto dal Decreto *Whistleblowing* e con riferimento a qualunque destinatario del Modello, si precisa che, tra le condotte passibili di sanzione, devono essere considerate anche le violazioni previste da detto decreto (per le quali oltre alle sanzioni disciplinari sono previste sanzioni amministrative pecuniarie da parte dell'ANAC)[1].

L'applicazione del sistema sanzionatorio e dei relativi provvedimenti è indipendente dallo svolgimento e dall'esito del procedimento penale che l'Autorità Giudiziaria abbia eventualmente avviato nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del D.Lgs. 231/2001.

Il presente capitolo contiene la descrizione delle misure sanzionatorie adottate dalla Società in caso di violazione del Modello da parte dei Destinatari, in coordinamento con il sistema disciplinare di cui al Contratto Collettivo Nazionale di Lavoro applicato da CAA, nel rispetto delle procedure previste dall'art. 7, legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori).

[1]Il Decreto *Whistleblowing* prevede sanzioni a carico di chi si rende responsabile delle seguenti condotte: 1) compimento di ritorsioni in relazione a segnalazioni; 2) ostacolo o tentato ostacolo all'effettuazione della segnalazione; 3) violazione degli obblighi di riservatezza previsti dalla Procedura e dal Decreto *Whistleblowing*; 4) mancata istituzione dei canali di segnalazione secondo i requisiti previsti dal Decreto *Whistleblowing*; 5) mancata adozione di una procedura per l'effettuazione e la gestione delle segnalazioni o mancata conformità della stessa al Decreto *Whistleblowing*; 6) mancata verifica e analisi delle segnalazioni ricevute. 7) È, inoltre, prevista l'irrogazione di una sanzione disciplinare nei confronti del segnalante quando è accertata in capo allo stesso: (i) anche con sentenza di primo grado, la responsabilità penale per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero (ii) la responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave.

## 5.2 Dipendenti soggetti al CCNL

### 5.2.1 Sistema sanzionatorio

La violazione da parte dei Dipendenti delle singole regole comportamentali di cui al presente Modello costituisce illecito disciplinare. Quanto di seguito riportato è esteso anche ai dipendenti e dirigenti di CA Vita per i servizi prestati a CAA in virtù dei contratti di servizio.

I provvedimenti sanzionatori irrogabili nei riguardi di detti lavoratori – nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) e delle eventuali normative speciali applicabili – sono quelli previsti dall'apparato sanzionatorio del CCNL applicato da CAA (in particolare, gli artt. 26 e ss., nonché artt. 75 e ss del CCNL relativi alla cessazione del rapporto di lavoro per giusta causa) e del relativo regolamento interno dalla Società adottato, e precisamente:

a) rimprovero verbale;

b) biasimo inflitto per iscritto;

c) sospensione dal servizio e dal trattamento economico per un periodo fino a 10 giorni;

d) risoluzione del rapporto di lavoro a seguito del recesso del datore di lavoro per giusta causa.

Restano ferme – e si intendono qui richiamate – tutte le previsioni dei richiamati CCNL e regolamento interno, relativamente alle procedure e agli obblighi da osservare nell'applicazione delle sanzioni.

Restano invariati i poteri già conferiti al *management* aziendale per quanto riguarda l'accertamento delle infrazioni, i procedimenti sanzionatori e l'irrogazione delle relative sanzioni.

### 5.2.2 Violazioni del Modello e relative sanzioni

Fermi restando gli obblighi per la Società nascenti dallo Statuto dei Lavoratori, i comportamenti sanzionabili sono i seguenti:

1) violazione di procedure interne previste dal presente Modello (ad esempio, non osservanza delle procedure prescritte, omissione di comunicazioni all'OdV in merito a informazioni prescritte, omissione di controlli, violazione non grave delle previsioni di cui al Regolamento per le Segnalazioni e del Decreto *Whistleblowing,*

ecc.) o adozione, nell'espletamento di attività connesse alle Attività Sensibili, di comportamenti non conformi alle prescrizioni del Modello;

- sanzione: rimprovero verbale

2) violazione di procedure interne previste dal presente Modello o adozione, nell'espletamento di attività connesse alle Attività Sensibili, di comportamenti non conformi alle prescrizioni del Modello stesso che espongano la Società ad una situazione oggettiva di rischio di commissione di uno dei Reati;

- sanzione: biasimo inflitto per scritto

3) adozione, nell'espletamento di attività connesse alle Attività Sensibili, di comportamenti non conformi alle prescrizioni del presente Modello e diretti dolosamente e in modo univoco al compimento di uno o più Reati, anche se poi non effettivamente perfezionati quale fattispecie criminosa;

- sanzione: sospensione dal servizio e del trattamento economico per un periodo non superiore a dieci giorni

4) adozione, nell'espletamento di attività connesse alle Attività Sensibili, di comportamenti palesemente in violazione delle prescrizioni del presente Modello, tale da determinare la concreta applicazione a carico della Società di sanzioni previste dal D. Lgs. 231/2001; violazione grave delle previsioni di cui al Regolamento per le Segnalazioni e del Decreto *Whistleblowing*:

- sanzione: risoluzione del rapporto di lavoro per recesso per giusta causa del datore di lavoro.

Le sanzioni verranno commisurate al livello di responsabilità e autonomia del Dipendente, all'eventuale esistenza di precedenti disciplinari a carico dello stesso, all'intenzionalità del suo comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui la Società può ragionevolmente ritenersi esposta - ai sensi e per gli effetti del D.Lgs. 231/2001 - a seguito della condotta censurata.

Il sistema sanzionatorio è soggetto a costante verifica e valutazione da parte dell'OdV e degli incaricati della gestione delle Risorse Umane, rimanendo quest'ultimi responsabili della concreta applicazione dei provvedimenti necessari su eventuale segnalazione dell'OdV e sentito il superiore gerarchico dell'autore della condotta censurata.

### 5.3 Misure nei confronti dei dirigenti

In caso di violazione, da parte di Dipendenti che ricoprano la qualifica di dirigenti, delle procedure previste dal presente Modello o di adozione, nell'espletamento di attività connesse con le Attività Sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso, la Società provvede ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dalla legge e dalla Contrattazione Collettiva applicabile.

La sanzione minima consisterà in una contestazione verbale o scritta al Dirigente.

Nelle ipotesi più gravi, come ad esempio la commissione di un Reato, sarà valutata l'ipotesi del licenziamento.

I comportamenti sanzionabili che costituiscono violazione del presente del Modello sono, a titolo esemplificativo, i seguenti:

a. adozione, nell'espletamento delle Attività Sensibili, di comportamenti non conformi alle prescrizioni del Modello e diretti in modo univoco al compimento di uno o più Reati riconducibili alla Società;

b. violazione di procedure interne previste dal presente Modello o adozione, nell'espletamento delle Attività Sensibili, di comportamenti non conformi alle prescrizioni del Modello stesso che espongano la Società ad una situazione oggettiva di rischio imminente di commissione di uno dei Reati;

c. violazione delle previsioni di cui al Regolamento per le Segnalazioni e del Decreto *Whistleblowing*.

Per quanto riguarda l'accertamento delle infrazioni e l'irrogazione delle sanzioni restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, agli Organi Societari e alle competenti direzioni aziendali.

***

Le sanzioni e l'eventuale richiesta di risarcimento dei danni verranno commisurate al livello di responsabilità e autonomia del dipendente e del dirigente, all'eventuale esistenza di precedenti disciplinari a carico del dipendente, all'intenzionalità del comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui la Società può ragionevolmente ritenersi esposta – ai sensi e per gli effetti del Decreto 231 – a seguito della condotta censurata.

L'adesione ai principi e alle regole contenute nel Modello costituisce elemento di fondamentale rilievo nella valutazione professionale della risorsa e ha riflessi diretti sul percorso di carriera e retributivo; in particolare, l'aderenza ai principi e alle regole che vengono richiamati nel Modello costituisce uno dei requisiti su cui vengono basati eventuali programmi di retribuzione variabile/premiale/MBO.

### 5.4 Misure nei confronti degli Amministratori

In caso di violazione del Modello da parte di uno o più membri del Consiglio di Amministrazione (ivi compresa l'ipotesi di violazione delle previsioni di cui al Regolamento per le Segnalazioni e del Decreto *Whistleblowing*), l'OdV informa il Collegio Sindacale e l'intero Consiglio di Amministrazione i quali prendono gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci al fine di adottare le misure più idonee previste dalla legge.

Inoltre, al momento della nomina dei nuovi amministratori, gli stessi procederanno a sottoscrivere impegni unilaterali di rispetto degli obblighi previsti dal Modello nonché un impegno a rassegnare le proprie dimissioni, rinunciando al proprio compenso relativo all'esercizio in corso, nel caso di condanna, anche di primo grado, per uno dei Reati.

Si coglie l'occasione per specificare che, nel caso in cui la Società venisse individuata quale ente incolpato nell'ambito di un procedimento *ex* Decreto 231 e in tale procedimento il legale rappresentante della Società fosse direttamente coinvolto in qualità di indagato per il reato presupposto dell'illecito amministrativo ascritto all'ente, la nomina del difensore dell'ente non verrebbe effettuata da detto legale rappresentante, bensì da altro/i soggetto/i, munito/i degli appositi poteri.

### 5.5 Misure nei confronti dei Sindaci

In caso di violazione del presente Modello da parte di uno o più Sindaci (ivi compresa l'ipotesi di violazione delle previsioni di cui al Regolamento per le Segnalazioni e del Decreto *Whistleblowing*), l'OdV informa l'intero Collegio Sindacale e il Consiglio di Amministrazione i quali prenderanno gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci al fine di adottare le misure più idonee previste dalla legge.

### 5.6 Misure nei confronti dei membri dell'OdV

In caso di violazione del presente Modello da parte di uno o più membri dell'OdV (ivi compresa l'ipotesi di violazione delle previsioni di cui al Regolamento per le Segnalazioni e

del Decreto *Whistleblowing*), gli altri membri dell'OdV ovvero uno qualsiasi tra i Sindaci o tra gli Amministratori, informerà immediatamente il Collegio Sindacale e il Consiglio di Amministrazione i quali prenderanno gli opportuni provvedimenti tra cui, ad esempio, la revoca dell'incarico ai membri dell'OdV che hanno violato il Modello e la conseguente nomina di nuovi membri in sostituzione degli stessi ovvero la revoca dell'incarico all'intero organo e la conseguente nomina di un nuovo OdV.

### 5.7 Misure nei confronti della Rete Distributiva, dei Consulenti, dei Fornitori e dei *Partner*

Ogni violazione da parte della Rete Distributiva, dei Consulenti, dei Fornitori o dei *Partner* delle regole di cui al presente Modello agli stessi applicabili (ivi compresa l'ipotesi di violazione delle previsioni di cui al e nel Regolamento per le Segnalazioni e del Decreto *Whistleblowing*) o di commissione dei Reati è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Società, come nel caso di applicazione alla stessa da parte dell'autorità giudiziaria delle misure previste dal D.Lgs. 231/2001.

## CAPITOLO 6

## VERIFICHE SULL'ADEGUATEZZA DEL MODELLO

Oltre all'attività di vigilanza che l'OdV svolge continuamente sull'effettività del Modello (e che si concreta nella verifica della coerenza tra i comportamenti concreti dei Destinatari e il Modello stesso), questo periodicamente effettua specifiche verifiche sulla reale capacità del Modello alla prevenzione dei Reati, coadiuvandosi con soggetti terzi in grado di assicurare una valutazione obiettiva dell'attività svolta.

Tale attività si concretizza in una verifica a campione dei principali atti societari e dei contratti di maggior rilevanza conclusi o negoziati da CAA in relazione alle Attività Sensibili e alla conformità degli stessi alle regole di cui al presente Modello.

Inoltre, viene svolta una *review* di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dall'OdV, degli eventi considerati rischiosi e della consapevolezza dei Dipendenti e degli Organi Sociali rispetto alla problematica della responsabilità penale dell'impresa con verifiche a campione.

Per le verifiche l'OdV si avvale, di norma, anche del supporto di quelle funzioni interne che, di volta in volta, si rendano a tal fine necessarie.

Le verifiche e il loro esito sono oggetto di *report* annuale al Consiglio di Amministrazione. In particolare, in caso di esito negativo, l'OdV esporrà, nel piano relativo all'anno, i miglioramenti da attuare.

# PARTI SPECIALI

**PARTE SPECIALE – A –**

**Reati nei rapporti con la Pubblica Amministrazione e induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria**

## CAPITOLO A.1

## Criteri per la definizione di pubblica amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio

I reati di cui alla presente Parte Speciale trovano tutti come presupposto l'instaurazione di rapporti con la P.A. (comprendendo in tale definizione anche la P.A. di Stati esteri).

Si indicano pertanto qui di seguito alcuni criteri generali per la definizione di "Pubblica Amministrazione", "Pubblici Ufficiali" e "Incaricati di Pubblico Servizio".

### A.1.1 Enti della Pubblica Amministrazione

Agli effetti della legge penale, viene comunemente considerato come "Ente della Pubblica Amministrazione" qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.

A titolo esemplificativo, si possono indicare quali soggetti della Pubblica Amministrazione, i seguenti Enti o categorie di Enti:

- enti e amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e Senato, Agenzia delle Entrate, Magistratura ordinaria e amministrativa);
- Regioni e Comuni;
- Società municipalizzate;
- Autorità di Vigilanza (quali ad esempio Banca d'Italia, Consob, AGCM, IVASS);
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, ISTAT, ENASARCO);
- ASL e ATS;
- ANAC;
- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano un pubblico servizio (ad esempio, Cassa Depositi e Prestiti, Ferrovie dello Stato);
- Fondazioni di previdenza e assistenza.

Fermo restando la natura puramente esemplificativa di tale elenco, si evidenzia come non tutte le persone fisiche che agiscono nella sfera e in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie di Reati nei rapporti con la P.A.

In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei "Pubblici Ufficiali" e degli "Incaricati di Pubblico Servizio".

**A.1.2 Pubblici Ufficiali**

L'art. 357 c.p. definisce **pubblici ufficiali** "*coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa*", precisando che "*è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi*".

Il codice penale prevede quindi 3 tipi di pubbliche funzioni: legislativa, giudiziaria e amministrativa.

Le prime due (legislativa e giudiziaria) non sono definite espressamente dall'art. 357 c.p. perché presentano caratteristiche tipiche che consentono una loro immediata individuazione; infatti:

- la funzione legislativa è l'attività svolta dagli organi pubblici (Parlamento, Regioni e Governo) che, secondo la Costituzione italiana, hanno il potere di emanare atti aventi valore di legge;
- la funzione giudiziaria è l'attività svolta dagli organi giudiziari (civili, penali e amministrativi) e dai loro ausiliari (cancelliere, segretario, perito, interprete, ecc.), per l'applicazione della legge al caso concreto.

La funzione amministrativa, così come definita dal comma secondo dell'art. 357 è un'attività che si caratterizza per il fatto di essere disciplinata da norme di diritto pubblico o da atti autoritativi della P.A. (e ciò la differenzia dalle attività di natura privatistica che sono disciplinate da strumenti di diritto privato, quali il contratto) e per la circostanza di essere accompagnata dalla titolarità di almeno uno dei seguenti tre poteri:

- potere di formare e manifestare la volontà della P.A. (ad esempio: sindaco o assessore di un comune, componenti di commissioni di gare di appalto, dirigenti di aziende pubbliche, ecc.);

- potere autoritativo, che comporta l'esercizio di potestà attraverso le quali si esplica il rapporto di supremazia della P.A. nei confronti dei privati cittadini (ad esempio, gli appartenenti alle forze dell'ordine, i componenti delle commissioni di collaudo di lavori eseguiti per un ente pubblico, i funzionari degli organismi di vigilanza – Banca d'Italia e Consob – ecc.);
- potere certificativo, vale a dire potere di redigere documentazione alla quale l'ordinamento giuridico attribuisce efficacia probatoria privilegiata (ad esempio notai).

Per fornire infine un contributo pratico alla risoluzione di eventuali "casi dubbi", può essere utile ricordare che assumono la qualifica di pubblici ufficiali non solo i soggetti al vertice politico-amministrativo dello Stato o di enti territoriali, ma anche tutti coloro che, in base allo statuto, nonché alle deleghe che esso consenta, ne formino legittimamente la volontà e/o la portino all'esterno in forza di un potere di rappresentanza.

Si segnala, altresì, come la Corte di cassazione abbia spiegato che, ai fini della determinazione della qualifica di "pubblico ufficiale" sia sempre necessario valutare le "specifiche mansioni svolte" dal soggetto: laddove queste siano "funzioni prettamente pubblicistiche", tale qualifica può dirsi integrata (Cass. pen., Sez. V, 28 giugno 2017, n. 31676, fattispecie in cui la Suprema Corte ha ritenuto qualificabile come pubblico ufficiale il *project manager* di una società partecipata da un ente pubblico).

### A.1.3 Incaricati di un pubblico servizio

La definizione della categoria di "soggetti incaricati di un pubblico servizio" si rinviene all'art. 358 c.p. a norma del quale, "*sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio.*

*Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale*".

Il legislatore puntualizza la nozione di "pubblico servizio" attraverso due ordini di criteri, uno positivo ed uno negativo. Il servizio, affinché possa definirsi pubblico, deve essere disciplinato, del pari alla "pubblica funzione", da norme di diritto pubblico, ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

Esempi di incaricati di pubblico servizio sono: i dipendenti delle autorità di vigilanza che non concorrono a formare la volontà dell'autorità e che non hanno poteri autoritativi, i

dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati, gli impiegati degli uffici pubblici, ecc.

## CAPITOLO A.2

## Le fattispecie dei reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/2001)

La presente Parte Speciale si riferisce ai reati realizzabili nell'ambito dei rapporti tra la Società e la P.A. Si descrivono brevemente qui di seguito le singole fattispecie contemplate nel D.Lgs. 231/2001 agli artt. 24 e 25 che appaiono astrattamente rilevanti in relazione all'attività svolta dalla Società.

### A.2.1 Reati di tipo corruttivo

***CORRUZIONE PER L'ESERCIZIO DELLA FUNZIONE E AMBITO APPLICATIVO (ARTT. 318, 320 E 321 C.P.)***

L'ipotesi di reato di cui all'art. 318 c.p. si configura nel caso in cui un pubblico ufficiale, per esercitare le proprie funzioni o i propri poteri riceve indebitamente, per sé o per un terzo, denaro o altra utilità, non dovuti o ne accetta la promessa.

Il legislatore, con la l. 6 novembre 2012, n. 190, ha eliminato ogni riferimento a un atto di ufficio già compiuto o da compiere.

La norma punisce sia la compravendita di singoli atti di ufficio, precedentemente riconducibili alla fattispecie di corruzione impropria, sia la cosiddetta corruzione per asservimento, ossia la messa a libro paga del pubblico agente, svincolata dal riferimento a uno specifico atto. In quest'ultima ipotesi il pubblico amministratore non si limita a fare mercimonio di un singolo atto d'ufficio, ma concede al privato la sua generale disponibilità in vista del conseguimento di una serie indeterminata di risultati vantaggiosi (si pensi ad esempio al caso in cui, un funzionario IVASS, a fronte della promessa di un Esponente Aziendale, circa l'assunzione o l'attribuzione di una consulenza fittizia ad un suo familiare, garantisca per un periodo prolungato l'ottenimento di una serie di autorizzazioni).

Ai sensi dell'art. 320 c.p. le disposizioni di cui all'art. 318 c.p. si applicano anche alla persona incaricata di un pubblico servizio, qualora rivesta la qualità di pubblico impiegato: in tali casi, tuttavia, le pene previste dal legislatore sono ridotte fino ad un terzo rispetto alle fattispecie delittuose che vedono coinvolto un pubblico ufficiale.

***CORRUZIONE PER UN ATTO CONTRARIO AI DOVERI DI UFFICIO, CIRCOSTANZE AGGRAVANTI E AMBITO APPLICATIVO (ARTT. 319, 319-BIS, 320 E 321 C.P.)***

L'ipotesi di reato di cui all'art. 319 c.p. si configura nel caso in cui il pubblico ufficiale, per compiere un atto contrario ai suoi doveri di ufficio o per omettere o ritardare un atto del suo ufficio riceve, per sé o per un terzo, denaro o altra utilità, non dovuta o ne accetta la promessa (si pensi ad esempio ad ipotesi corruttive nei confronti dei funzionari IVASS da parte di Esponenti Aziendali o a mezzo di Consulenti per impedire la comminazione di sanzioni pecuniarie).

Ai fini della configurabilità di tale reato in relazione al compimento di un atto contrario ai doveri di ufficio vanno considerati sia gli atti illegittimi o illeciti (vietati, cioè, da norme imperative o contrastanti con norme dettate per la loro validità ed efficacia) sia quegli atti che, pur formalmente regolari, siano stati posti in essere dal pubblico ufficiale violando il dovere d'imparzialità o asservendo la sua funzione ad interessi privati o comunque estranei a quelli proprio della Pubblica Amministrazione.

Per questa fattispecie di reato la pena può essere aumentata ai sensi dell'art. 319-*bis* c.p. qualora l'atto contrario ai doveri di ufficio abbia ad oggetto il conferimento di pubblici impieghi, stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene, nonché il pagamento o il rimborso di tributi.

Ai sensi dell'art. 320 c.p., le disposizioni dell'art. 319 c.p. si applicano anche all'incaricato di un pubblico servizio: in tali casi, tuttavia, le pene previste dal legislatore sono ridotte fino ad un terzo rispetto alle fattispecie delittuose che vedono coinvolto un pubblico ufficiale.

*****

Ai sensi dell'art. 321 c.p. le pene previste dagli artt. 318 e 319 c.p. si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il danaro o altra utilità.

Si sottolinea infine come le ipotesi di reato di cui agli artt. 318 e 319 c.p. si differenzino dalla concussione in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

***CORRUZIONE IN ATTI GIUDIZIARI (ART. 319-TER C.P.)***

Tale ipotesi di reato si configura nel caso in cui, per favorire o danneggiare una parte in un procedimento giudiziario (penale, civile o amministrativo), si corrompa un pubblico ufficiale, e dunque un magistrato, un cancelliere o altro funzionario dell'Autorità giudiziaria

(si pensi ad esempio al caso in cui un Esponente Aziendale della Società faccia indebite "pressioni" su un Pubblico Ministero per ottenere una richiesta di archiviazione di un procedimento penale).

È importante sottolineare come il reato possa configurarsi a carico di una società indipendentemente dal fatto che la stessa sia parte del procedimento.

Se dalla commissione della fattispecie criminosa deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è aumentata.

***INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ (ART. 319-QUATER)***

La presente fattispecie di reato è stata introdotta dalla legge 6 novembre 2012, n. 190, scorporando l'induzione alla corruzione rispetto alla concussione.

Tale ipotesi di reato si configura qualora il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induca taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità. Sono previste pene diverse per il pubblico ufficiale o incaricato di pubblico servizio che induce il privato a dare o promettere utilità e quelle per il privato cittadino che asseconda tale richiesta.

Il legislatore del 2012 ha esteso la punibilità anche al privato che subisce l'attività induttiva, a cui è riservato un regime sanzionatorio più mite rispetto a quello previsto per il pubblico funzionario.

La pena è aumentata quando il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000.

***ISTIGAZIONE ALLA CORRUZIONE (ART. 322 C.P.)***

Tale ipotesi di reato si configura nel caso in cui venga offerto o promesso danaro o altra utilità non dovuti ad un pubblico ufficiale o incaricato di pubblico servizio (per indurlo a compiere le proprie funzioni o esercitare i propri poteri ovvero a omettere o ritardare un atto di sua competenza o compiere un atto contrario ai suoi doveri di ufficio) e tale offerta o promessa non venga accettata.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la pena prevista per la fattispecie di cui all'art. 318 c.p., ridotta di un terzo, qualora l'offerta o la promessa sia fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad esercitare le proprie funzioni; qualora invece l'offerta o la promessa sia fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o ritardare un atto

del suo ufficio, o a compiere un atto contrario ai propri doveri d'ufficio la pena è quella prevista per la fattispecie di cui all'art. 319 c.p., ridotta di un terzo.

***PECULATO, INDEBITA DESTINAZIONE DI DENARO O COSE MOBILI, CONCUSSIONE, INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ, CORRUZIONE E ISTIGAZIONE ALLA CORRUZIONE, ABUSO D'UFFICIO DI MEMBRI DELLE CORTI INTERNAZIONALI O DEGLI ORGANI DELLE COMUNITÀ EUROPEE O DI ASSEMBLEE PARLAMENTARI INTERNAZIONALI O DI ORGANIZZAZIONI INTERNAZIONALI E DI FUNZIONARI DELLE COMUNITÀ EUROPEE E DI STATI ESTERI (ART. 322-BIS C.P.)***

Sulla base del richiamo all'art. 322-*bis* operato dall'art. 25 del Decreto, le fattispecie di reato previste dagli articoli 314, 314-*bis*, 316, da 317 a 320, 322, terzo e quarto comma, c.p. . si configurano anche nel caso in cui il denaro o altra utilità siano dati, offerti o promessi, anche a seguito di induzione a farlo:

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

2. a 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. a 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. a membri e ad addetti di 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;

5-*bis*. ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri e agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale;

5-*ter*. alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali;

5-*quater*. ai membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e ai giudici e funzionari delle corti internazionali;

5-*quinquies*. alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di Stati non appartenenti all'Unione europea, quando il fatto offende gli interessi finanziari dell'Unione.

Le disposizioni degli articoli 319-*quater*, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità sono dati, offerti o promessi:

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

b) alle 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.

***TRAFFICO DI INFLUENZE ILLECITE (ART. 346-BIS C.P.)***

La norma in parola prevede la punizione di chiunque, all'infuori dei casi di concorso nei reati di cui agli artt. 318, 319 e 319-*ter*, e nei reati di corruzione di cui all'art. 322-*bis* c.p., utilizzando intenzionalmente allo scopo relazioni esistenti con un pubblico ufficiale o con un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'art. 322-*bis* c.p., indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità economica, come prezzo per remunerare un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'art. 322-*bis* c.p., in relazione all'esercizio delle sue funzioni, ovvero per realizzare un'altra mediazione illecita.

Parimenti, è punito chi indebitamente dà o promette denaro o altra utilità.

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

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

È prevista la diminuzione della pena nel caso i fatti siano di particolare tenuità.

*****

Con riferimento alle fattispecie di reato di cui al presente paragrafo A.2.1, profili di rischio in capo alla Società si individuano essenzialmente nelle ipotesi in cui gli Esponenti Aziendali e/o i Consulenti della stessa agiscano quali corruttori nei confronti di pubblici ufficiali o incaricati di pubblico servizio.

Per quanto riguarda invece la cosiddetta corruzione passiva, la Società non potrebbe commettere il reato in proprio in quanto essa è sprovvista della necessaria qualifica pubblicistica; potrebbe tuttavia concorrere in un reato di corruzione commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, nel caso in cui fornisse un qualsiasi di sostegno, materiale o morale ai sensi dell'art. 110 c.p., al pubblico funzionario per la commissione del reato. A tal riguardo, si precisa che sussiste l'ipotesi del concorso nel reato di corruzione, anche quando si agisca quale mediatore tra il privato e il pubblico funzionario.

### A.2.2 La concussione, il peculato e l'indebita destinazione di denaro o cose mobili

***CONCUSSIONE (ART. 317 C.P.)***

L'art. 317 c.p., come modificato dalla legge 6 novembre 2012, n. 190 e dalla legge 27 maggio 2015, n. 69, punisce il pubblico ufficiale o l'incaricato di un pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Nella formulazione codicistica antecedente alla modifica apportata dalla legge 27 maggio 2015, n. 69, la fattispecie in esame prevedeva quale soggetto attivo solo il pubblico ufficiale. Il legislatore con tale ultima modifica ha riesteso la soggettività attiva del reato anche all'incaricato di pubblico servizio.

La concussione, al pari della corruzione, prevede una condotta bilaterale, ovverosia da parte del concussore e del concusso.

Tuttavia, a differenza della corruzione, solo il concussore è assoggettato a pena (reclusione da sei a dodici anni), in quanto il concusso è la vittima del reato.

***PECULATO (ART. 314, COMMA 1, E ART. 316 C.P.)***

Il reato è commesso dal pubblico ufficiale o dall'incaricato di pubblico servizio che si appropria di denaro o di beni mobili altrui di cui abbia per ragione di servizio il possesso o la disponibilità, oppure che riceve o trattiene indebitamente per sé o per terzi denaro o altra utilità, percepiti approfittando dell'errore altrui.
Tali condotte comportano la responsabilità amministrativa ai sensi del D. Lgs. n. 231/2001 solo se i fatti offendano gli interessi finanziari dell'Unione europea.

Si tratta di illeciti contestabili in situazioni in cui non ricorrano gli elementi di altri reati, quali ad esempio quello di truffa ai danni dell'Unione europea.

***INDEBITA DESTINAZIONE DI DENARO O COSE MOBILI (ART. 314-BIS C.P.)***

Fuori dai casi previsti dall'art. 314 c.p., il pubblico ufficiale o l'incaricato di pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, li destina ad un uso diverso da quello previsto da specifiche disposizioni di legge o da atti aventi forza di legge dai quali non residuano margini di discrezionalità e intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale o ad altri un danno ingiusto, è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da sei mesi a quattro anni quando il fatto offende gli interessi finanziari dell'Unione europea e l'ingiusto vantaggio patrimoniale o il danno ingiusto sono superiori ad euro 100.000.

Tale fattispecie di reato rileva ai fini del D.Lgs. 231/2001 quando il fatto offende gli interessi finanziari dell'Unione europea.

****

Per la natura privatistica dell'attività svolta dalla Società, i suoi esponenti non potrebbero commettere in proprio i reati di concussione, peculato e indebita destinazione di denaro o cose mobili in quanto sprovvisti della necessaria qualifica pubblicistica; i medesimi potrebbero tutt'al più concorrere nei reati commessi da un pubblico ufficiale o da un incaricato di pubblico servizio ai sensi dell'art. 110 c.p. o rispondere di diversa ipotesi delittuosa (qualora, ad esempio, la condotta del Pubblico Ufficiale o dell'incaricato di pubblico servizio si sostanzi in un'induzione indebita a dare o premettere denaro o altra utilità, prevista e punita dall'art. 319-*quater* c.p.).

Inoltre, è astrattamente possibile che un dipendente della Società rivesta, al di fuori dell'attività lavorativa, una pubblica funzione o svolga un pubblico servizio: si pensi al dipendente della Società che svolga l'incarico di componente di una giunta comunale. In tale ipotesi, questi, nello svolgimento del proprio ufficio o servizio, dovrà astenersi dal tenere comportamenti che, in violazione dei propri doveri d'ufficio e/o con abuso delle proprie funzioni, siano idonei a recare un vantaggio alla Società.

### A.2.3 Le ipotesi di truffa

***TRUFFA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (ART. 640, COMMA 2, N. 1 C.P.)***

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere artifizi o raggiri (intendendosi inclusa in tale definizione anche l'eventuale omissione di informazioni che, se conosciute, avrebbero certamente determinato in senso negativo, o comunque diversamente, la volontà dello Stato, di altro ente pubblico o dell'Unione europea) tali da indurre in errore e da arrecare un danno (di tipo patrimoniale) a tali enti.

Si pensi, in particolare, alla trasmissione all'amministrazione finanziaria di documentazione contenente false informazioni al fine di ottenere un rimborso fiscale non dovuto; ovvero, più in generale, all'invio ad enti previdenziali o amministrazioni locali di comunicazioni contenenti dati falsi in vista di un qualsiasi vantaggio o agevolazione per la Società.

Si pensi, ancora, alla falsa prospettazione dolosa di determinati vantaggi a seguito della sottoscrizione di uno strumento finanziario che già *ex ante* non possiede tali caratteristiche vantaggiose.

***TRUFFA AGGRAVATA PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE (ART. 640-BIS C.P.)***

Il reato in oggetto si perfeziona allorquando i fatti di cui al precedente art. 640 c.p. riguardano l'ottenimento di contributi, sovvenzioni, finanziamenti o altre erogazioni concesse dallo Stato, da altri enti pubblici o dell'Unione europea.

Si pensi ad esempio alle ipotesi di indebito ottenimento di un finanziamento pubblico finalizzato al sostegno delle attività imprenditoriali in determinati settori, mediante la produzione di falsa documentazione attestante la sussistenza dei requisiti per l'ottenimento del finanziamento.

***FRODE INFORMATICA (ART. 640-TER C.P.)***

Si configura il reato di frode informatica quando, procurando a sé o ad altri un ingiusto profitto con altrui danno, venga alterato in qualsiasi modo il funzionamento di un sistema informatico, o si intervenga, senza diritto, su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti.

Ad esempio, integra il reato la modificazione delle informazioni relative alla situazione contabile di un rapporto contrattuale in essere con un ente pubblico, ovvero l'alterazione dei dati fiscali e/o previdenziali contenuti in una banca dati facente capo alla P.A.

Sono previsti aggravi di pena se il fatto è commesso con abuso della qualità di operatore del sistema, se ricorre una delle circostanze di cui all'art. 640, comma 2 c.p. o se il fatto è

commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti nonché se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale.

***FRODE NELLE PUBBLICHE FORNITURE (ART. 356 C.P.)***

Commette il reato chiunque nell'esecuzione di contratti di fornitura con lo Stato, con un altro ente pubblico o con un'impresa esercente servizi pubblici o di pubblica necessità non adempia ai propri obblighi indicati nell'art. 355 c.p., facendo ricorso ad artifici o raggiri tali da ingannare la controparte sul contenuto della propria prestazione, facendo mancare in tutto o in parte cose o opere necessarie a uno stabilimento pubblico o a un servizio pubblico.

### A.2.4 Le ipotesi di malversazione e di indebita percezione di erogazioni

***MALVERSAZIONE DI EROGAZIONI PUBBLICHE (ART. 316-BIS C.P.)***

Tale ipotesi di reati su configura nei confronti di chiunque, avendo ottenuto dallo Stato, da altro ente pubblico o dall'Unione europea contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, destinati alla realizzazione di una o più finalità non li destina alle finalità previste.

Per l'integrazione del reato è sufficiente che anche solo una parte delle attribuzioni ricevute sia stata impiegata per scopi diversi da quelli previsti, non rilevando, in alcun modo, che l'attività programmata sia stata comunque svolta. Risultano altresì irrilevanti le finalità che l'autore del reato abbia voluto perseguire, poiché l'elemento soggettivo del reato medesimo è costituito dalla volontà di sottrarre risorse destinate ad uno scopo prefissato.

Tipico esempio è rappresentato dall'ottenimento di un finanziamento pubblico erogato in vista dell'assunzione presso la società di personale appartenente a categorie privilegiate successivamente disattesa.

***INDEBITA PERCEZIONE DI EROGAZIONI PUBBLICHE (ART. 316-TER C.P.)***

Tale ipotesi di reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere ovvero mediante l'omissione di informazioni dovute – si ottengano, senza averne diritto, contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominati, concessi o erogati dallo Stato da altri enti o dall'Unione europea.

In questo caso, contrariamente a quanto visto in merito al reato precedente, a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

La pena è aumentata se il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000.
Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie di cui all'art. 640-*bis* c.p. (truffa aggravata per il conseguimento di erogazioni pubbliche), nel senso che si configura solo nei casi in cui la condotta non integri gli estremi del reato di cui a quest'ultima disposizione.

*****

Per ciò che concerne i reati di cui agli artt. 316-*bis,* 316-*ter* e 640-*bis* c.p., si precisa che i contributi e le sovvenzioni sono attribuzioni pecuniarie a fondo perduto che possono avere carattere periodico o *una tantum,* in misura fissa o determinata in base a parametri variabili, natura vincolata all'*an* o al *quantum* o di pura discrezionalità; i finanziamenti sono atti negoziali caratterizzati dall'obbligo di destinazione delle somme o di restituzione o da ulteriori e diversi oneri; i mutui agevolati sono erogazioni di somme di denaro con obbligo di restituzione per il medesimo importo, ma con interessi in misura minore a quelli praticati sul mercato.

*****

### *INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 377-*BIS *C.P.)*

La Legge 3 agosto 2009, n. 116 ha introdotto nel D.Lgs. 231/2001 l'art. 25-*decies* per il reato di "induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" come previsto all'art. 377-*bis* c.p.
Ai sensi di tale ultimo articolo, salvo che il fatto costituisca più grave reato, chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere.

## CAPITOLO A.3

### Attività Sensibili nei rapporti con la P.A.

Di seguito sono elencate le attività già esposte nella Parte Generale del presente Modello e che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati di cui al D.Lgs. 231/2001:

1) *Rapporti con la Pubblica Amministrazione: trattasi di rapporti con le Autorità di Vigilanza (IVASS, Consap, Garante Privacy e Autorità Garante della Concorrenza e del Mercato), l'amministrazione finanziaria (Agenzia delle Entrate e Guardia di Finanza), gli enti previdenziali e assistenziali (Ministero del Lavoro delle Politiche Sociali, Inps e Inail) e i soggetti pubblici per gli aspetti che riguardano la sicurezza e l'igiene sul lavoro ex D.Lgs. 81/2008 (Ministero della Salute e delle Politiche Sociali e ASL)* che la Società intrattiene attraverso:

   - *Corrispondenza scritta:* tale corrispondenza può avvenire con frequenza periodica o occasionalmente, per effetto di richiesta espressa della Pubblica Amministrazione o della Compagnia medesima;
   - *Incontri con la Pubblica Amministrazione:* trattasi di rapporti diretti con Pubblici Ufficiali.

2) *Rapporti contrattuali con la P.A. o con soggetti incaricati di un pubblico servizio*

   - *Negoziazione, stipulazione ed esecuzione di contratti/convenzioni con soggetti pubblici mediante procedure negoziate (affidamento o trattativa privata)*: si tratta dell'attività di negoziazione/stipulazione/esecuzione di Polizze e/o convenzioni con Enti Pubblici (Ente sottoscrittore e beneficiario / Ente sottoscrittore e beneficiari i dipendenti), Polizze con dipendenti o rappresentanti di Enti Pubblici quando tale loro ruolo sia noto (nell'ambito di un rapporto privatistico - "privati sensibili"), Polizze fidejussorie a soggetti privati in favore di Enti Pubblici.

3) *Richieste e gestione di fondi pubblici erogati alla Compagnia*

   - *Ottenimento da parte dello Stato, da altro ente pubblico o dall'Unione Europea di contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominati e gestione degli stessi*: l'attività – qualora venisse compiuta – si presenterebbe a rischio sia nel momento della formulazione della richiesta (in relazione all'eventuale presentazione di documenti o informazioni non corrispondenti al vero) sia nella gestione dei fondi eventualmente ricevuti (in

relazione all'eventuale uso di tali fondi per finalità diverse da quelle a cui erano destinati).

4) *Gestione delle ispezioni*

- L'attività consiste nella gestione di tutti i rapporti con i funzionari pubblici in caso di ispezione.

5) *Gestione dei contenziosi*

- L'attività consiste nella gestione di tutte le controversie giudiziali e stragiudiziali con assicurati o altre controparti contrattuali, costituiti in forma societaria. In particolare l'attività si presenta a rischio in considerazione della possibilità che la Società, attraverso un proprio rappresentante, corrompa un Pubblico Ufficiale o Incaricato di pubblico servizio al fine di ottenere un vantaggio nella gestione della lite (ad esempio, rinuncia, transazioni a condizioni particolarmente favorevoli ecc.). L'attività si presenta a rischio anche in considerazione del fatto che, nell'ambito di un procedimento civile, amministrativo o penale che dovesse coinvolgere la Società, questa potrebbe fare pressioni indebite al fine di indurre un soggetto chiamato a testimoniare a rendere false dichiarazioni per favorirla.

6) *Liquidazione dei sinistri relativi a polizze stipulate con gli enti pubblici, pubblici ufficiali e incaricati di pubblico servizio:*

- La rischiosità astratta dell'attività è legata ad eventuali utilizzi distorti dello strumento assicurativo, nella misura in cui tale attività fosse finalizzata a riconoscere un trattamento di maggior favore verso particolari soggetti al fine unico o prevalente di influenzarne l'imparzialità e l'autonomia di giudizio.

**Attività Strumentali alla commissione dei reati di tipo corruttivo**

Alcune attività che non comportano rapporti diretti con la P.A. possono tuttavia essere strumentali alla commissione della tipologia di reati di tipo corruttivo.

Ciò può accadere:

1) quando l'attività costituisce strumento di creazione di disponibilità occulte, da utilizzare per la corruzione di pubblici ufficiali.

   Si pensi ad esempio al caso in cui la Società acquisti beni o servizi da Fornitori o affidi incarichi a Consulenti, pagando somme superiori al valore effettivo della prestazione,

con l'accordo che il fornitore/collaboratore restituirà parte del prezzo pagato attraverso modalità non regolari.

2) quando l'attività costituisce il mezzo per corrispondere, direttamente o per interposta persona, ai funzionari pubblici, in forma occulta o indiretta, denaro o altra utilità in cambio di interessamenti indebiti.

Si indicano di seguito alcune tipologie di attività che possono comportare rischi nel senso sopra indicato:

- *Selezione, assunzione e gestione del personale*: si pensi, ad esempio, alla prospettata assunzione di un familiare del pubblico funzionario (o, in futuro, dello stesso pubblico funzionario) presso la Società, in vista del compimento di atti in suo favore. L'attività può inoltre presentare profili di rischio nell'ipotesi in cui siano riconosciute a un eventuale congiunto di un pubblico funzionario, dipendente della Società, privilegi o vantaggi professionali indebiti o non dovuti e collegati all'interessamento del pubblico funzionario medesimo in una pratica relativa alla Società;

- *Selezione di Consulenti, Fornitori e* Partner *e gestione dei rapporti con gli stessi*:

a. L'attribuzione di consulenze, di forniture o altri incarichi, può essere strumentalizzata sotto un duplice profilo:

  - può essere utilizzata quale forma di retribuzione di prestazioni indebite erogate da pubblici funzionari; si pensi alla stipulazione di un contratto di consulenza a favore di un familiare di un pubblico funzionario, quale corrispettivo dell'interessamento da parte del medesimo in una pratica relativa alla Società;

  - possono essere preferiti nella selezione coloro che si prestano a corrompere, in nome e per conto della Società, Pubblici Ufficiali o Incaricati di Pubblico Servizio.

- *Gestione degli omaggi e delle sponsorizzazioni ed effettuazione di altri atti di liberalità e correntezza:* la gestione delle prestazioni gratuite erogate in qualsiasi forma dalla Società a titolo di omaggio a favore della clientela o di terzi (omaggi in occasione di ricorrenze; pranzi e viaggi; servizi di qualsiasi natura ecc.) si presenta a rischio, in quanto possibile forma di corresponsione di utilità non dovute a pubblici funzionari o soggetti ad essi collegati; si pensi all'invio ad un pubblico funzionario, in occasione della conclusione di un contratto o delle festività natalizie, di un omaggio quale

corrispettivo all'interessamento di detto funzionario nella pratica relativa alla Società. Come sopra evidenziato, qualsiasi prestazione gratuita erogata dalla Società a favore della clientela presenta profili di rischio in relazione alle fattispecie corruttive; in particolare, mentre gli atti di correntezza possono essere motivati da considerazioni di ordine tecnico, quelli di liberalità potrebbero essere mossi da valutazioni di opportunità commerciale e/o aziendale;

- *Gestione della contabilità e dei flussi finanziari:* nell'ambito della gestione della contabilità e dei flussi finanziari potrebbero essere realizzate operazioni volte a costituire fondi neri da utilizzare per corrompere Pubblici Ufficiali o Incaricati di Pubblico Servizio. Il corruttore, infatti, per porre in essere la condotta corruttiva deve poter disporre di risorse finanziarie adeguate, attingendo quindi dal patrimonio aziendale. Un adeguato sistema di controlli sui flussi finanziari della Società consente di prevenire il rischio di formazione di provviste potenzialmente utili a porre in essere condotte corruttive.

- *Definizione delle politiche di remunerazione e incentivazione*: gli amministratori e i *manager* che sono intenzionati a porre in essere condotte corruttive potrebbero ricorrere a risorse economiche apparentemente non societarie, ma proprie. Un tipico esempio di risorse finanziarie non societarie utilizzate per corrompere soggetti terzi sono i *bonus* e le remunerazioni riconosciute dall'azienda: la corresponsione di remunerazioni particolarmente elevate agli amministratori e ai manager potrebbe, infatti, nascondere la "provvista" necessaria a questi ultimi per porre in essere condotte corruttive concordate a livello aziendale.

- *Gestione dei rimborsi spese*: una modalità di utilizzo di risorse proprie per porre in essere condotte corruttive consiste nel sostenere personalmente le spese, salvo poi chiederne il relativo rimborso. È da ritenersi infatti responsabile per il reato in oggetto anche la società che dovesse consentire o agevolare il rimborso di spese effettuate personalmente da amministratori e *manager* per porre in essere condotte corruttive.

Eventuali modifiche o integrazioni delle suddette Attività Sensibili sono rimesse alla competenza dell'Amministratore Delegato e sottoposte annualmente al Consiglio di Amministrazione che potrà procedere con la successiva attività di ratifica secondo quanto indicato nella Parte Generale del Modello.

## CAPITOLO A.4

### Principi generali di comportamento

I seguenti principi di carattere generale si applicano ai Destinatari.

In via generale, è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate; sono altresì proibite le violazioni ai principi e alle procedure aziendali previste nella presente Parte Speciale.

In particolare:

a) è fatto divieto di accordare vantaggi di qualsiasi natura (denaro, promesse di assunzione, ecc.) in favore di rappresentanti della P.A. italiana o straniera, o a loro familiari, rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale o che possa comunque influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda;

b) è fatto divieto di distribuire omaggi al di fuori di quanto previsto dalle *policy* aziendali (vale a dire ogni forma di omaggio offerto eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di omaggio a rappresentanti della P.A. o a loro familiari che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore e, pertanto, non potranno essere superiori a Euro 150 annuali per singolo destinatario, salvo deroghe approvate per iscritto (a livello generale per categorie di omaggi o in modo specifico per singoli omaggi) dall'Amministratore Delegato con l'indicazione della motivazione sottesa al compimento dell'atto di liberalità;

c) è vietato eseguire erogazioni liberali, sponsorizzazioni, atti di correntezza e donazioni in favore di enti pubblici o soggetti incaricati di un pubblico servizio in difformità a quanto previsto dalle apposite procedure interne (emanate sulla base del principio procedurale di cui al successivo paragrafo A.5.1, punto 8) e dalle regole aziendali al riguardo dagli Organi Sociali;

d) è vietato assecondare o sottostare ad eventuali richieste, da parte di pubblici ufficiali o di soggetti terzi, di accordare vantaggi di qualsiasi natura (beni, denaro o qualsiasi altra

utilità) a favore di pubblici ufficiali italiani o stranieri per l'esercizio di attività pubbliche. Ove venissero formulate richieste di tal genere, deve essere immediatamente informato il Responsabile Area *Compliance*, il quale, valutata la riconducibilità della richiesta ad uno dei Reati di cui alla presente Parte Speciale, né dà avviso all'OdV e al Consiglio di Amministrazione;

e) è fatto divieto di accettare qualsiasi tipo di regalo d'affari e/o di vantaggio che possa compromettere l'indipendenza, l'imparzialità e l'integrità dei dipendenti (o dei componenti degli Organi Sociali) della Società. A questo fine, la Società ha fissato un importo pari a Euro 150 quale limite massimo di valore per gli omaggi ricevuti sia da clienti sia da Fornitori sia da terzi in genere. Tale limite si intende su base annua;

f) è vietato effettuare prestazioni in favore dei Consulenti e dei *Partner* che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi, nonché riconoscere compensi in favore medesimi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti nel settore;

g) è vietato emettere dichiarazioni o rilasciare alla pubblica amministrazione dati, documenti o informazioni non corrispondenti al vero al fine di ottenere contributi, sovvenzioni, finanziamento mutui agevolati o altre forme di erogazione, comunque denominate, dallo Stato o da una pubblica amministrazione italiana o europea;

h) è vietato utilizzare contributi, sovvenzioni, finanziamenti, mutui agevolati o altre forme di erogazioni dello stesso tipo, comunque denominate, ottenute dallo Stato o da una pubblica amministrazione italiana o europea per scopi diversi da quelli a cui i medesimi sono destinati;

i) per i contratti di assicurazione contro i danni, è vietato ricevere denaro contante a titolo di pagamento di premi di importo superiore a Euro 750,00 annui (Euro settecentocinquanta) per ciascun contratto; il limite di incasso di premi in contanti per il ramo r.c. auto è invece quello stabilito *ex lege* dal D.Lgs. 21 novembre 2007, n. 231.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, codici di comportamento, *policy* e procedure aziendali.

Tali *policy* e procedure e loro eventuali successive integrazioni o modifiche si considerano parte integrante del Modello e, pertanto, si devono intendere come recepite nella loro configurazione.

## CAPITOLO A.5

## Principi procedurali specifici

### A.5.1 Principi procedurali specifici generalmente applicabili

Ai fini dell'attuazione dei principi e regole generali e dei divieti elencati al precedente cap. A.4, devono rispettarsi gli specifici principi procedurali qui di seguito descritti, oltre alle regole e principi generali contenuti nella Parte Generale del Modello. Le regole qui di seguito descritte, devono essere rispettate sia nell'esplicazione dell'attività di CAA in territorio italiano, sia eventualmente all'estero.

### A.5.2. Principi procedurali specifici relativi alle Attività Sensibili

In relazione alle Attività Sensibili individuate nel precedente Capitolo A.3 la Società pone in essere i seguenti principi procedurali specifici:

1. *Rapporti con la Pubblica Amministrazione (Autorità di Vigilanza, amministrazione finanziaria, Agenzia delle Entrate, enti previdenziali e assistenziali e soggetti pubblici per gli aspetti che riguardano la sicurezza e l'igiene sul lavoro ex D. Lgs. 81/2008)*

    a. Ai Dipendenti, Organi Sociali, Rete Distributiva, dipendenti di CA Vita per i servizi prestati a CAA, Consulenti, Fornitori e *Partner* che materialmente intrattengono rapporti con la P.A. per conto di CAA deve essere formalmente conferito potere in tal senso dalla stessa Società (con apposita delega per i Dipendenti e gli Organi Sociali ovvero nel relativo mandato, contratto di consulenza o di *partnership* per gli altri soggetti indicati). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta che rispetti tutti i criteri previsti nel Capitolo 2.5.1.2 della Parte Generale del presente Modello.

    b. La Società garantisce, attraverso procedure interne di protocollazione della corrispondenza e strumenti informatici messi direttamente a disposizione da parte della pubblica autorità, la tracciabilità di tutte le comunicazioni intercorse per iscritto tra la Società e la Pubblica Amministrazione, nonché di tutti i flussi informativi e statistici trasmessi alla medesima.

    c. Tutte le comunicazioni scritte trasmesse alla Pubblica Amministrazione sono condivise tra più funzioni.

    d. Tutta la corrispondenza con la Pubblica Amministrazione viene conservata e archiviata in formato cartaceo ed elettronico.

2. *Rapporti contrattuali con la P.A. o con soggetti incaricati di un pubblico servizio*

   a. Le operazioni di negoziazione/stipulazione/esecuzione di contratti/convenzioni con soggetti pubblici o incaricati di un pubblico servizio e, in generale tutti i rapporti con la Pubblica Amministrazione, devono avere debita evidenza e uniformità di gestione, essendo queste considerate, alla luce del Modello, come Attività Sensibili.

   b. In particolare, i Responsabili delle Funzioni aziendali che sono coinvolte nello svolgimento delle operazioni sensibili di cui sopra devono:

      - comunicare – attraverso la redazione di *report* informativi – all'Organismo di Vigilanza qualunque anomalia o criticità riscontrata nel corso dello svolgimento dell'attività nell'ambito della funzione di competenza;

      - verificare la concreta ed efficace attuazione – nell'ambito delle Direzioni e/o funzioni di competenza – delle procedure aziendali relative all'attività in oggetto e dei principi di cui al presente Modello di organizzazione, gestione e controllo;

      - prevedere misure idonee a garantire la regolarità delle richieste di informazioni avanzate dalla Società nei confronti degli uffici competenti della Pubblica Amministrazione, ovvero delle richieste avanzate nei confronti di CAA da esponenti della Pubblica Amministrazione;

      - assicurare la correttezza e veridicità dei documenti e delle informazioni fornite dalla Società nei confronti della Pubblica Amministrazione o di altro Ente Pubblico;

      - documentare in modo idoneo, su supporto cartaceo o informatico, i principali adempimenti eseguiti dalla funzione aziendale preposta nel corso delle relazioni o dei contatti diretti con la Pubblica Amministrazione o con altro Ente pubblico.

   c. La Società effettua verifiche a campione al fine di accertare che eventuali deroghe alle condizioni generali di assicurazione non siano finalizzate a garantire trattamenti di favore a Enti Pubblici, Pubblici Ufficiali o Incaricati di Pubblico Servizio.

3. *Richiesta e gestione di fondi pubblici erogati alla Compagnia*

   a. L'ottenimento di fondi pubblici deve essere basato su principi di correttezza e trasparenza: in caso di richiesta di fondi pubblici la Compagnia adotta specifici presidi procedurali e operativi, nonché sistemi di controllo volti ad assicurare la correttezza delle informazioni, dei dati e dei documenti trasmessi alla Pubblica

Amministrazione erogante, nonché sistemi di controllo volti ad assicurare la tracciabilità delle operazioni poste in essere nell'impiego dei fondi ottenuti.

b. Al fine di porre in essere i principi di cui sopra la Società individua all'interno della propria organizzazione aziendale i soggetti responsabili del monitoraggio di tali attività.

4. *Gestione delle ispezioni*

a. La Società garantisce che i rapporti con funzionari pubblici in caso di ispezione vengano gestiti nel rispetto dei principi stabiliti all'interno di apposita procedura interna.

b. Alle ispezioni o verifiche condotte da pubbliche autorità (ad esempio relative al D.Lgs. 81/08, verifiche tributarie, INPS, IVASS, ecc.) devono partecipare almeno due soggetti a ciò espressamente delegati.

c. Nel corso dell'attività ispettiva, deve essere prestata, da parte delle funzioni coinvolte nei processi aziendali ispezionati, la massima collaborazione all'espletamento degli accertamenti da parte dei funzionari pubblici. In particolare, devono essere messi a disposizione con tempestività e completezza i documenti che gli incaricati ritengano necessario acquisire, previo il consenso del responsabile incaricato di volta in volta di interloquire con l'autorità.

d. Dell'ispezione o verifica devono essere conservati tutti i documenti e il verbale predisposto dall'Autorità all'esito dell'attività ispettiva.

e. Nel caso di richiesta, nell'ambito di un'ispezione/accertamento da parte della P.A. (comprese le Autorità di Vigilanza), di interviste/colloqui con specifici soggetti all'interno della Compagnia ovvero con terzi che operano in favore della stessa, questi ultimi dovranno attenersi alle regole previste nella presente Parte Speciale e dalle procedure interne.

L'OdV dovrà essere prontamente informato in merito ad ogni attività ispettiva nei confronti della Società da parte della P.A. (dalla fase di avvio alla fase conclusiva dell'ispezione). All'OdV, pertanto, deve essere trasmessa e consentito l'accesso alla documentazione prodotta dall'Autorità ispezionante e dalla Società, fino alla conclusione dell'ispezione (ivi compresi i verbali relativi all'ispezione, che devono, in ogni caso, essere archiviati dalla funzione a ciò preposta).

5. *Gestione dei contenziosi*

a. Nella gestione del contenzioso giudiziale e stragiudiziale la Società adotta specifiche procedure aziendali volte a stabilire:

   - i ruoli e le responsabilità dei soggetti incaricati di gestire il contenzioso medesimo;
   - i criteri per definire le controversie in sede giudiziale o stragiudiziale;
   - le modalità di gestione delle stesse nei rapporti con i difensori e le controparti.

b. Nella gestione del contenzioso giudiziale o arbitrale la Società affida il mandato alle liti a difensori, selezionati sulla base delle procedure in vigore e che si impegnino contrattualmente a non porre in essere alcun tipo di condotta, direttamente o indirettamente, idonea, anche solo in via strumentale, a configurare un reato di quelli ricompresi nella presente Parte Speciale, a pena di revoca del mandato stesso.

c. Nella gestione del contenzioso stragiudiziale, la negoziazione di accordi transattivi o conciliativi viene seguita da almeno due soggetti e viene mantenuta traccia di ogni fase della stessa.

d. La Società tiene traccia dei contenziosi pendenti e dei mandati conferiti ai difensori.

6. *Liquidazione dei sinistri relativi a polizze stipulate con gli enti pubblici, pubblici ufficiali e incaricati di pubblico servizio*

   a. La liquidazione dei sinistri deve essere eseguita nel rispetto delle procedure aziendali che ne regolano l'*iter* e che garantiscono parità di trattamento tra tutti gli assicurati.

   b. In relazione alla liquidazione dei sinistri, la Società deve prevedere:

      - l'individuazione dei soggetti incaricati a raccogliere le richieste di liquidazione dei sinistri, a gestire le pratiche stesse, ad autorizzare e ad effettuare i pagamenti, garantendo il rispetto del principio di separazione dei ruoli;
      - l'adozione di strumenti informatici che prevedono il calcolo automatico degli importi da rimborsare e liquidare, assicurando quindi oggettività nella determinazione di tali importi e parità di trattamento tra tutti i soggetti destinatari dei pagamenti in oggetto;
      - la tracciabilità di tutti i flussi informativi intercorrenti tra i soggetti coinvolti nella gestione dei sinistri, nonché della corrispondenza intercorrente con gli assicurati.

### A.5.3. Principi procedurali specifici relativi alle Attività Strumentali alla commissione di reati contro la Pubblica Amministrazione

Al fine di presidiare le Attività Sensibili e limitare il rischio di commissione di reati contro la Pubblica Amministrazione la Società adotta nell'ambito delle Attività Strumentali i seguenti principi procedurali specifici.

1. *Selezione, assunzione e gestione del personale*

a. La Società adotta procedure di selezione, assunzione e gestione del personale dipendente di qualsiasi livello e di collaboratori a progetto che garantiscono (anche nel caso in cui tali attività siano in parte affidate a società di *head hunting*):

   - parità di accesso a tutti i candidati;
   - modalità di scelta basate su criteri di meritocrazia, professionalità e onorabilità dei candidati.

b. La Società conserva la documentazione esibita in sede di assunzione anche al fine di consentirne la consultazione da parte dell'OdV nell'espletamento della consueta attività di vigilanza e controllo.

c. La Società accerta che il candidato o suo familiare non ricoprano cariche nell'ambito della P.A. ovvero non le abbiano ricoperte nel periodo precedente presso Autorità che esercitano poteri autoritativi e/o negoziali nei confronti della Società;

d. La Società mette a disposizione dei neoassunti copia del Modello 231, del Codice Etico, della Carta Etica e Codice di Condotta, con la richiesta di prenderne visione e di impegnarsi al rispetto dei principi contenuti negli stessi.

e. La Società prevede contrattualmente che il datore di lavoro somministrante accerti la sussistenza dei requisiti di onorabilità dei propri dipendenti, consentendo alla Società di risolvere con effetto immediato il contratto di somministrazione di attività lavorativa qualora il dipendente somministrato risultasse indagato o condannato per reati di cui al D.Lgs. 231/2001.

f. La Società consente l'effettuazione di segnalazioni di candidature da parte di Dipendenti (cosiddetto "*referral*") nel rispetto di apposito regolamento interno e delle procedure di selezione e assunzione del personale.

g. Il processo di inserimento della risorsa all'interno della Società deve avvenire nel rispetto degli obblighi di formazione e aggiornamento previsti dalle procedure aziendali in base al ruolo e all'attività svolta all'interno dell'azienda.

h. Eventuali avanzamenti interni di carriera e riconoscimenti di premi (ivi compresa l'eventuale previsione, nel trattamento retributivo, di una componente variabile legata al raggiungimento di specifici obiettivi) devono essere assegnati secondo criteri oggettivi basati sulla parità di trattamento, sulla valorizzazione del merito e della professionalità nonché sul rispetto della normativa aziendale.

2. *Selezione di Consulenti, Fornitori e* Partner *e gestione dei rapporti con gli stessi*

a. La Società verifica l'attendibilità commerciale e professionale dei Fornitori, *Partner* e dei Consulenti.

b. La Società adotta procedure o policy aziendali volte a garantire che il processo di selezione dei Fornitori, dei Partner e del Consulenti avvenga nel rispetto dei criteri di trasparenza, pari opportunità di accesso, professionalità, affidabilità ed economicità, fermo restando la prevalenza dei requisiti di legalità rispetto a tutti gli altri.

c. La Società tiene traccia dei Consulenti, Fornitori, *Partner* e altre controparti con i quali siano già intercorsi rapporti contrattuali.

d. La Società si impegna, in occasione di ogni rinnovo contrattuale con Fornitori, *Partner* e Consulenti, a richiedere la sottoscrizione da parte di questi ultimi di un'autodichiarazione circa la persistenza dei requisiti di onorabilità che in fase di selezione iniziale hanno permesso l'instaurazione del rapporto.

e. I rapporti tra CAA e i Consulenti, i Fornitori e i *Partner* devono essere definiti per iscritto in tutte le loro condizioni e termini e rispettare quanto indicato ai successivi punti.

f. I contratti con i Consulenti, i Fornitori e i *Partner* devono contenere (anche in caso di rinnovo) una clausola standard (cosiddetta "**Clausola 231**"), con cui questi ultimi:

- dichiarino di conoscere la disciplina di cui al Decreto 231 e le sue implicazioni in termini di adempimenti e responsabilità;
- si impegnino al rispetto delle disposizioni in esso contenute e dichiarino di non essere mai stati coinvolti in procedimenti giudiziari relativi ai reati contemplati nella suddetta normativa;

- dichiarino di essere a conoscenza (avendone presa visione) del contenuto del Codice Etico e del Modello della Società ed – eventualmente – di aver adottato a loro volta un codice etico e un modello di organizzazione, gestione e controllo;
- si impegnino a rispettare il contenuto del Codice Etico e del Modello della Società.

g. In conformità con le indicazioni fornite a livello di Gruppo, i contratti con i Consulenti, i Fornitori e i *Partner* prevedono, inoltre, il rispetto da parte dei medesimi di normative nazionali e/o internazionali applicabili e rilevanti.

h. A integrazione dei principi sopra esposti, nel caso di instaurazione di rapporti continuativi con controparti contrattuali, la Società si impegna ad attuare efficacemente controlli periodici circa

- la persistenza in capo a questi ultimi dei requisiti che in fase di selezione iniziale hanno permesso l'instaurazione del rapporto;
- l'effettiva prestazione della consulenza/fornitura e la congruità del prezzo pattuito.

3. *Gestione degli omaggi e delle sponsorizzazioni ed effettuazione di altri atti di liberalità e correntezza*

a. Fermo restando quanto previsto per gli omaggi aziendali al precedente Paragrafo A.4. le erogazioni liberali effettuate in qualsiasi forma, le sponsorizzazioni e le donazioni in favore di enti pubblici devono essere, indipendentemente dall'importo, deliberate e approvate dall'Amministratore Delegato e deve essere indicata la motivazione sottesa al compimento dell'atto di liberalità, sentito il Responsabile Area *Compliance*.

b. Di tali erogazioni deve essere informato anche l'OdV; se ritenuto opportuno dal manager che ha proposto l'erogazione liberale / donazione / sponsorizzazione, di tale azione può essere informato anche il Comitato Esecutivo (o Comex).

c. Le sponsorizzazioni al pari degli omaggi e regali sono mappate in apposito registro tenuto dall'unita aziendale preposta.

d. L'*iter* da seguire per l'effettuazione di una sponsorizzazione prevede le seguenti fasi: (i) fase di analisi della documentazione; (ii) fase contrattuale (gestita secondo le linee guida aziendali in base all'importo della sponsorizzazione); (iii) controllo dell'utilizzo dei fondi; (iv) tracciabilità delle singole operazioni.

4. *Gestione della contabilità e dei flussi finanziari*

a) La Società adotta procedure specificamente finalizzate a regolare i processi di tenuta della contabilità. In particolare, tale procedura prevede:

- la registrazione a livello informatico di tutte le voci di spesa;
- controlli specifici su: a) la coerenza delle dei pagamenti rispetto ai corrispettivi pattuiti contrattualmente; b) l'avvenuta esecuzione dei delle prestazioni rese da soggetti terzi all'organizzazione aziendale; c) il rispetto del *budget* assegnato a ciascuna funzione per l'esercizio delle attività di propria competenza.

b) La Società adotta sistemi contabili idonei ad assicurare che:

- tutti i flussi finanziari in entrata e in uscita siano adeguatamente identificabili e tracciabili, nonché correttamente e regolarmente registrati in appositi libri e registri contabili;
- tutti i flussi finanziari in entrata e in uscita siano supportati da specifica documentazione giustificatrice, che riporti chiaramente e fedelmente le transazioni a cui fa riferimento;
- sia rispettato il principio di segregazione dei ruoli tra i soggetti che autorizzano, coloro che eseguono e coloro che controllano i flussi finanziari in entrata e in uscita;
- siano rispettati i limiti di spesa assegnati ai soggetti che richiedono l'esecuzione di flussi finanziari in uscita;
- non siano creati conti segreti o scritture non registrate e che non siano effettuati pagamenti per spese inesistenti o elementi di passività il cui oggetto non sia correttamente identificato;
- il denaro contante sia utilizzato solo per pagamenti di piccola cassa e supportati da documentazione idonea a comprovare l'effettivo pagamento.

5. *Definizione delle politiche di Remunerazione e incentivazione*

a. La Società adotta politiche di remunerazione degli amministratori e di incentivazione del *management* e del personale dipendente che siano in linea con gli obiettivi, le strategie economiche, i valori e gli obiettivi di lungo periodo. In particolare, la politica di remunerazione e i piani di incentivazione:

- sono approvati dall'assemblea dei soci e definiti per iscritto in modo chiaro e trasparente;

- prevedono un adeguato equilibrio tra componenti fisse e componenti variabili;
- prevedono che le componenti variabili degli incentivi e delle remunerazioni siano limitate a determinati importi e siano subordinate al raggiungimento di risultati predeterminati e quantitativamente / qualitativamente misurabili;
- evitano che i sistemi premianti dei soggetti con poteri di spesa o facoltà decisionali a rilevanza esterna siano basati su *target* di *performance* sostanzialmente irraggiungibili;
- includono una revisione delle competenze etiche aziendali nella valutazione e nella promozione di dirigenti e funzionari, misurando il raggiungimento degli obiettivi non soltanto rispetto al conseguimento di *target* finanziari ma anche rispetto alle modalità con cui tali obiettivi sono stati conseguiti e in particolare alla conformità dei comportamenti tenuti rispetto alla presente Parte Speciale e alla normativa aziendale;
- prevedono un aggiornamento periodico per assicurare che le remunerazioni e i piani di incentivazione siano adeguati ai mutamenti aziendali intervenuti;
- prevedono sistemi di controllo finalizzati a verificare la coerenza delle remunerazioni e delle incentivazioni riconosciute agli amministratori, ai dirigenti e ai dipendenti rispetto alla politica e ai piani aziendali, nonché l'effettivo raggiungimento degli obiettivi prestabiliti.

b. La definizione degli obiettivi assegnati a tutte le figure disciplinate dal Regolamento Ivass 38/2018 è effettuata in accordo con i Direttori delle Aree *Compliance* e *Risk Management* e Controlli Permanenti.

6. *Gestione dei rimborsi spese*

a. La Società garantisce la previsione di specifici limiti e modalità per il rimborso di spese anticipate da esponenti aziendali e dipendenti;

b. l'utilizzo di carte di credito aziendali o carte prepagate è consentito solo a soggetti specificamente individuati dal vertice aziendale;

c. tutte le spese di viaggio e di rappresentanza sostenute dal personale e dai Fornitori/Consulenti della Società devono essere comprovate da idonea documentazione e giustificate da stretta attinenza all'attività lavorativa;

d. il rimborso delle spese sostenute avviene con modalità tracciabili.

## CAPITOLO A.6

## I controlli dell'OdV e flussi informativi

### A.6.1 Il controllo in generale

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui agli artt. 24, 25 e 25-*decies* del Decreto, commessi nell'interesse o a vantaggio della Società anche tramite la rete distributiva del Gruppo, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

I compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati di cui agli artt. 24, 25 e 25-*decies* del Decreto sono i seguenti:

i. proporre che vengano costantemente aggiornate le procedure aziendali per prevenire la commissione dei reati nei rapporti con la Pubblica Amministrazione, di cui alla presente Parte Speciale; con riferimento a tale punto l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio di commissione dei suddetti reati, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere; o proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Attività Sensibili individuate nella presente Parte Speciale;

ii. monitoraggio sul rispetto delle procedure interne per la prevenzione dei reati oggetto della presente Parte Speciale. Sulla base dei flussi informativi ricevuti l'Organismo di Vigilanza condurrà verifiche mirate su determinate operazioni effettuate nell'ambito delle Attività Sensibili, volte ad accertare da un lato il rispetto di quanto stabilito nel Modello e nei protocolli, dall'altro l'effettiva adeguatezza delle prescrizioni in essi contenute a prevenire i reati potenzialmente commissibili;

iii. esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute. L'Organismo di Vigilanza,

inoltre, è tenuto alla conservazione dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti.

A tal fine, all'OdV viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Per i flussi informativi si rimanda, in particolare, alla compilazione da parte delle funzioni competenti delle "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento) che costituiscono un allegato al Modello.

**PARTE SPECIALE – B –**

**Reati Societari**

## CAPITOLO B.1

## Le fattispecie dei reati societari (art. 25-*ter* del D.Lgs. 231/2001)

Si provvede qui di seguito a fornire una breve descrizione dei reati contemplati dall'art. 25-*ter* del Decreto che assumono rilevanza in relazione all'attività della Società (di seguito i "Reati Societari").

Si rende noto che i reati di cui agli artt. 2635 e 2635-*bis* c.c. ( corruzione tra privati e istigazione alla corruzione tra privati), indicati anch'essi all'art. 25-*ter* del Decreto, sono trattati nella Parte Speciale L – Corruzione tra privati.

### B.1.1 Le ipotesi di falsità

***FALSE COMUNICAZIONI SOCIALI (ART. 2621 C.C.)***

L'ipotesi di reato di cui all'art. 2621 c.c. si configura nel caso in cui, consapevolmente, "*al fine di conseguire per sé o per altri un ingiusto profitto, vengano esposti nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali rilevanti non rispondenti al vero, ovvero vengano omesse 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*".

Soggetti attivi di tali reati sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori.

Si precisa che:

- ai sensi dell'art. 2621-*bis* c.c., la pena può essere ridotta se i fatti di cui alla disposizione citata siano di lieve entità o se riguardino società che non superino i limiti indicati dall'art. 1, comma 2, del regio decreto del 16 marzo 1942 n. 267;
- ai sensi dell'art. 2621-*ter*, la condotta non è punibile se il fatto sia di particolare tenuità.

***FALSE O OMESSE DICHIARAZIONI PER IL RILASCIO DEL CERTIFICATO PRELIMINARE (ART. 54 D.LGS. 19/2023)***

La norma punisce chiunque, al fine di far apparire adempiute le condizioni per il rilascio del certificato preliminare di cui all'art. 29 del D.Lgs. 19/2023 (ovverosia, il certificato attraverso il quale l'autorità preposta – per quanto riguarda lo Stato italiano, il notaio – verifica e attesta il rispetto dei requisiti di legalità per la realizzazione dell'operazione

transfrontaliera), forma documenti in tutto o in parte falsi, altera documenti veri, rende dichiarazioni false oppure omette informazioni rilevanti.

### B.1.2 La tutela del capitale sociale

***INDEBITA RESTITUZIONE DEI CONFERIMENTI (ART. 2626 C.C.)***

Il reato in questione, come quello previsto dal successivo art. 2627 c.c., riguarda la tutela dell'integrità del capitale sociale e si compie quando gli amministratori, in assenza di legittime ipotesi di riduzione del capitale sociale, provvedono a restituire, anche per equivalente, i conferimenti effettuati dai soci ovvero liberano i soci dall'obbligo di eseguirli. Il reato in esame assume rilievo solo quando, per effetto degli atti compiuti dagli amministratori, si intacca il capitale sociale e non i fondi o le riserve. Per questi ultimi, eventualmente, sarà applicabile il reato contemplato dal successivo art. 2627 c.c.

La restituzione dei conferimenti può essere palese (quando gli amministratori restituiscono beni ai soci senza incasso di alcun corrispettivo o rilasciano dichiarazioni dirette a liberare i soci dai loro obblighi di versamento) ovvero, più probabilmente, simulata (quando per realizzare il loro scopo gli amministratori utilizzano stratagemmi o artifici quali, per esempio, la distribuzione di utili fittizi con somme prelevate dal capitale sociale e non dalle riserve, oppure la compensazione del credito vantato dalla società con crediti inesistenti vantati da uno o più soci).

Soggetti attivi del reato possono essere solo gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della restituzione o della liberazione, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

***ILLEGALE RIPARTIZIONE DEGLI UTILI E DELLE RISERVE (ART. 2627 C.C.)***

Tale ipotesi di reato consiste nella ripartizione di utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, ovvero nella ripartizione di riserve (anche non costituite con utili) che non possono per legge essere distribuite.

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

Soggetti attivi del reato sono gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della ripartizione degli utili o delle riserve, escludendo il concorso

necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

***ILLECITE OPERAZIONI SULLE AZIONI O QUOTE SOCIALI O DELLA SOCIETÀ CONTROLLANTE (ART. 2628 C.C.)***

Tale ipotesi di reato consiste nel procedere – fuori dai casi consentiti dalla legge – all'acquisto o alla sottoscrizione di azioni o quote emesse dalla società (o dalla società controllante) che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

La norma è diretta alla tutela dell'effettività e integrità del capitale sociale e non può prescindere dall'analisi di cui all'art. 2357 c.c. il quale prevede che la società per azioni non può acquistare azioni proprie, nemmeno tramite società fiduciaria o interposta persona, se non nei limiti degli utili distribuibili o delle riserve disponibili risultanti dall'ultimo bilancio regolarmente approvato. La norma prevede che le azioni debbano essere interamente liberate.

Tra le fattispecie tramite le quali può essere realizzato l'illecito vanno annoverate non solo le ipotesi di semplice acquisto ma anche quelle di trasferimento della proprietà delle azioni, per esempio, mediante permuta o contratti di riporto, o anche quelle di trasferimento senza corrispettivo, quale la donazione.

Soggetti attivi del reato sono gli amministratori. Inoltre, è configurabile una responsabilità a titolo di concorso degli amministratori della controllante con quelli della controllata, nell'ipotesi in cui le operazioni illecite sulle azioni della controllante medesima siano effettuate da questi ultimi su istigazione dei primi.

***OPERAZIONI IN PREGIUDIZIO DEI CREDITORI (ART. 2629 C.C.)***

Tale ipotesi di reato consiste nell'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o di scissioni, tali da cagionare danno ai creditori.

Si fa presente che:

- il risarcimento del danno ai creditori prima del giudizio estingue il reato.
- Il reato è punibile a querela di parte.

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

***FORMAZIONE FITTIZIA DEL CAPITALE (ART. 2632 C.C.)***

Tale ipotesi di reato è integrata dalle seguenti condotte:

- formazione o aumento in modo fittizio del capitale sociale, anche in parte, mediante attribuzione di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale;
- sottoscrizione reciproca di azioni o quote;
- sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori e i soci conferenti.

**B.1.3 La tutela del corretto funzionamento della società**

***IMPEDITO CONTROLLO (ART. 2625 C.C.)***

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

L'illecito può essere commesso esclusivamente dagli amministratori.

**B.1.4 La tutela penale contro le frodi**

***AGGIOTAGGIO (ART. 2637 C.C.)***

Tale ipotesi di reato consiste nel diffondere notizie false ovvero nel realizzare operazioni simulate o altri artifici, concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero nell'incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari.

È prevista una circostanza aggravante nel caso in cui il fatto sia commesso mediante l'impiego di sistemi di intelligenza artificiale.

Si pensi ad esempio al caso in cui vengano diffuse dalla Società degli studi su società non quotate con previsioni di dati e suggerimenti esagerati e/o falsi.

Anche questo è un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

### B.1.5 La tutela delle funzioni di vigilanza

***OSTACOLO ALL'ESERCIZIO DELLE FUNZIONI DELLE AUTORITÀ PUBBLICHE DI VIGILANZA (ART. 2638 C.C.)***

Si tratta di un'ipotesi di reato che può essere realizzata con due condotte distinte:

- la prima (i) attraverso l'esposizione nelle comunicazioni previste dalla legge alle Autorità pubbliche di Vigilanza, quali Consob, Banca d'Italia o IVASS, (al fine di ostacolare l'esercizio delle funzioni di queste ultime) di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero (ii) mediante l'occultamento, con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati e concernenti la medesima situazione economica, patrimoniale o finanziaria.

  La responsabilità sussiste anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;

- la seconda si realizza con il semplice ostacolo all'esercizio delle funzioni di vigilanza svolte da parte di pubbliche autorità, attuato consapevolmente e in qualsiasi forma, anche omettendo le comunicazioni dovute alle autorità medesime.

Soggetti attivi del reato sono gli amministratori, i direttori generali, i sindaci e i liquidatori.

## CAPITOLO B.2

### Attività Sensibili nell'ambito dei reati societari

Di seguito sono elencate le attività già esposte nella Parte Generale del presente Modello che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati societari di cui all'art. 25-*ter* del D.Lgs. 231/2001, ritenuti astrattamente rilevanti[2]:

a) **Predisposizione delle comunicazioni alle Autorità di Vigilanza e gestione dei rapporti con le stesse**: trattasi dei rapporti con le Autorità di Vigilanza in merito agli adempimenti previsti in tema di comunicazioni dei dati societari.

b) **Predisposizione delle comunicazioni relative alla situazione economica, patrimoniale e finanziaria della Società previste dalla legge e dirette ai soci o al pubblico**: trattasi di informazioni relative ai bilanci e relazioni riguardanti la situazione economica, patrimoniale e finanziaria della Società o del gruppo al quale essa appartiene.

c) **Tenuta della contabilità, predisposizione di bilanci, relazioni, comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori per legge e/o per disposizioni di Autorità di Vigilanza:** trattasi di contabilità in genere e bilanci, relazione semestrale, situazioni trimestrali, relazioni e prospetti allegati al bilancio e qualsiasi altro dato o prospetto richiesto da Autorità di vigilanza; ci si riferisce, altresì, ai rapporti con le Autorità di vigilanza in merito agli adempimenti previsti in tema di comunicazioni dei dati societari.

d) **Gestione dei rapporti con il Collegio Sindacale, società di revisione e altri organi Sociali, nonché redazione, tenuta e conservazione dei documenti su cui gli stessi potrebbero esercitare il controllo.**

e) **Operazioni relative al capitale e operazioni sulle azioni:** trattasi degli adempimenti legislativi legati alla gestione delle attività in oggetto al fine di salvaguardare il patrimonio della società (operazioni su azioni; acconti su dividendi; conferimenti, fusioni e scissioni; distribuzione utili).

[2] Per le Attività Sensibili individuate in relazione alle fattispecie di corruzione tra privati si rimanda alla Parte Speciale L.

f) **Comunicazioni di interessi da parte degli amministratori della Società:** trattasi delle comunicazione cui sono tenuti tutti gli amministratori in occasione di una delibera per la quale hanno un particolare interesse, per conto proprio o di terzi.

## CAPITOLO B.3

## Regole e principi generali

### B.3.1 Principi generali di comportamento

Obiettivo della presente Parte Speciale è che i Dipendenti, gli Organi Sociali, i Consulenti e i soggetti dipendenti della Società CA Vita per i servizi prestati a CAA, si attengano – nei limiti delle rispettive competenze e nella misura in cui siano coinvolti nello svolgimento delle attività nelle Attività Sensibili individuate in precedenza – a regole di condotta conformi a quanto prescritto in tale Parte Speciale e nelle *policy* e procedure cui la stessa fa riferimento diretto o indiretto, al fine di prevenire la commissione dei Reati Societari.

In particolare, gli Esponenti Aziendali, da un lato, e i Consulenti e i soggetti dipendenti della Società CA Vita, dall'altro, nei limiti delle pattuizioni contrattuali, in relazione al tipo di rapporto in essere con la Società, dovranno attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati Societari;
2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, al fine di fornire ai soci e al pubblico in generale una informazione veritiera e appropriata sulla situazione economica, patrimoniale e finanziaria della Società.

   In ordine a tale punto, è fatto divieto di:

   (i) predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società;

   (ii) omettere di comunicare dati e informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;

(iii) non attenersi ai principi e alle prescrizioni contenute nelle istruzioni predisposte o applicate dalla Società per la redazione dei bilanci;

(iv) osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale e agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere al riguardo.

In ordine a tale ultimo punto, è fatto divieto di:

(i) restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;

(ii) ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve (anche non costituite con utili) che non possono per legge essere distribuite;

(iii) acquistare o sottoscrivere azioni della Società o dell'eventuale società controllante fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge;

(iv) effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;

(v) procedere in ogni modo a formazione o aumento fittizi del capitale sociale;

(vi) ripartire i beni sociali tra i soci – in fase di liquidazione – prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli;

5. assicurare il regolare funzionamento della Società e degli organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare.

In ordine a tale punto, è fatto divieto di:

(i) tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale o della società di revisione o dei soci;

(ii) porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;

(iii) astenersi dal dare notizia al Consiglio di Amministrazione e al Collegio Sindacale da parte di ciascun componente del Consiglio di Amministrazione qualora abbia un interesse, per conto proprio o di terzi, in una determinata operazione;

6. astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false o non corrette (anche mediante l'utilizzo di strumenti di intelligenza artificiale), idonee a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato.

   In ordine a tale punto, è fatto divieto di pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento o ingannatorio suscettibili di determinare riflessi su strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato e idonei ad alterarne sensibilmente il prezzo.

7. effettuare con tempestività, correttezza e completezza tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate.

   In ordine a tale punto, è fatto divieto di:

   (i) omettere di effettuare, con la dovuta chiarezza, completezza e tempestività, nei confronti delle Autorità in questione, (a) tutte le comunicazioni, periodiche e non, previste dalla legge e dalla ulteriore normativa di settore, nonché (b) la trasmissione dei dati e documenti previsti dalle norme in vigore e/o specificamente richiesti dalle predette Autorità;

   (ii) esporre in tali comunicazioni e nella documentazione trasmessa fatti non rispondenti al vero oppure occultare fatti concernenti la situazione economica, patrimoniale o finanziaria della Società;

   (iii) porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle Autorità pubbliche di Vigilanza, anche in sede di ispezione (espressa opposizione, rifiuti pretestuosi, comportamenti

ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, codici di comportamento, policy e procedure aziendali.

Tali *policy* e procedure e loro eventuali successive integrazioni o modifiche si considerano parte integrante del Modello e, pertanto, si devono intendere come recepite nella loro configurazione.

## CAPITOLO B.4

### Principi procedurali specifici

Ai fini dell'attuazione dei principi e regole generali e dei divieti elencati al precedente Capitolo B.3, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del Modello, gli specifici principi procedurali qui di seguito descritti.

a. *Predisposizione delle comunicazioni alle Autorità di Vigilanza e gestione dei rapporti con le stesse*

Con riferimento alle attività soggette alla vigilanza di Pubbliche Autorità, in base alle specifiche normative applicabili, al fine di prevenire la commissione dei reati di false comunicazioni alle Autorità e di ostacolo alle funzioni di vigilanza, le attività soggette a vigilanza devono essere svolte in base alle procedure aziendali esistenti, contenenti la disciplina delle modalità e l'attribuzione di specifiche responsabilità in relazione:

- ai flussi informativi periodici alle autorità previste da leggi e regolamenti;
- alla trasmissione a queste ultime dei documenti previsti in leggi e regolamenti (ad esempio, la relazione sui reclami, bilanci e verbali delle riunioni degli Organi Sociali);
- alla trasmissione di dati e documenti specificamente richiesti dalle autorità di vigilanza;
- al comportamento da tenere nel corso degli accertamenti ispettivi.

I principi posti a fondamento di tali procedure sono:

- attuazione di tutti gli interventi di natura organizzativa necessari ad estrarre i dati e le informazioni per la corretta compilazione delle segnalazioni e il loro puntuale invio all'autorità di vigilanza e/o alla pubblica amministrazione, nonché per una corretta formalizzazione e conservazione delle stesse, secondo le modalità e i tempi stabiliti dalla normativa applicabile;
- nel corso dell'attività ispettiva, deve essere prestata, da parte delle funzioni coinvolte nei processi aziendali ispezionati, la massima collaborazione all'espletamento degli accertamenti da parte dei funzionari pubblici. In particolare, devono essere messi a disposizione con tempestività e completezza i documenti che gli incaricati ritengano necessario acquisire, previo il consenso del responsabile incaricato di volta in volta di interloquire con l'autorità;

- i rapporti con funzionari pubblici in caso di ispezione vengano gestiti nel rispetto dei principi stabiliti all'interno di apposita procedura interna.

Nel caso di richiesta, nell'ambito di un'ispezione/accertamento da parte di Autorità di Vigilanza, di interviste/colloqui con specifici soggetti all'interno della Compagnia ovvero con terzi che operano in favore della stessa, anche questi ultimi dovranno attenersi alle regole previste nella presente Parte Speciale e dalle procedure interne.

L'OdV dovrà essere prontamente informato in merito ad ogni attività ispettiva nei confronti della Compagnia da parte di Autorità di Vigilanza (dalla fase di avvio alla fase conclusiva dell'ispezione). All'OdV, pertanto, deve essere trasmessa e consentito l'accesso alla documentazione prodotta dall'Autorità ispezionante e dalla Compagnia, fino alla conclusione dell'ispezione (ivi compresi i verbali relativi all'ispezione che devono, in ogni caso, essere archiviati dalla funzione a ciò preposta).

*b.* *Predisposizione delle comunicazioni relative alla situazione economica, patrimoniale e finanziaria della società previste dalla legge e dirette ai soci o al pubblico*

Nella predisposizione dei suddetti documenti devono essere rispettati i seguenti principi:

- determinare con chiarezza e completezza i dati e le notizie che ciascuna funzione deve fornire, i criteri contabili per l'elaborazione dei dati e la tempistica per la loro consegna alle funzioni responsabili;
- prevedere la trasmissione di dati e informazioni alla funzione responsabile attraverso un sistema (anche in via telematica) che consenta la tracciatura dei singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- prevedere – anche per il tramite della società di revisione esterna – controlli di merito indipendenti sulle poste di bilancio maggiormente critiche;
- prevedere controlli periodici e di scostamento dei dati contabili con quelli di budget, lasciando evidenza documentale dei controlli effettuati;
- monitorare i rischi di alterazione delle scritture contabili da parte dei soggetti che partecipano al processo di alimentazione della contabilità generale/gestionale.

Prima della presentazione e approvazione del progetto di bilancio occorre seguire alcune regole finalizzate alla diffusione del documento, che possono così riepilogarsi:

- tempestiva messa a disposizione di tutti i componenti del Consiglio di Amministrazione e del Collegio Sindacale della bozza del bilancio/situazione infrannuale e documentazione collegata, prima della riunione del Consiglio di Amministrazione per l'approvazione del bilancio, attraverso una piattaforma informatica, che consente la tracciabilità degli accessi e della presa visione dei documenti;

- adeguata giustificazione, documentazione e archiviazione di eventuali modifiche apportate alla bozza di bilancio/situazioni infrannuali da parte degli Amministratori.

c. *Tenuta della contabilità, predisposizione di bilanci, relazioni, comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori per legge e/o per disposizioni di Autorità di Vigilanza*

Nella predisposizione delle scritture contabili la Società adotta i seguenti presidi:

- predisposizione di procedure che regolino l'*iter* di formazione delle scritture contabili coinvolgendo diverse funzioni aziendali;
- implementazione di un adeguato sistema informatico per la tenuta della contabilità attraverso il quale si possa provvedere all'integrazione e al controllo dei dati contabili;
- previsione di controlli di diversi livelli per verificare tutte le poste contabili inserite nei documenti contabili, nelle comunicazioni sociali e nel bilancio d'esercizio.

d. *Gestione dei rapporti con il Collegio Sindacale, società di revisione e altri organi Sociali, nonché redazione, tenuta e conservazione dei documenti su cui gli stessi potrebbero esercitare il controllo*

Nell'ambito dell'Attività Sensibile in oggetto, per quel che concerne i rapporti tra CAA e la società di revisione contabile sono adottati i seguenti presidi:

- gli incarichi di consulenza, aventi ad oggetto attività diversa dalla revisione contabile, vengono conferiti alla società di revisione, previo controllo del Collegio Sindacale che ne dà atto nei verbali delle proprie riunioni;

- il conferimento a soggetti che siano parte della "rete" o del "*network*" a cui appartiene la società di revisione, di incarichi diversi dalla revisione contabile che appaiono incompatibili con quest'ultima, può avvenire solo qualora tali incarichi no siano suscettibili di pregiudicare l'indipendenza della società di revisione incaricata.

e. *Operazioni relative al capitale sociale e operazioni sulle azioni*

Tutte le operazioni sul capitale sociale, nonché la costituzione di società, l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni devono essere effettuate (anche per quelle fasi di attività affidate a consulenti esterni) nel rispetto della normativa (anche regolamentare) e delle *best practice* in materia di *corporate governance*.

In caso di operazioni transfrontaliere, la Società cura che vengano debitamente rispettate le previsioni di cui all'art. 29 del D.Lgs. 19/2023 in relazione al certificato inerente ai requisiti di legalità per la realizzazione dell'operazione.

*f.* *Comunicazioni di interessi da parte degli amministratori della Società*

Con riferimento agli obblighi degli amministratori sono adottati i seguenti presidi:

- obbligo di comunicare, all'apertura della riunione del Consiglio di Amministrazione agli altri amministratori e al Collegio Sindacale l'eventuale presenza di interessi che – per conto proprio o di terzi – si abbiano in una determinata operazione della società, precisando, ove presente, l'interesse, la natura, l'origine o la portata e dandone atto all'interno del verbale della relativa riunione;
- obbligo di procedere alla richiesta preventiva a tutti i partecipanti ad una riunione di Consiglio di Amministrazione di dichiarare, all'apertura della riunione, l'esistenza di interessi la cui comunicazione sia richiesta a norma dell'art. 2391 c.c.

*Altre regole finalizzate alla prevenzione dei reati societari in genere*

Oltre alle regole di *Corporate Governance* e delle procedure esistenti, si dispone l'attuazione dei seguenti presidi integrativi:

- previsione di periodici incontri tra Collegio Sindacale e OdV per verificare l'osservanza della normativa nell'ambito del Decreto 231, tra cui anche la disciplina in tema di normativa societaria e di *corporate governance*;
- messa a disposizione, anche tramite apposita piattaforma, al Collegio Sindacale, con congruo anticipo, di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del Consiglio di Amministrazione o sui quali esso debba esprimere un parere ai sensi di legge;
- trasmissione all'OdV dell'Ordine del Giorno delle riunioni assembleari da parte della funzione *Legale e Affari societari*, successivamente alle stesse, del relativo verbale, nel caso in cui siano all'Ordine del Giorno materie che potrebbero avere un impatto con le Attività Sensibili descritte nella presente Parte Speciale B;

- aggiornamento delle procedure nel rispetto della normativa societaria.

## CAPITOLO B.5

## I controlli dell'OdV e i flussi informativi

### B. 5.1 Il controllo in generale

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di reati societari diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della Società.

Principi procedurali da osservare nelle aree a rischio al fine di attivare le eventuali verifiche, l'Organismo di Vigilanza dovrà avere evidenza e mantenere traccia:

(i) di quanto posto in essere nella Società al fine di fornire opportune indicazioni per la corretta redazione del bilancio;

(ii) dei verbali degli incontri nei quali si dibattono i temi del bilancio tra le funzioni coinvolte). Per quanto attiene agli scambi di informazioni da e verso la società di revisione, l'Organismo di Vigilanza dovrà mantenere agli atti evidenza;

(iii) delle riunioni del Collegio Sindacale, alle quali è invitato a partecipare.

Per quanto concerne il conferimento dell'incarico, l'Organismo di Vigilanza dovrà mantenere agli atti evidenza degli incarichi conferiti.

L'Organismo di Vigilanza dovrà, inoltre, esaminare le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari o opportuni.

Inoltre, i compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati societari sono i seguenti:

(i) proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Parte Speciale;

(ii) monitoraggio sul rispetto delle procedure interne per la prevenzione dei reati societari. L'Organismo di Vigilanza è tenuto alla conservazione delle evidenze dei controlli e delle verifiche eseguiti;

(iii) esaminare eventuali segnalazioni specifiche provenienti dagli Organi Societari, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Per i flussi informativi si rimanda, in particolare, alla compilazione da parte delle funzioni competenti delle "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento) che costituiscono un allegato al Modello.

**PARTE SPECIALE – C –**

**Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio, reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori e reati di finanziamento del terrorismo, reati con finalità di terrorismo o eversione dell'ordine democratico**

## CAPITOLO C.1

La presente Parte Speciale si riferisce ai Reati di riciclaggio di cui all'art. 25-*octies* del D.Lgs. 231/2001, ai reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori di cui all'art. 25-*octies*.1 del D.Lgs. 231/2001 nonché ai Reati con finalità di terrorismo e di eversione dell'ordine democratico di cui all'art. 25-*quater* del D.Lgs. 231/2001 (tra cui anche il reato di finanziamento del terrorismo previsto dall'art. 2 della Convenzione internazionale "*per la repressione del finanziamento del terrorismo*" sottoscritta a New York il 9 dicembre 1999).

Le suddette fattispecie di reato, sebbene tutelino beni giuridici diversi[3], vengono tutte trattate nella presente Parte Speciale poiché:

- sono risultate a rischio nell'ambito delle medesime Attività Sensibili (ad esempio, selezione dei Fornitori e del personale dipendente);
- la commissione delle stesse può essere impedita attraverso l'implementazione dei medesimi presidi (ad esempio, le attività di verifica previste in materia di antiriciclaggio possono essere estese anche nell'ambito delle Attività Sensibili alla commissione di Reati con finalità di terrorismo).

### C.1.1. Le fattispecie dei reati di Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio (Art. 25-*octies*, D.Lgs. 231/2001)

La presente Parte Speciale si riferisce ai Reati di Riciclaggio introdotti nel *corpus* del D.Lgs. 231 del 2001, all'art. 25-*octies*, attraverso il Decreto Legislativo 21 novembre 2007, n. 231 reacante "*Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione*" e successive modifiche e integrazioni (di seguito "**Decreto 231/2007**" o "**Decreto Antiriciclaggio**").

Ai fini della presente Parte Speciale si indicano di seguito i reati previsti dall'art. 25-*octies* del D.Lgs. 231/2001 ("**Reati di Riciclaggio**").

[3] Mentre i reati di ricettazione, riciclaggio e utilizzo di denaro, beni o utilità di provenienza illecita rientrano nella categoria dei "delitti contro il patrimonio mediante frode", i reati con finalità di terrorismo o di eversione dell'ordine democratico rientrano nella categoria dei "delitti contro la personalità internazionale dello Stato", ossia i delitti offensivi della sovranità statale.

***RICETTAZIONE (ART. 648 C.P.)***

Tale ipotesi di reato si configura nel caso in cui un soggetto, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta danaro o cose provenienti da un qualsiasi delitto o contravvenzione, o comunque si intromette nel farli acquistare, ricevere od occultare.

Per "acquisto" si intende l'effetto di un'attività negoziale, a titolo gratuito ed oneroso, mediante la quale l'agente consegua il possesso del bene.

Per "ricezione" si intende ogni forma di conseguimento del possesso de bene proveniente dal delitto, anche se solo temporaneamente.

Per "occultamento" si intende il nascondimento del bene proveniente da delitto dopo averlo ricevuto.

Perché sussista il reato non è necessario che il denaro o i beni debbano provenire direttamente o immediatamente da un qualsiasi reato, ma è sufficiente anche una provenienza mediata, a condizione che l'agente sia consapevole di tale provenienza. Ricorre pertanto il delitto in esame non solo in relazione al prodotto o al profitto del reato, ma anche al denaro o alle cose che costituiscono il prezzo del reato, cioè alle cose acquistate col denaro di provenienza illecita oppure al denaro conseguito dall'alienazione di cose della medesima provenienza (si pensi al caso in cui la Società, al fine di ottenere un prezzo vantaggioso, acquisti beni da un soggetto che, parallelamente alla fornitura di tali beni, notoriamente svolga attività illecite quali lo spaccio di stupefacenti o faccia parte di un'associazione di tipo mafioso e utilizzi i profitti derivanti da tali attività illecite per investirli nell'attività lecita).

***RICICLAGGIO (ART. 648-BIS C.P.)***

Tale ipotesi di reato si configura nel caso in cui un soggetto sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto o contravvenzione, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Per "sostituzione" si intende la condotta consistente nel rimpiazzare il denaro, i beni o le altre utilità di provenienza illecita con valori diversi.

Per "trasferimento" si intende la condotta consistente nel ripulire il denaro, i beni o le altre utilità mediante il compimento di atti negoziali.

Per la realizzazione di tale reato, dunque, è richiesto un *quid pluris* rispetto al reato di ricettazione, ovvero il compimento di atti o fatti diretti alla sostituzione del denaro.

La pena è aumentata quando il fatto è commesso nell'esercizio dell'attività professionale.

***IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA (ART. 648-TER C.P.)***

Tale ipotesi di reato si configura nel caso di impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto o contravvenzione.

La punibilità per tale reato è prevista solo per coloro i quali non siano già compartecipi del reato principale ovvero non siano imputabili a titolo di ricettazione o riciclaggio.

Il termine "impiegare" è normalmente sinonimo di "utilizzo per qualsiasi scopo": tuttavia, considerato che il fine ultimo perseguito dal legislatore consiste nell'impedire il turbamento del sistema economico e dell'equilibrio concorrenziale attraverso l'utilizzo di capitali illeciti reperibili a costi inferiori rispetto a quelli leciti, si ritiene che per "impiegare" debba intendersi in realtà "investire". Pertanto, dovrebbe ritenersi rilevante un utilizzo a fini di profitto.

Premesso che presupposto comune di tutte e tre le fattispecie incriminatrici di cui agli artt. 648, 648-*bis* e 648-*ter* c.p. è quello costituito dalla provenienza da reato del denaro o di quasiasi altra utilità di cui l'agente sia venuto a disporre, si precisa che tali fattispecie si distinguono sotto il profilo soggettivo, per il fatto che la prima di esse richiede, oltre alla consapevolezza della su indicata provenienza, necessaria anche per le altre, solo una generica finalità di profitto, mentre la seconda o la terza richiedono la specifica finalità di far perdere le tracce dell'origine illecita, con l'ulteriore peculiarità, quanto alla terza, che detta finalità deve essere perseguita mediante l'impiego delle risorse in attività economiche o finanziarie.

La pena è aumentata quando il fatto è commesso nell'esercizio dell'attività professionale.

***AUTORICICLAGGIO (ART. 648-TER.1 C.P.)***

L'art. 648-*ter*.1 c.p. punische chi "*avendo commesso o concorso a commettere un delitto, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa*".

È previsto un trattamento sanzionatorio più mite "*quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi*".

È, altresì, prevista una circostanza attenuante se denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni (così determinando una diversificazione della pena a seconda della gravità del reato presupposto commesso).

Tale fattispecie, pertanto, prevede e punisce una condotta tale per cui l'autore, dopo aver commesso o concorso a commettere un reato, impieghi, sostituisca ovvero trasferisca "*in attività economiche, finanziarie, imprenditoriali o speculative*" il provento ricavato da detto reato, con modalità tali da "*ostacolare concretamente l'identificazione della provenienza delittuosa*".

Costituiscono circostanze aggravanti:

- l'aver commesso tale reato con le modalità di cui all'art. 416-*bis* c.p., concernente il reato di "Associazioni di tipo mafioso anche straniere" ovvero al fine di agevolare l'attività delle associazioni di tipo mafioso: in tal caso troveranno, in ogni caso, applicazione le pene previste dal primo comma dell'art. 648-*ter.1* c.p.;
- l'aver commesso tale reato nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale.

Costituisce invece una circostanza attenuante – che comporta la diminuzione della pena fino alla metà – il fatto che il reo "*si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto*".

Non è invece punibile l'autore del Reato di Autoriciclaggio allorquando il denaro, i beni o le altre utilità vengano destinati "*alla mera utilizzazione o al godimento personale*".

* * *

La Legge n. 186/2014 – come anche rilevato da Confindustria con la circolare n. 19867/15 ("*Il reato di autoriciclaggio e la responsabilità* ex *Decreto 231*") – non specifica se la responsabilità dell'ente sia limitata al caso in cui il reato-base dell'autoriciclaggio (ovverosia il "delitto non colposo" il cui provento venga reimpiegato) rientri tra i reati presupposto di cui al Decreto 231 ovvero se essa possa configurarsi anche in presenza di fattispecie diverse.

Un'interpretazione rigorosa della normativa imporrebbe – come sottolineato da Confindustria nella menzionata circolare – di limitare la responsabilità dell'ente al caso in cui il reato-base sia già previsto nel catalogo dei reati presupposto 231 (il rischio di commissione dei quali, peraltro, risulta già presidiato dalle altre Parti Speciali del presente Modello).

Tuttavia, nell'ottica di ridurre – a livello generale – il rischio di commissioni di illeciti nell'ambito dell'attività societaria e al fine di migliorare ad ogni livello la *compliance* aziendale, si è ritenuto di dare rilievo – oltre alla fattispecie di "false comunicazioni sociali", prevista e punita dall'art. 2621 c.c. – anche a fattispecie delittuose (non ricomprese nel catalogo dei reati presupposto), che, in virtù delle condotte sanzionate, risultano *prima facie* a rischio in relazione all'attività assicurativa, ossia taluni reati tributari e il reato di truffa, in particolare, nella forma della cosiddetta truffa contrattuale.

**A) Reati tributari**

In particolare, si è valutato il rischio di commissione dei seguenti reati tributari (i quali non risultano direttamente richiamati dall'art. 25-*quinquiesdecies* del D.Lgs. 231/2001, cui è dedicata la Parte Speciale M del presente Modello):

- omesso versamento di ritenute dovute o certificate;
- omesso versamento di IVA.

**B) Il reato di truffa**

Il reato di truffa si configura ai sensi dell'art. 640 c.p. ogni volta in cui un qualsiasi soggetto, inducendo qualcuno in errore con artifizi o raggiri, procuri per sé o per altri un ingiusto profitto in danno di altri.

Il suddetto reato punisce le condotte aggressive contro il patrimonio personale altrui realizzate attraverso:

- artifizi, ossia attraverso una manipolazione o una trasfigurazione della realtà esterna, provocata mediante la simulazione di fatti o circostanze in realtà inesistenti;
- raggiri, ossia attraverso un'attività simulatrice posta in essere con parole e argomentazioni che fanno scambiare il falso per il vero.

Si tenga conto che le suddette condotte devono essere idonee ad indurre in errore la vittima e pertanto non rilevano ai fini della configurazione del reato in esame artifizi o raggiri grossolani e palesemente non credibili.

In considerazione dell'attività svolta dalla Società, il suddetto reato assume particolare rilevanza nella forma della cosiddetta "*truffa contrattuale*", ossia di quella elaborazione giurisprudenziale del reato di truffa *ex* art. 640 c.p. che è configurabile tutte le volte in cui, nell'ambito di un rapporto contrattuale, uno dei contraenti ponga in essere artifizi o raggiri diretti a tacere o a dissimulare fatti o circostanze tali che, ove conosciuti, avrebbero indotto l'altro contraente ad astenersi dal concludere il contratto.

In tali casi gli artifizi o i raggiri richiesti per la sussistenza del reato possono consistere anche nel silenzio maliziosamente serbato su alcune circostanze da parte di chi abbia il dovere di farle conoscere, indipendentemente dal fatto che dette circostanze potessero essere conoscibili dalla controparte con ordinaria diligenza. Tali fattispecie, pertanto, sono particolarmente diffuse nelle relazioni contrattuali che, essendo connotate da un alto grado di asimmetria informativa, trovano specifica e dettagliata regolamentazione da parte delle Autorità di Vigilanza. Le disposizioni regolamentari, infatti, prevedono in capo ai soggetti vigilati l'obbligo di comportarsi con diligenza e correttezza nell'interesse dei clienti operando in modo che essi siano adeguatamente informati e impongono agli stessi specifici obblighi giuridici di agire in modo tale da assicurare trasparenza ed equo apprezzamento delle condizioni contrattuali.

### C.1.2 Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (Art. 25-*octies.*1, D.Lgs. 231/2001)

***INDEBITO UTILIZZO E FALSIFICAZIONE DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART. 493-TER C.P.)***

L'art. 493-*ter* c.p. punisce la condotta di chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti.

Il primo comma della norma prevede che è, altresì, punito chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

***DETENZIONE E DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A COMMETTERE REATI RIGUARDANTI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART. 493-QUATER C.P.)***

Ai sensi dell'art. 493-*quater* c.p., è punito, salvo che il fatto costituisca più grave reato, chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

***TRASFERIMENTO FRAUDOLENTO DI VALORI (ART. 512-BIS C.P.)***

La fattispecie in oggetto si configura a carico di chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648-*bis* e 648-*ter* c.p.

***FRODE INFORMATICA (ART. 640-TER C.P.)***

Si configura il reato di frode informatica quando, procurando a sé o ad altri un ingiusto profitto con altrui danno, venga alterato in qualsiasi modo il funzionamento di un sistema informatico, o si intervenga, senza diritto, su dati, informazioni o programmi contenuti in un sistema informatico.

Il reato di frode informatica è richiamato dall'art. 25-*octies*.1 con riferimento alla sola ipotesi aggravata di cui al secondo comma dell'art. 640-*ter* c.p. ("*se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema*").

### C.1.3 Delitti con finalità di terrorismo o eversione dell'ordine democratico ("Reati di Terrorismo")

I reati con finalità di terrorismo e di eversione dell'ordine democratico sono stati introdotti nel D.Lgs. 231/2001 (art. 25-*quater*) dalla legge 14 gennaio 2003, n. 7 recante "*Ratifica ed esecuzione della Convenzione internazionale per la repressione del finanziamento del terrorismo, fatta a New York il 9 dicembre 1999, e norme di adeguamento dell'ordinamento interno*".

I reati con finalità di terrorismo e di eversione dell'ordine democratico previsti dall'art. 25-*quater* del D.Lgs. 231/2001 ricomprendono, quindi, fattispecie di reato previste in:

A. codice penale;

B. leggi speciali;

C. Convenzione di New York del 9 dicembre 1999.

Si riportano qui di seguito le fattispecie di reato che sono risultate – anche solo astrattamente – realizzabili nell'ambito delle attività aziendali

**A) Reati con finalità di terrorismo e di eversione dell'ordine democratico previsti nel codice penale**

***ASSOCIAZIONI SOVVERSIVE (ART. 270 C.P.)***

Tale ipotesi di reato è commesso da chiunque nel territorio dello Stato promuova, costituisca, organizzi o diriga associazioni dirette a stabilire violentemente la dittatura di una classe sociale sulle altre, ovvero a sopprimere violentemente una classe sociale o, comunque, a sovvertire violentemente gli ordinamenti economici o sociali costituiti nello Stato ovvero, infine, aventi come scopo la soppressione violenta di ogni ordinamento politico e giuridico della società.

***ASSOCIAZIONE CON FINALITÀ DI TERRORISMO ANCHE INTERNAZIONALE O DI EVERSIONE DELL'ORDINAMENTO DEMOCRATICO (ART. 270-BIS C.P.)***

Tale ipotesi di reato è integrato da chiunque promuova, costituisca, organizzi, diriga o finanzi associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico.

Ai fini della legge penale, la finalità di terrorismo ricorre anche quando gli atti di violenza siano rivolti contro una Stato estero, un'istituzione o un organismo internazionale.

***FINANZIAMENTO DI CONDOTTE CON FINALITÀ DI TERRORISMO (ART. 270-QUINQUIES.1 C.P.)***

La condotta punita è quella di chi, al di fuori dei casi di cui agli artt. 270-*bis* c.p. e 270-*quater*.1 c.p. (*Organizzazione di trasferimenti per finalità di terrorismo*), raccoglie, eroga o mette a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento delle condotte con finalità di terrorismo di cui all'art. 270-*sexies* c.p., nonché chiunque deposita o custodisce i beni o il denaro prima indicati.

**B) Delitti con finalità di terrorismo o eversione dell'ordine democratico previsti da leggi penali speciali**

Accanto alle fattispecie espressamente disciplinate dal codice penale, vengono in considerazione i reati previsti in materia da apposite leggi speciali. I reati di terrorismo previsti dalle leggi speciali consistono in tutta quella parte della legislazione italiana volta a combattere il terrorismo.

Tra le disposizioni di cui sopra va ricordato l'art. 1, Legge 6 febbraio 1980, n. 15 che prevede, come circostanza aggravante applicabile a qualsiasi reato il fatto che il reato stesso sia stato "*commesso per finalità di terrorismo o di eversione dell'ordine democratico*". Ne consegue che qualsiasi delitto previsto dal codice penale o dalle leggi speciali, anche diverso da quelli espressamente diretti a punire il terrorismo può diventare, purché commesso con dette finalità, uno di quelli suscettibili di costituire, a norma dell'art. 25-*quater*, presupposto per l'affermazione della responsabilità dell'ente.

Altre disposizioni specificamente dirette alla prevenzione dei reati commessi con finalità di terrorismo, sono contenute nella Legge 10 maggio 1976, n. 342, in materia di repressione di delitti contro la sicurezza della navigazione aerea, e nella Legge 28 dicembre 1989, n. 422, in materia di repressione dei reati diretti contro la sicurezza della navigazione marittima e dei reati diretti contro la sicurezza delle installazioni fisse sulla piattaforma intercontinentale.

**C) Delitto di finanziamento del terrorismo previsto dall'art. 2 della Convenzione di New York del 9 Dicembre 1999**

Il richiamo a tale disposizione tende chiaramente ad evitare possibili lacune nella disciplina, già generale e generica, dettata ed è dunque diretto a rafforzare e completare l'ambito di riferimento anche mediante il rinvio ad atti internazionali.

Ai sensi del citato articolo, commette un reato chiunque con qualsiasi mezzo, direttamente o indirettamente, illegalmente e intenzionalmente, fornisca o raccolga fondi con l'intento di utilizzarli o sapendo che sono destinati ad essere utilizzati, integralmente o parzialmente, al fine di compiere qualsiasi altro atto diretto a causare la morte o gravi lesioni fisiche ad un civile, o a qualsiasi altra persona che non abbia parte attiva in situazioni di conflitto armato, quando la finalità di tale atto sia quella di intimidire una popolazione, o di obbligare un governo o un'organizzazione internazionale a compiere o ad astenersi dal compiere qualcosa.

Perché un atto possa comportare una delle suddette fattispecie non è necessario che i fondi siano effettivamente utilizzati per compiere quanto sopra descritto.

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

Commette altresì un reato chiunque:

- prenda parte in qualità di complice al compimento di un reato di cui sopra;
- organizzi o diriga altre persone al fine di commettere un reato di cui sopra;

- contribuisca al compimento di uno o più reati di cui sopra con un gruppo di persone che agiscono con una finalità comune. Tale contributo deve essere intenzionale e:
  - deve essere compiuto al fine di facilitare l'attività o la finalità criminale del gruppo, laddove tale attività o finalità implichino la commissione del reato;
  - deve essere fornito con la piena consapevolezza che l'intento del gruppo è di compiere un reato.

Al fine di poter affermare se sia o meno ravvisabile il rischio di commissione di tale tipologia di reati, occorre esaminare il profilo soggettivo richiesto dalla norma ai fini della configurabilità del reato.

Dal punto di vista dell'elemento soggettivo, i reati di terrorismo si configurano come reati dolosi. Quindi, perché si realizzi la fattispecie dolosa è necessario, dal punto di vista della rappresentazione psicologica dell'agente, che il medesimo abbia coscienza dell'evento antigiuridico e lo voglia realizzare attraverso una condotta a lui attribuibile. Pertanto, affinché si possano configurare le fattispecie di reato in esame, è necessario che l'agente abbia coscienza del carattere terroristico dell'attività e abbia l'intento di favorirla.

Peraltro, sarebbe altresì configurabile il perfezionamento della fattispecie criminosa, qualora il soggetto agisca a titolo di dolo eventuale. In tal caso, l'agente dovrebbe prevedere e accettare il rischio del verificarsi dell'evento, pur non volendolo direttamente. La previsione del rischio del verificarsi dell'evento e la determinazione volontaria nell'adottare la condotta criminosa devono comunque desumersi da elementi univoci e obiettivi.

### C.1.4 La normativa di prevenzione del Reato di Finanziamento del Terrorismo

Il D.Lgs. 22 giugno 2007, n.109 ha introdotto nel nostro ordinamento "*Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE*", emanata dal Parlamento Europeo e dal Consiglio in data 26 ottobre 2005.

La normativa in tema di Finanziamento del Terrorismo prevede che siano adottate le medesime misure di prevenzione già vigenti contro i Reati di Riciclaggio e introdotte con il Decreto Antiriciclaggio. Tale normativa prevede inoltre altre norme idonee per attuare il "*congelamento dei fondi*" e delle "*risorse economiche*" disposto dalle numerose risoluzioni del Consiglio di sicurezza delle Nazioni Unite che si sono succedute dal 1999 ad oggi, dal Regolamento CE n. 2580/2001 emanato dal Consiglio in data 27 dicembre 2001 e relativo a misure restrittive specifiche destinate a combattere il terrorismo, nonché dai Regolamenti

comunitari emanati ai sensi degli artt. 60 e 301 del Trattato istitutivo della Comunità Europea (ora artt. 75 e 215 del Trattato sul funzionamento dell'Unione europea) per il contrasto dell'attività dei Paesi che minacciano la pace e la sicurezza internazionale.

Ai sensi del D.Lgs. 109/2007, per "*congelamento di fondi*" si intende il divieto di movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi o di accesso ad essi, così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consente l'uso dei fondi, compresa la gestione del portafoglio. Per "*congelamento di risorse economiche*" si intende, invece, il divieto di trasferimento, disposizione o, al fine di ottenere in qualsiasi modo fondi, beni o servizi, utilizzo delle risorse economiche, compresi, a titolo meramente esemplificativo, la vendita, la locazione, l'affitto o la costituzione di diritti reali di garanzia

Il congelamento dei fondi e delle risorse economiche è disposto, con decreto, su proposta del Comitato di Sicurezza Finanziaria, dal Ministro dell'Economia e delle Finanze, di concerto con il Ministro degli affari esteri.

## CAPITOLO C.2

### C.2.1 Attività Sensibili nell'ambito dei Reati di Riciclaggio, dei Reati di Terrorismo e dei Reati in materia di strumenti di pagamento diversi dal contante e trasferimento fraudolento di valori

I reati trattati nella presente Parte Speciale, come del resto indicato anche dalla Linee Guida ANIA, sono senz'altro astrattamente ipotizzabili per il settore assicurativo, specialmente quello di riciclaggio e di finanziamento del terrorismo.

Al riguardo, sebbene le imprese di assicurazione esercenti il ramo danni nel quadro della legislazione antiriciclaggio non siano destinatarie di specifici obblighi di identificazione e segnalazione *ex* Decreto Antiriciclaggio, la Società ha ritenuto di predisporre la seguente Parte Speciale anche a presidio di un ambito comunque a rischio di commissione di Reati il cui elemento determinante è costituito dai rapporti con la clientela nell'ambito dei quali si può rinvenire a carico di coloro che agiscono per l'ente una finalità illecita o la consapevolezza di una altrui finalità illecita.

Di seguito sono elencate le attività che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati di cui al D.Lgs. 231/2001 trattati nella presente Parte Speciale:

- identificazione, registrazione e conservazione dati per ciascun cliente;
- liquidazione sinistri;
- selezione di Consulenti, Fornitori e *Partner* e gestione dei rapporti con gli stessi;
- gestione dei flussi finanziari (in entrata e in uscita);
- attività di investimento in Paesi a rischio terrorismo;
- gestione delle sponsorizzazioni ed effettuazione di altri atti di liberalità e correntezza;
- predisposizione e tenuta dei bilanci e delle altre scritture contabili;
- predisposizione delle dichiarazioni e gestione degli adempimenti fiscali (nonché attività di fatturazione infragruppo);
- gestione di strumenti di pagamento diversi dal contante;
- operazioni su *asset* aziendali.

### C.2.2 Principi generali di comportamento in relazione ai Reati di Riciclaggio, ai Reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori e ai Reati di Terrorismo

Obiettivo della presente Parte Speciale è che tutti i Dipendenti, Organi Sociali, i dipendenti di CA Vita per i servizi prestati a CAA, e i soggetti che operano a livello periferico si attengano – nei limiti delle rispettive competenze e nella misura in cui siano coinvolti nello svolgimento di Attività Sensibili individuate in precedenza – a regole di condotta conformi a quanto prescritto in tale Parte Speciale e nelle *policy* e procedure cui la stessa fa riferimento diretto o indiretto, al fine di prevenire la commissione dei Reati di Riciclaggio, Reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori e Reati con Finalità di Terrorismo.

In particolare, i soggetti sopra indicati, anche in relazione al tipo di rapporto posto in essere con la Società, dovranno attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai Reati di Riciclaggio, dai Reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori, dai Reati di Terrorismo;
2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di Fornitori /clienti/*Partner* anche stranieri;
4. non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura;
5. non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
6. non attribuire fittiziamente ad altri soggetti la titolarità o la disponibilità di denaro, beni o altre utilità, al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando e/o di agevolare la commissione di uno

dei delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

La Società, a sua volta, al fine di prevenire il rischio di commissione dei Reati di Riciclaggio, dei Reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori, dei Reati di Terrorismo :

1. adotta un sistema di individuazione e gestione del rischio di Riciclaggio e Finanziamento del Terrorismo conforme a quanto previsto dalle disposizioni normative tempo per tempo vigenti;
2. adotta sistemi, anche informatici, di identificazione, registrazione e conservazione dei dati per ciascun cliente che consentano la corretta imputazione di ogni operazione;
3. adotta specifiche procedure per la selezione e la gestione dei rapporti con i Consulenti e con i Fornitori;
4. adotta presidi idonei a prevenire il rischio di finanziamento del terrorismo in fase di liquidazione dei sinistri con controlli periodici;
5. adotta una politica finanziaria che preveda l'assoluto divieto di investire in "*Paesi a rischio di terrorismo*";
6. gestisce la liquidità in modo tale che non siano trasferite somme di denaro contante o libretti di deposito, bancari o postali, al portatore o altri titoli al portatore in euro o valuta estera, per importi pari o superiori a quello stabilito *ex lege* dal D.Lgs. 21 novembre 2007, n. 231 limiti di legge;
7. effettua un costante e regolare monitoraggio dei flussi finanziari aziendali, garantendone la tracciabilità e fornendo evidenza giustificativa di ciascuno di essi.

Fermi restando i principi previsti dalle Parti Speciali B (relativa ai Reati Societari) e M (relativa ai Reati Tributari), è fatto divieto di:

- commercializzare polizze assicurative attraverso canali distributivi non autorizzati dalla Società;
- commercializzare polizze assicurative attraverso soggetti non autorizzati all'intermediazione dei prodotti assicurativi;
- indurre con frode, raggiri o artifizi un consumatore a stipulare una polizza o ad acquistare un prodotto assicurativo.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, codici di comportamento, policy e procedure aziendali.

Tali *policy* e procedure e loro eventuali successive integrazioni o modifiche si considerano parte integrante del Modello e, pertanto, si devono intendere come recepite nella loro configurazione.

**C.2.3 Principi procedurali specifici in relazione ai Reati di Riciclaggio, ai Reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori e ai Reati di Terrorismo**

1) *Identificazione della clientela*

a. La Società:

- raccoglie e conserva i dati identificativi della clientela in fase di sottoscrizione di nuovi contratti assicurativi e in fase liquidativa;
- effettua controlli periodici o su richiesta delle autorità finalizzati a verificare che la clientela non sia presente all'interno di *Black List*, Liste Embargo o di Liste di soggetti segnalati, indagati o condannati per fatti criminosi.

2) *Liquidazione sinistri*

a. In relazione alla liquidazione dei sinistri, la Società:

- individua soggetti incaricati a raccogliere le richieste di liquidazione dei sinistri, a gestire le pratiche stesse, ad autorizzare e ad effettuare i pagamenti, garantendo il rispetto del principio di separazione dei ruoli;
- adotta specifiche procedure per la liquidazione dei sinistri che prevedano attività di identificazione e verifica del contraente a favore del quale deve essere disposto il pagamento;
- addotta presidi volti ad impedire che le operazioni di liquidazione delle polizze assicurative non vengano disposte a favore di soggetti elencati nelle Black List nazionali e internazionali o su conti correnti di persone fisiche e giuridiche che si trovino in Paesi "a rischio terrorismo" o per le quali sono state disposte misure restrittive da parte delle autorità europee e internazionali;
- adotta sistemi informatici volti ad evitare che la liquidazione del sinistro venga accreditato a favore di persona diversa dal contraente per il quale sono state regolarmente compiute attività di verifica;
- prevede che eventuali anomalie o incoerenze rilevate in fase di istruttoria o di liquidazione siano adeguatamente approfondite e gestite secondo le procedure interne, anche mediante il coinvolgimento delle funzioni competenti, prima di procedere al pagamento

3) *Selezione di Consulenti, Fornitori e* Partner *e gestione dei rapporti con gli stessi*

a. La Società verifica l'attendibilità commerciale e professionale dei Fornitori, *Partner* e dei Consulenti.

b. La Società adotta procedure o policy aziendali volte a garantire che il processo di selezione dei Fornitori, dei *Partner* e del Consulenti avvenga nel rispetto dei criteri di trasparenza, pari opportunità di accesso, professionalità, affidabilità ed economicità, fermo restando la prevalenza dei requisiti di legalità rispetto a tutti gli altri.

c. La Società tiene traccia dei Consulenti, Fornitori, *Partner*, e altre controparti con i quali siano già intercorsi rapporti contrattuali.

d. La Società si impegna, in occasione di ogni rinnovo contrattuale con Fornitori, *Partner* e Consulenti, a richiedere la sottoscrizione da parte di questi ultimi di un'autodichiarazione circa la persistenza dei requisiti di onorabilità che in fase di selezione iniziale hanno permesso l'instaurazione del rapporto;

e. I rapporti tra CAA e i Consulenti, i Fornitori e i *Partner* devono essere definiti per iscritto in tutte le loro condizioni e termini e rispettare quanto indicato ai successivi punti.

f. I contratti con Fornitori, *Partner* e Consulenti devono contenere (anche in caso di rinnovo) una clausola standard (cosiddetta "**Clausola 231**"), con cui questi ultimi:

   - dichiarino di conoscere la disciplina di cui al Decreto 231 e le sue implicazioni in termini di adempimenti e responsabilità;
   - si impegnino al rispetto delle disposizioni in esso contenute e dichiarino di non essere mai stato coinvolto in procedimenti giudiziari relativi ai reati contemplati nella suddetta normativa;
   - dichiarino di essere a conoscenza (avendone presa visione) del contenuto del Codice Etico e del Modello della Società ed – eventualmente – di aver adottato a loro volta un codice etico e un modello di organizzazione, gestione e controllo;
   - si impegnino a rispettare il contenuto del Codice Etico e del Modello della Società.

g. In conformità con le indicazioni fornite a livello di Gruppo, i contratti con i Consulenti, i Fornitori e i *Partner* prevedono, inoltre, il rispetto da parte dei medesimi di normative nazionali e/o internazionali applicabili e rilevanti.

4) *Gestione dei flussi finanziari in entrata e in uscita*

a. La Società effettua controlli sia formali che sostanziali dei flussi finanziari aziendali in entrata ed uscita. Tali controlli devono tener conto della sede legale della società controparte (ad esempio paradisi fiscali, Paesi a rischio terrorismo ecc.), degli istituti di credito utilizzati (sede delle banche coinvolte nelle operazioni) e di eventuali schermi societari e strutture fiduciarie utilizzate per eventuali operazioni straordinarie;

b. Per altre tipologie di incassi, è previsto il diniego di accettazione di denaro e titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) per importi complessivamente superiori ai limiti stabiliti *ex lege* dal D.Lgs. 21 novembre 2007, n. 231, se non tramite intermediari a ciò abilitati, quali banche, istituti di moneta elettronica e Poste Italiane S.p.A. da parte di clienti;

c. Sono previste modalità formalizzate per la modifica delle coordinate bancarie di pagamento del fornitore rispetto a quelle inizialmente concordate in sede contrattuale ovvero rispetto a quelle dallo stesso utilizzate in precedenti rapporti contrattuali.

d. Eventuali pagamenti "extra-sistema" possono essere effettuati solo in casi particolari (ad esempio, quando serve effettuare pagamenti su conti esteri extra SEPA oppure quando si ha necessità di fare un pagamento con estrema urgenza) e devono essere rendicontati periodicamente mediante caricamento sul sistema gestionale e/o mediante comunicazione all'ufficio interno competente.

e. Ad integrazione dei principi sopra esposti, nel caso di instaurazione di rapporti continuativi con controparti contrattuali, la Società si impegna ad attuare efficacemente controlli periodici circa

- la persistenza in capo a questi ultimi dei requisiti che in fase di selezione iniziale hanno permesso l'instaurazione del rapporto;
- l'effettiva esecuzione della consulenza/fornitura e la congruità del prezzo pattuito.

5) *Selezione, assunzione e gestione del personale e degli intermediari assicurativi*

a. La Società adotta procedure di selezione e assunzione del personale dipendente di qualsiasi livello e di collaboratori a progetto che garantiscano (anche nel caso in cui tali attività siano in parte affidate a società di *head hunting*):

   - parità di accesso a tutti i candidati;
   - modalità di scelta basate su criteri di meritocrazia, professionalità e onorabilità dei candidati;
   - affidabilità rispetto al rischio di infiltrazione criminale;

b. La Società conserva la documentazione esibita in sede di assunzione anche al fine di consentirne la consultazione da parte dell'OdV nell'espletamento della consueta attività di vigilanza e controllo.

c. La Società mette a disposizione copia del Modello 231 e del Codice Etico con la richiesta di prenderne visione e di impegnarsi al rispetto dei principi contenuti negli stessi.

d. La Società prevede contrattualmente che il datore di lavoro somministrante accerti la sussistenza dei requisiti di onorabilità dei propri dipendenti, consentendo alla Società di risolvere con effetto immediato il contratto di somministrazione di attività lavorativa qualora il dipendente somministrato risultasse indagato o condannato per reati di cui al D.Lgs. 231/2001.

e. Il processo di inserimento della risorsa all'interno della Società deve avvenire nel rispetto degli obblighi di formazione e aggiornamento previsti dalle procedure aziendali in base al ruolo e all'attività svolta all'interno dell'azienda.

f. Eventuali avanzamenti interni di carriera e riconoscimenti di premi (ivi compresa l'eventuale previsione, nel trattamento retributivo, di una componente variabile legata al raggiungimento di specifici obiettivi) devono essere assegnati secondo criteri oggettivi basati sulla parità di trattamento, sulla valorizzazione del merito e della professionalità nonché sul rispetto della normativa aziendale.

6) *Attività di investimento in Paesi a rischio terrorismo*

a. Gli investimenti da parte della Società vengono effettuati sulla base di un'apposita *investment policy*.

b. La Società adotta una politica finanziaria che preveda il divieto a carico della Compagnia, e degli eventuali terzi cui la stessa ha conferito incarico o mandato:

- di effettuare acquisti di strumenti o prodotti finanziari, partecipativi o non partecipativi, quotati o non quotati, titoli, investimenti in genere che abbiano a oggetto – diretto o indiretto – società o enti inseriti nelle *Black List* per il riciclaggio e per il finanziamento al terrorismo emanate e aggiornate dalle autorità italiane o straniere competenti;
- di avvalersi di servizi finanziari effettuati da società, enti o persone fisiche inseriti nelle *Black List* sopra richiamate.

7) *Gestione delle sponsorizzazioni ed effettuazione di altri atti di liberalità e correntezza*

a. La Società prevede che:

- le erogazioni liberali effettuate in qualsiasi forma, le donazioni e le sponsorizzazioni devono essere, indipendentemente dall'importo, deliberate e approvate dall'Amministratore Delegato e deve essere indicata la motivazione sottesa al compimento dell'atto di liberalità, sentito il Responsabile Area *Compliance*;
- di tali erogazioni deve essere informato anche l'OdV; se ritenuto opportuno dal manager che ha proposto l'erogazione liberale / donazione / sponsorizzazione, di tale azione può essere informato anche il Comitato Esecutivo (o Comex);
- le sponsorizzazioni al pari degli omaggi e regali sono mappate in apposito registro tenuto dall'unita aziendale preposta.
- L'*iter* da seguire per l'effettuazione di una sponsorizzazione prevede le seguenti fasi: (i) fase di analisi della documentazione; (ii) fase contrattuale (gestita secondo le linee guida aziendali in base all'importo della sponsorizzazione); (iii) controllo dell'utilizzo dei fondi; (iv) tracciabilità delle singole operazioni.

8) *Predisposizione e tenuta dei bilanci e delle altre scritture contabili*:

- sul punto, si rinvia a quanto previsto al cap. B.4 della Parte Speciale B.

9) *Predisposizione delle dichiarazioni e gestione degli adempimenti fiscali (nonché attività di fatturazione infragruppo)*:

- sul punto, si rinvia a quanto previsto al cap. M.4 della Parte Speciale M.

10) *Gestione di strumenti di pagamento diversi dal contante*

a. La Società garantisce:

- una chiara identificazione dei soggetti eventualmente intestatari di strumenti di pagamento diversi dal contante (ad esempio, carte di credito aziendali, laddove presenti) e delle modalità di autorizzazione dei pagamenti;
- il rispetto del divieto di falsificare, alterare, utilizzare indebitamente – non essendone titolare e al fine di trarne profitto per sé o altri (compresa la Società) – carte di credito o di pagamento, ogni documento che abiliti al prelievo di denaro contante o all'acquisto di beni o servizi e ogni altro strumento di pagamento diverso dai contanti (ad esempio, è fatto divieto di utilizzare carte di credito non riferibili alla Società per effettuare pagamenti per conto di quest'ultima e, in particolare, carte di credito intestate ad altri soggetti – persone fisiche o giuridiche – anche se collegati alla Società);
- che le spese effettuate per conto della Società mediante carte di credito o altre carte di pagamento (ad esempio, carta carburante) siano adeguatamente rendicontate;
- il divieto di produrre, importare, esportare, vendere, trasportare, distribuire ovvero mettere a disposizione apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono ideati al fine di commettere delitti con strumenti di pagamento diversi dai contanti;
- il rispetto del divieto di alterare in qualsiasi modo il funzionamento di sistemi informatici o telematici o intervenire sui contenuti di detti sistemi o comunque utilizzare gli stessi al fine di realizzare un trasferimento di denaro, di valore monetario o di valuta virtuale.

11) Operazioni su *asset*

In caso di eventuali operazioni societarie – riguardanti *asset* fisici (quali un immobile) ovvero partecipazioni societarie – devono essere rispettati i seguenti princìpi di comportamento:

- il rispetto del sistema di deleghe e procure in essere e garanzia di un doppio livello di controllo su ciascuna fase del processo (stima, determinazione del valore e cessione);

- un'accurata verifica sulle controparti coinvolte nelle operazioni di cessione, al fine di verificare la liceità dell'operazione e l'assenza di collegamenti con attività illecite;
- l'adozione di modalità trasparenti e tracciabili per tutti i passaggi del relativo *iter* e per quanto riguarda gli spostamenti di denaro che gli stessi comportano;
- la massima trasparenza nelle operazioni di cessione degli *asset* aziendale, anche mediante la corretta archiviazione delle documentazione a supporto e nel rispetto del principio di segregazione dei ruoli;
- che non venga posta in essere alcuna azione volta a pregiudicare in qualsivoglia modo le ragioni dell'erario (anche in relazione alla soddisfazione di eventuali pagamenti di imposte ovvero di interessi o sanzioni amministrative relativi a dette imposte) ovvero volta ad agevolare la commissione di un reato.

La Società – oltre ai presidi previsti in relazione alle specifiche Attività Sensibili sopra individuate – garantisce l'adozione dei seguenti principi procedurali specifici relativi ai rischi legati alla frode contrattuale (che potrebbe costituire un reato-base del reato di autoriciclaggio):

a) Nei confronti della clientela, la Società si impegna a svolgere la propria attività con trasparenza, diligenza e professionalità, sin dalla prima fase di informazione precontrattuale e durante tutto il rapporto di fornitura dei servizi assicurativi, compresa l'assistenza durante l'esecuzione del rapporto contrattuale, la liquidazione dei sinistri, nonché in caso di reclamo.

b) La Società, nell'osservanza delle disposizioni emanate dall'Autorità di Vigilanza, rispetta i principi volti a prevenire le frodi contrattuali, anche attraverso l'adozione di procedure o *policy* aziendali volte a specificare le diverse fasi di progettazione, commercializzazione, pubblicizzazione e gestione dei rapporti contrattuali, che prevedano, in particolare:

   - la definizione degli obiettivi, delle metodologie e delle funzioni coinvolte nelle diverse fasi di analisi, studio, controllo di conformità, realizzazione, promozione e pubblicità dei prodotti assicurativi;
   - la definizione dei processi autorizzativi per la commercializzazione e pubblicizzazione dei nuovi prodotti;

- l'istituzione di un comitato interfunzionale (Comitato Nuove Attività e Prodotti) il quale, composto dai responsabili delle funzioni interessate allo sviluppo e alla promozione di nuovi prodotti assicurativi nonché alla redazione delle disposizioni contrattuali, definisca gli obiettivi, le modalità e i contenuti principali dei prodotti di nuova erogazione o le modifiche da apportare ai prodotti già erogati dalla Società;
- la verbalizzazione degli incontri del suddetto comitato, nonché appositi flussi informativi con l'organo amministrativo.

c) La Società affida la distribuzione dei propri prodotti esclusivamente a soggetti autorizzati dall'Autorità di Vigilanza all'attività di intermediazione assicurativa.

d) La Società, in conformità alle disposizioni di Vigilanza, effettua controlli sulla vendita dei prodotti assicurativi volti specificamente a verificare la corretta esposizione ai clienti da parte degli intermediari delle condizioni generali di polizza in fase precontrattuale, nonché la raccolta e conservazione di tutta la documentazione e delle informazioni necessarie per la profilazione del cliente.

e) La Società si dota di risorse e strumenti conformi alla normativa di Vigilanza volti a garantire al cliente l'ottenimento di informazioni o chiarimenti esaustivi sui rapporti contrattuali in essere nonché la gestione di eventuali reclami.

f) La Società si impegna a fornire ai propri intermediari tutte le informazioni, istruzioni e documenti necessari alla commercializzazione delle polizze assicurative, nonché ad organizzare o verificare che siano effettuati adeguati corsi di formazione.

## CAPITOLO C.2.4

## I controlli dell'OdV in relazione ai Reati di Riciclaggio, ai Reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori e ai Reati di Terrorismo

L'OdV effettua dei periodici controlli diretti a verificare il corretto adempimento da parte dei Destinatari, nei limiti dei rispettivi compiti e attribuzioni, delle regole e principi contenuti nella presente Parte Speciale e nelle procedure aziendali cui la stessa fa esplicito o implicito richiamo.

In particolare, è compito dell'Organismo di Vigilanza:

a) monitorare l'efficacia delle procedure interne in relazione alla prevenzione dei Reati di Riciclaggio, dei Reati in materia di strumenti di pagamento diversi dai contanti e di Finanziamento del Terrorismo e Reati con Finalità di Terrorismo;

b) proporre eventuali modifiche nelle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;

c) esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi esponente della Società ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti, l'OdV può incontrarsi e consultarsi, in particolare, con:

a) il Responsabile dell'Area *Finance & Strategy*.

b) il Responsabile del Servizio Fiscale.

Per i flussi informativi si rimanda, in particolare, alla compilazione da parte delle funzioni competenti delle "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento) che costituiscono un allegato al Modello.

**PARTE SPECIALE – D –**

**Delitti contro la personalità individuale e impiego di cittadini di paesi terzi il cui soggiorno è irregolare**

## CAPITOLO D.1

### D.1.1 Le fattispecie dei delitti contro la personalità individuale (art. 25-*quinquies*, D.Lgs. 231/2001)

La presente Parte Speciale si riferisce ai reati contro la personalità individuale introdotti ai sensi dell'art. 5, Legge 11 agosto 2003, n. 228, in tema di misure contro la tratta delle persone che ha aggiunto nel *corpus* del Decreto l'art. 25-*quinquies* (di seguito "***Reati contro la personalità individuale***").

Si provvede qui di seguito a fornire una breve descrizione dei reati contemplati nella presente Parte Speciale "D", così come indicati all'art. 25-*quinquies* del Decreto e ritenuti astrattamente applicabili alla Società.

***RIDUZIONE O MANTENIMENTO IN SCHIAVITÙ O IN SERVITÙ (ART. 600 C.P.)***

L'articolo punisce chiunque esercita su una persona poteri corrispondenti a quelli del diritto di proprietà ovvero chiunque riduce o mantiene una persona in uno stato di soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque al compimento di attività illecite che ne comportino lo sfruttamento ovvero a sottoporsi a prelievo di organi.

La riduzione o il mantenimento nello stato di soggezione ha luogo quando la condotta è attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di vulnerabilità, di inferiorità fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona.

La pena è aumentata da un terzo alla metà se i fatti di cui al primo comma sono commessi in danno di minore degli anni diciotto o sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi.

***INTERMEDIAZIONE ILLECITA E SFRUTTAMENTO DEL LAVORO (ART. 603-BIS C.P.)***

In data 4 novembre 2016, è entrato in vigore l'articolo 603-*bis* c.p. nella nuova formulazione. La legge in oggetto modifica, inoltre, l'art. 25-*quinquies* del Decreto 231, in tema di delitti contro la personalità individuale, aggiungendo, al comma 1, lett. a, il richiamo al nuovo reato di cui all'art. 603-*bis* c.p.

Il nuovo testo dell'articolo 603-*bis*, c.p., rubricato "intermediazione illecita e sfruttamento del lavoro" dispone che "*Salvo che il fatto costituisca più grave reato*" sia punito chiunque: "*1)*

*recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori; 2) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento e approfittando del loro stato di bisogno*". È prevista una pena più severa "*se i fatti sono commessi mediante violenza o minaccia*". Inoltre, ai fini dell'articolo in parola, "*costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni: 1) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato; 2) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie; 3) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro; 4) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti*". Costituiscono, invece, aggravanti del reato: "*1) il fatto che il numero di lavoratori reclutati sia superiore a tre; 2) il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa; 3) l'aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro*".

Con la nuova formulazione della fattispecie, è scomparso l'ambiguo riferimento al requisito dell'"organizzazione" dell'opera di intermediazione, presente nella precedente formulazione della norma, aprendo così le porte anche alla condanna di chi non compie tale attività in maniera stabile. Inoltre, per il perfezionamento della fattispecie non è più richiesto che lo stesso sia commesso mediante violenza o minaccia (o intimidazione), le quali configurano ora una mera ipotesi aggravante.

***

Per quanto attiene ai reati connessi alla schiavitù, tali ipotesi di reato si estendono non solo al soggetto che direttamente realizza la fattispecie illecita, ma anche a chi consapevolmente agevola anche solo finanziariamente la medesima condotta.

La condotta rilevante in questi casi può essere costituita dal procacciamento illegale della forza lavoro attraverso il traffico di migranti e la tratta degli schiavi.

Un esempio potrebbe essere rappresentato dal procacciamento di servizi (ad esempio l'attività di pulizia della sede della società) tramite un'impresa appaltatrice che si serva di persone ridotte quasi in schiavitù e che, per tale ragione, prestano la propria attività a prezzo sensibilmente inferiore rispetto alla concorrenza.

***

### D.1.2. Le fattispecie di delitto di impiego di cittadini terzi il cui soggiorno è irregolare, procurato ingresso illecito di stranieri nel territorio dello Stato e favoreggiamento dell'immigrazione clandestina (art. 25-*duodecies*, D.Lgs. 231/2001)

La presente Parte Speciale si riferisce anche al delitto di "*impiego di cittadini terzi il cui soggiorno è irregolare*" introdotto nel novero dei reati presupposto del Decreto 231, sotto l'articolo l'art. 25-*duodecies*, dal Decreto Legislativo 16 luglio 2012, n. 109, il quale, entrato in vigore il 9 agosto 2012, disciplina l'attuazione della Direttiva 2009/52/CE.

Tale reato si configura qualora il soggetto che riveste la qualifica di datore di lavoro occupi alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno[4], ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, o sia stato revocato o annullato, laddove i lavoratori occupati siano:

a) in numero superiore a tre;

b) minori in età non lavorativa;

c) sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-*bis*, c.p.

L'art. 25-*duodecies* è stato oggetto di modifiche ad opera della Legge 161 del 4 novembre 2017, che ha introdotto il richiamo all'art. 12 del D.Lgs. 25 luglio 1998, n. 286 ("*Disposizioni contro le immigrazioni clandestine*"), in relazione alle condotte di procurato ingresso illecito di stranieri nel territorio dello Stato e favoreggiamento dell'immigrazione clandestina. Il novellato art. 25-*duodecies* richiama l'art. 12 del D.Lgs. 25 luglio 1998, n. 286 limitatamente alle seguenti previsioni:

**Art. 12, commi 3, 3-*bis*, 3-*ter*, D.Lgs. 286/1998**

Tale fattispecie punisce chiunque, in violazione delle disposizioni del D.Lgs. 286/1998 promuove, dirige, organizza, finanzia o effettua il trasporto di stranieri nel territorio dello Stato ovvero compie altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente; si applica una multa per ogni persona nel caso in cui:

a. il fatto riguarda l'ingresso o la permanenza illegale nel territorio dello Stato di cinque o più persone;

[4] Per permesso di soggiorno si intende il documento che consente al cittadino extracomunitario di soggiornare sul territorio italiano regolarmente.

b. la persona trasportata è stata esposta a pericolo per la sua vita o per la sua incolumità per procurarne l'ingresso o la permanenza illegale;

c. la persona trasportata è stata sottoposta a trattamento inumano o degradante per procurarne l'ingresso o la permanenza illegale;

d. il fatto è commesso da tre o più persone in concorso tra loro o utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti;

e. gli autori del fatto hanno la disponibilità di armi o materie esplodenti.

Se ricorrono due o più delle ipotesi di cui all'elenco sopra, la pena è aumentata.

La pena è aumentata anche se i fatti:

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

**Articolo 12, comma 5, D.Lgs. 286/1998**

Tale fattispecie punisce chiunque fuori dei casi previsti dai commi precedenti, e salvo che il fatto non costituisca più grave reato, al fine di trarre un ingiusto profitto dalla condizione di illegalità dello straniero o nell'ambito delle attività punite a norma del presente articolo, favorisce la permanenza di questi nel territorio dello Stato in violazione delle disposizioni di cui al D.Lgs. 286/1998.Quando il fatto è commesso in concorso da due o più persone, ovvero riguarda la permanenza di cinque o più persone, è previsto un aumento di pena.

## CAPITOLO D.2

## Attività Sensibili

### D.2.1. Attività Sensibili in relazione ai delitti contro la personalità individuale

I delitti in oggetto non sono né facilmente né tutti ipotizzabili per il settore assicurativo, ma la Società ha preferito comunque tenerne conto e considerare i relativi rischi sia per l'attività aziendale sia per la prestazione assicurativa. Pertanto, pur escludendo coinvolgimenti tali da far pensare ad una impresa di assicurazione diretta a perseguire, in tutto o in parte, finalità identificabili o connesse con il compimento di attività criminose configuranti i reati predetti, sono state contemplate solo le fattispecie di concorso o di fiancheggiamento nei reati stessi.

Di seguito è indicata l'attività che, per il suo contenuto intrinseco, è considerata maggiormente esposta alla commissione dei Reati di cui al D.Lgs. 231/2001:

- contratti di consulenza finanziaria prestata a favore di clienti o affidamento di contratti di fornitura di servizi e appalto a soggetti che – direttamente o indirettamente – gestiscano attività illecite come il traffico di minori o impongano condizioni lavorative ai propri dipendenti tali da configurare vere e proprie forme di schiavitù ovvero contratti volti a costituire forme di appalto illecite.

### D.2.2. Attività Sensibili in relazione alle fattispecie di delitto di impiego di cittadini terzi il cui soggiorno è irregolare, procurato ingresso illecito di stranieri nel territorio dello Stato e favoreggiamento dell'immigrazione clandestina

Sebbene le fattispecie in oggetto non siano facilmente ipotizzabili in una realtà come quella della Compagnia, si è tenuto comunque conto dei relativi rischi sia per l'attività assicurativa sia per i rapporti con i soggetti terzi. Di seguito sono descritte le attività ritenute più specificamente a rischio:

- *Selezione, assunzione e gestione del personale*: si tratta di attività finalizzate all'assunzione di personale dipendente e consistenti nell'accertamento del possesso di tutta la documentazione necessaria per poter soggiornare regolarmente nel territorio italiano. Le attività di assunzione del personale si svolgono attraverso l'attribuzione di specifico incarico a società di *head hunting* o attraverso la selezione diretta da parte dei responsabili di funzione interessati all'integrazione della risorsa.

L'Attività Sensibile in esame è legata ai profili di rischiosità connessi – nell'ottica della possibile commissione del delitto in oggetto – all'impiego in azienda di personale senza regolare permesso di soggiorno.

- *Affidamento di attività in appalto*: si tratta di attività finalizzate ad accertare che le controparti contrattuali (appaltatori e subappaltatori) non impieghino nell'ambito dei servizi prestati in favore della Compagnia cittadini stranieri privi del regolare permesso di soggiorno.

## CAPITOLO D.3

## Principi generali di comportamento

### D.3.1 Principi di comportamento

Obiettivo della presente Parte Speciale è che i Dipendenti, gli Organi Sociali, i soggetti che operano a livello periferico (agenti, sub-agenti, personale d'agenzia, promotori, *broker*) e i *Partner* della Società, come meglio individuati nella Parte Generale del Modello, si attengano a regole di condotta conformi a quanto infra prescritto nonché alle *policy* e procedure cui la stessa fa riferimento diretto o indiretto, al fine di prevenire e impedire il verificarsi di condotte rilevanti o un coinvolgimento nella commissione dei Reati contro la personalità individuale.

Ai Destinatari individuati nei paragrafi precedenti è vietato:

a) porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 25-*quinquies* e 25-*duodecies* del Decreto);

b) porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo o favorirne la commissione.

A tal fine la Società:

a) considera sempre prevalente la tutela dei diritti delle persone e dei lavoratori rispetto a qualsiasi considerazione economica;

b) vieta l'assunzione di dipendenti stranieri privi di permesso di soggiorno regolare e vieta di conferire incarichi ad appaltatori e/o subappaltatori che, al contrario, se ne avvalgano;

c) non si avvale, in alcun modo, del lavoro minorile e non collabora con soggetti che vi facciano ricorso.

I Destinatari sono tenuti a utilizzare in modo adeguato gli strumenti informatici in proprio possesso non accedendo a siti internet non autorizzati (con particolare riferimento ai siti contenenti materiale illecito, quale il materiale pedo-pornografico).

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, codici di comportamento, policy e procedure aziendali.

Tali *policy* e procedure e loro eventuali successive integrazioni o modifiche si considerano parte integrante del Modello e, pertanto, si devono intendere come recepite nella loro configurazione.

## CAPITOLO D.4.

### Principi procedurali specifici

Ai fini dell'attuazione dei principi e regole generali e dei divieti elencati al precedente cap. D.3, devono rispettarsi gli specifici principi procedurali qui di seguito descritti, oltre alle regole e principi generali contenuti nella Parte Generale del Modello. Le regole qui di seguito descritte, devono essere rispettate sia nell'esplicazione dell'attività di CAA in territorio italiano, sia eventualmente all'estero.

### D.4.1. Principi procedurali specifici relativi ai reati contro la personalità individuale

1) *Contratti di consulenza finanziaria prestata a favore di clienti o affidamento di contratti di fornitura di servizi e appalto a soggetti che – direttamente o indirettamente – gestiscano attività illecite come il traffico di minori o impongano condizioni lavorative ai propri dipendenti tali da configurare vere e proprie forme di schiavitù*:

a) I Destinatari del presente Modello sono obbligati:

- nei rapporti con i Fornitori e con i clienti, a rispettare tutti i principi procedurali indicati dalle *policy* aziendali con riguardo all'instaurazione dei suddetti rapporti;
- ad instaurare e mantenere rapporti con i Fornitori e clienti improntati alla massima correttezza e trasparenza richiedendo, in sede contrattuale, garanzie (con facoltà della Società di svolgere controlli in merito) sul rispetto da parte di questi ultimi della normativa di settore in materia giurislavoristica (compreso il rispetto del CCNL applicabile), di salute e sicurezza sul luogo di lavoro nonché dei principi etici a tutela della persona;
- a inserire nei contratti con i Fornitori la Clausola 231 una clausola standard (cosiddetta "**Clausola 231**"), con cui questi ultimi:
  - dichiarino di conoscere la disciplina di cui al Decreto 231 e le sue implicazioni in termini di adempimenti e responsabilità;
  - si impegnino al rispetto delle disposizioni in esso contenute e dichiarino di non essere mai stato coinvolto in procedimenti giudiziari relativi ai reati contemplati nella suddetta normativa;
  - dichiarino di essere a conoscenza (avendone presa visione) del contenuto del Codice Etico e del Modello della Società ed – eventualmente – di aver

adottato a loro volta un codice etico e un modello di organizzazione, gestione e controllo;

- si impegnino a rispettare il contenuto del Codice Etico e del Modello della Società.

b) Al fine di prevenire i reati contro la personalità individuale la Società:

(i) provvede a richiedere le necessarie informazioni ai Fornitori al fine di valutare la trasparenza degli stessi nell'ambito del rispetto dei diritti del lavoratore e della normativa in materia di salute e sicurezza;

(ii) chiede al Fornitore di comunicare il ricorso a eventuali subappaltatori nell'ambito del servizio o dell'opera oggetto del contratto di appalto per consentire alla Società di svolgere le valutazioni del caso;

(iii) nell'ambito delle verifiche svolte prima dell'istaurazione di rapporti contrattuali con i Fornitori prevede l'effettuazione di un controllo sulla capacità organizzativa del Fornitore rispetto alla realizzazione del servizio o dell'opera oggetto del contratto di appalto con la Società;

(iv) laddove intenda locare immobili di proprietà, valuta e disciplina con particolare dovizia la stipula dei relativi contratti di locazione (*i.e.* procedendo ad un'accurata valutazione della controparte al fine di escludere che negli immobili locati vengano realizzate le condotte illecite di cui al Capitolo D.1).

### D.4.2. Principi di comportamento in relazione al delitto di impiego di cittadini terzi il cui soggiorno è irregolare

1) *Selezione, assunzione e gestione del personale:*

a) Al fine di prevenire e impedire il verificarsi di condotte rilevanti o un coinvolgimento nella commissione del delitto di impiego di cittadini terzi il cui soggiorno è irregolare, la Società:

(i) nell'ambito delle attività di assunzione di dipendenti stranieri esegue tutte le procedure previste dalle disposizioni normative vigenti in tema di immigrazione e in particolare:

- in caso di assunzione di cittadini stranieri residenti in Paesi Extracomunitari, si attiva presso le autorità competenti al fine di ottenere tutta la

documentazione necessaria a consentire l'ingresso legale in Italia del cittadino straniero e l'instaurazione di un rapporto di lavoro regolare;

- in caso di assunzione di cittadini stranieri già soggiornanti in Italia verifica che i medesimi siano in possesso di un permesso di soggiorno regolare o che in caso di scadenza dello stesso i medesimi abbiano provveduto ad avviare le pratiche per il rinnovo.

b) Nella gestione rei rapporti di lavoro, la Società controlla che in occasione della scadenza dei permessi di soggiorno dei dipendenti stranieri, questi ultimi abbiamo provveduto ad avviare le relative pratiche di rinnovo, assicurando loro collaborazione nel rilascio della documentazione attestante l'impiego regolare presso la Società.

c) Nel caso in cui la Società intenda fare ricorso alla somministrazione di lavoro da parte di società specificamente autorizzate dal Ministero del Lavoro e delle Politiche Sociali, pone in essere dei presidi contrattuali volti a garantire che tali soggetti si avvalgano di lavoratori stranieri in regola con la normativa in materia di permesso di soggiorno e inserisce nei relativi contratti la Clausola 231.

2) *Affidamento di attività in appalto:*

a) Vengono adottati presidi idonei a garantire che l'appaltatore e il subappaltatore non impieghino cittadini stranieri privi di permesso di soggiorno o con permesso di soggiorno irregolare. A tal fine, la Società si impegna a verificare il rispetto dei seguenti presidi:

(i) la garanzia da parte dell'appaltatore di impiegare nella prestazione di servizi a favore della Società esclusivamente lavoratori stranieri lecitamente soggiornanti in Italia e con rapporto di lavoro regolare;

(ii) l'impegno da parte dell'appaltatore a comunicare l'elenco, con specificazione delle generalità, dei dipendenti preposti allo svolgimento del servizio in appalto e subappalto presso la Società e a comunicare con almeno tre giorni di preavviso ogni eventuale variazione dell'elenco medesimo;

(iii) l'impegno da parte dell'appaltatore a fornire all'atto della sottoscrizione del contratto e successivamente con periodicità stabilita dalle parti copia del Documento Unico di Regolarità Contributiva relativo alla posizione amministrativa dell'appaltatore e dei propri subappaltatori rilasciato dalle autorità competenti;

(iv) l'impegno, in generale, dell'appaltatore a rispettare, senza alcuna riserva, i diritti e la dignità dei propri lavoratori dipendenti e dei minori;

(v) la facoltà da parte della Società di richiedere in ogni momento copia del Libro Unico del Lavoro tenuto dall'appaltatore e dagli eventuali subappaltatori.

## CAPITOLO D.5

## I controlli dell'OdV e i flussi informativi

### D.5.1 Il controllo in generale

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui alla presente Parte Speciale, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

Inoltre, i compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i Reati contro la personalità individuale sono i seguenti:

- proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei Reati contro la personalità individuale e di impiego di cittadini di stati terzi privi di permesso di soggiorno regolare di cui alla presente Parte Speciale;
- monitoraggio sul rispetto delle procedure per la prevenzione dei Reati contro la personalità individuale e del reato di impiego di cittadini stranieri privi di permesso di soggiorno regolare in costante coordinamento con le funzioni *Compliance Data Protection, Reclami e controlli reti distributive* e *Internal Audit*;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Per i flussi informativi si rimanda alla compilazione da parte delle funzioni competenti delle "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento) che costituiscono un allegato al Modello

**PARTE SPECIALE – E –**

**Reati e illeciti amministrativi di abuso di mercato**

## CAPITOLO E.1

## Le fattispecie dei reati e di illeciti amministrativi di abuso di mercato (Art. 25-*sexies*, D.Lgs. 231/2001 e Art. 187-*quinquies* TUF)

Si descrivono di seguito le singole fattispecie di reato e di illecito amministrativo per le quali l'art. 25-*sexies*, D.Lgs. 231/2001 e l'art. 187-*quinquies* D.Lgs. n. 58/98 (di seguito, "**TUF**") prevedono la responsabilità della Società nei casi in cui tali reati e illeciti amministrativi siano stati compiuti nell'interesse o a vantaggio della società stessa. I reati e gli illeciti amministrativi di cui alla presente Parte Speciale si riferiscono a strumenti finanziari ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altro Paese dell'Unione Europea. La relativa disciplina è stata innovata con il Regolamento (UE) n. 596/2014 del Parlamento Europeo e del Consiglio del 16 aprile 2014 (cosiddetto "**Regolamento MAR**"), relativo agli abusi di mercato, al quale – a seguito della novella legislativa intervenuta con il D.Lgs. 10 agosto 2018, n. 107 – vengono ora effettuati diversi rimandi da parte del TUF.

### E.1.1 La definizione di "informazione privilegiata"

Attorno al concetto di informazione privilegiata ruota l'intera disciplina sull'*insider trading* e quella concernente l'informazione societaria disciplinata nel Titolo III, Capo I, artt. 114 e seguenti del TUF e nel Regolamento Emittenti n. 11971/1999.

Secondo quanto previsto dall'art. 180, lett. b-*ter*, TUF, si intendono di carattere privilegiato le informazioni che presentano le seguenti caratteristiche (qui di seguito le "**Informazioni Privilegiate**"):

a. sono di carattere preciso e pertanto:

   (i) devono essere inerenti a un complesso di circostanze o eventi esistenti o verificatisi o a circostanze o eventi che ragionevolmente possa prevedersi che verranno ad esistenza o che si verificheranno (il riferimento è ai casi in cui la notizia è in via di formazione e riguarda eventi non ancora verificatisi, si pensi al caso caratterizzato dalla notizia che una società quotata stia per lanciare un'OPA, oppure il caso riguardante un piano strategico di riposizionamento produttivo della società emittente i titoli); e

   (ii) devono essere sufficientemente specifiche (ossia esplicite e dettagliate), in modo che chi le impiega sia posto in condizione di ritenere che dall'uso delle stesse

potranno effettivamente realizzarsi quegli effetti sul prezzo degli strumenti finanziari;

b. non sono ancora state rese pubbliche;

c. riguardano, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, e sono relative alla situazione economica patrimoniale ("corporate information") ovvero a vicende organizzative dell'emittente ("market information");

d. sono *"price sensitive"*, ossia sono tali che, se rese pubbliche, sarebbero presumibilmente utilizzate da un investitore ragionevole come uno degli elementi su cui fondare le proprie decisioni di investimento.

Inoltre, il legislatore dell'Unione Europea – con il Regolamento MAR – ha precisato ulteriormente il concetto in esame, specificando, all'art. 7, che "*nel caso di un processo prolungato che è inteso a concretizzare, o che determina una particolare circostanza o un particolare evento, tale futura circostanza o futuro evento, nonché le tappe intermedie di detto processo che sono collegate alla concretizzazione o alla determinazione della circostanza o dell'evento futuri possono essere considerate come informazioni aventi carattere preciso*" e che, di conseguenza, "*una tappa intermedia in un processo prolungato è considerata un'informazione privilegiata*".

Con riferimento alla definizione in oggetto si elencano qui di seguito, a mero titolo esemplificativo e non esaustivo, alcune circostanze in cui la Società potrebbe trovarsi a dover gestire Informazioni Privilegiate appartenenti ad altre società:

- distribuzione di prodotti assicurativi a prevalente contenuto finanziario;
- dati revisionali e obiettivi quantitativi concernenti l'andamento della gestione;
- comunicazioni relative a operazioni di fusione/scissione e a nuove iniziative di particolare rilievo ovvero a trattative e/o accordi in merito all'acquisizione e/o cessione di *asset* significativi;
- attività di finanza straordinaria, quali, a titolo esemplificativo, fusioni, scissioni, incorporazioni, scorpori;
- mutamento nel controllo o nei patti parasociali di controllo;
- cambiamenti nell'organo di amministrazione e controllo;
- modifica del revisore o qualsiasi informazione collegata alla sua attività;

- operazioni sul capitale o emissione di obbligazioni o warrant per acquistare/sottoscrivere azioni;
- aumento o diminuzione del capitale sociale;
- acquisto o cessione di partecipazioni o altri asset o attività rilevanti;
- ristrutturazione o riorganizzazione che abbiano un effetto sul bilancio;
- decisioni relative ai programmi di acquisto di azioni proprie o operazioni aventi ad oggetto altri strumenti finanziari quotati;
- modifiche dei diritti relativi a determinate categorie di azioni quotate;
- istanze di fallimento ovvero ordinanze del tribunale relative a procedure concorsuali;
- significative controversie legali;
- revoca o cancellazione di linee di credito;
- liquidazione volontaria o altre cause di liquidazione;
- rilevante cambiamento nel valore degli *asset*;
- insolvenza dei principali debitori;
- riduzione del valore delle proprietà immobiliari;
- introduzione di processi o prodotti innovativi;
- decremento o incremento nel valore degli strumenti finanziari in portafoglio;
- aggiudicazione di gare per l'acquisto di *asset* rilevanti;
- ordini rilevanti ricevuti da clienti, loro cancellazione o rilevanti modifiche;
- ritiro o ingresso in rilevanti settori di business;
- rilevanti modifiche nella politica degli investimenti;
- informazioni relative al pagamento dei dividendi;
- analisi relative a strumenti finanziari o emittenti in particolare se contenenti raccomandazioni di investimento;
- rapporti delle agenzie di *rating*, ricerche da parte di banche d'affari, raccomandazioni o suggerimenti concernenti gli strumenti finanziari;

- decisioni riguardanti le modifiche delle regole di *governance* degli indici di mercato, con particolare riguardo alla loro composizione;
- decisioni delle autorità della concorrenza e del mercato relative alle società quotate non ancora pubblicate.

### E.1.2 I reati di abuso di mercato

***ABUSO O COMUNICAZIONE ILLECITA DI INFORMAZIONI PRIVILEGIATE. RACCOMANDAZIONE O INDUZIONE DI ALTRI ALLA COMMISSIONE DI ABUSO DI INFORMAZIONI PRIVILEGIATE (ART. 184 TUF)***

La fattispecie punisce chiunque, essendo in possesso di informazioni privilegiate per essere membro di organi amministrativi, di direzione o di controllo di una società emittente, oppure per essere socio, ovvero per averle apprese nell'esercizio di un'attività lavorativa, di una professione o di una funzione privata o pubblica, o di un ufficio:

a. acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni privilegiate acquisite nelle modalità sopra descritte (c.d. "*insider trading*");

b. comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio cui si è preposti (a prescindere dalla circostanza che i terzi destinatari utilizzino effettivamente l'informazione comunicata per compiere operazioni) (c.d. "*tipping*");

c. raccomanda o induce altri, sulla base delle informazioni privilegiate delle quali è in possesso, a compiere taluna delle operazioni indicate nella lettera a) (c.d. "*tuyautage*").

La fattispecie punisce, inoltre, i soggetti che, entrando in possesso di informazioni privilegiate a causa della preparazione o della realizzazione di attività delittuose, compiono taluna delle azioni di cui sopra (è l'ipotesi, ad esempio, del pirata informatico che a seguito dell'accesso abusivo al sistema informatizzato di una società riesce ad entrare in possesso di informazioni riservate *"price sensitive"*).

Inoltre, fuori dai casi di concorso nel reato, la fattispecie punisce anche chiunque essendo in possesso di informazioni privilegiate per motivi diversi da quelli sopra indicati (cosiddetto "*insider* secondario") e conoscendo il carattere privilegiato di tali informazioni commette taluni dei fatti sopra indicati.

***MANIPOLAZIONE DI MERCATO (ART. 185 TUF)***

La fattispecie punisce chiunque diffonde notizie false (c.d. manipolazione informativa) o pone in essere operazioni simulate o altri artifizi (c.d. manipolazione operativa) concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

È prevista una circostanza aggravante nel caso in cui il fatto sia commesso mediante l'impiego di sistemi di intelligenza artificiale.

Si ha manipolazione informativa anche allorquando la creazione di un'indicazione fuorviante derivi dall'inosservanza degli obblighi di comunicazione da parte dell'emittente o di altri soggetti obbligati.

### E.1.3 Gli illeciti amministrativi *ex* art. 187-*quinquies* del TUF

L'art. 187-*quinquies* del TUF opera un rinvio espresso alla normativa europea, disponendo, in particolare, che siano vietate le condotte che violino l'art. 14 o l'art. 15 del Regolamento MAR.

***ABUSO DI INFORMAZIONI PRIVILEGIATE E COMUNICAZIONE ILLECITA DI INFORMAZIONI PRIVILEGIATE (ART. 14 REGOLAMENTO MAR)***

L'art. 14 del Regolamento MAR prevede che non sia consentito:

a) abusare o tentare di abusare di informazioni privilegiate;

b) raccomandare ad altri di abusare di informazioni privilegiate o indurre altri ad abusare di informazioni privilegiate; oppure

c) comunicare in modo illecito informazioni privilegiate.

I comportamenti degli *insider* secondari sono puniti sia se sono commessi a titolo di dolo sia se sono commessi con colpa.

***DIVIETO DI MANIPOLAZIONE DEL MERCATO (ART. 15 REGOLAMENTO MAR)***

L'art. 15 del Regolamento MAR prevede che non sia consentito effettuare manipolazioni di mercato o tentare di effettuare manipolazioni di mercato.

Sulla scorta dell'interpretazione fornita da dottrina e giurisprudenza in merito alla disciplina previgente alla novella, si precisa che l'illecito amministrativo di manipolazione del mercato è teso ad ampliare le condotte rilevanti ai fini dell'applicabilità delle sanzioni amministrative rispetto a quelle penalmente sanzionate dalla corrispondente fattispecie delittuosa e punisce chiunque, tramite qualsiasi mezzo di informazione, compreso internet, diffonde informazioni, voci o notizie false o fuorvianti che forniscano o siano suscettibili di fornire indicazioni false ovvero fuorvianti in merito agli strumenti finanziari. A differenza di quanto previsto dalla corrispondente fattispecie di reato, pertanto, non è richiesto, ai fini della sanzionabilità delle condotte, che le notizie false, le operazioni simulate o gli altri artifizi siano "concretamente idonee" ad alterare i prezzi.

* * *

Prevede l'art. 187-*quinquies* che l'ente sia punito con una sanzione amministrativa pecuniaria che può arrivare al quindici per cento del fatturato (quando tale importo sia superiore a quindici milioni di euro e il fatturato sia determinabile ai sensi dell'articolo 195, comma 1-*bis* TUF[5]), nel caso in cui sia commessa nel suo interesse o a suo vantaggio una violazione del divieto di cui all'articolo 14 o del divieto di cui all'articolo 15 del Regolamento MAR:

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria o funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

Se, in seguito alla commissione degli illeciti, il prodotto o il profitto conseguito dall'ente è di rilevante entità, la sanzione è aumentata fino a dieci volte tale prodotto o profitto.

Si sottolinea, inoltre, che anche il semplice tentativo può rilevare ai fini dell'applicabilità della disciplina in oggetto, essendo questo – nei casi di specie – equiparato alla consumazione.

[5] Il quale prevede che "ai fini dell'applicazione delle sanzioni amministrative pecuniarie previste dal presente titolo, per fatturato si intende il fatturato totale annuo della società o dell'ente, risultante dall'ultimo bilancio disponibile approvato dall'organo competente, così come definito dalle disposizioni attuative di cui all'articolo 196-bis".

## CAPITOLO E.2

### Attività Sensibili nell'ambito dei reati di abuso di mercato

È opportuno ricordare che le imprese di assicurazione non rientrano nella categoria degli intermediari finanziari (c.d. soggetti abilitati) come individuati dall'art. 1 TUF e vengono parificate a questi esclusivamente in casi specifici, che prevedono per alcuni operatori economici l'adempimento di vari oneri per il contrasto, a livello finanziario, di determinate fattispecie criminose, quali il riciclaggio di denaro e il terrorismo internazionale.

Tuttavia, sebbene debba essere sempre verificata l'esistenza dell'interesse o vantaggio dell'ente, i Reati in questione sono ipotizzabili, almeno astrattamente, per il settore assicurativo, in quanto l'impresa di assicurazione riveste il ruolo di investitore istituzionale o, comunque, di investitore molto attivo, nonché elabora e diffonde studi, ricerche o raccomandazioni di tipo economico-finanziario.

Inoltre, anche in riferimento al tipo di Reati *de quibus* vanno anzitutto ricordati i vincoli e gli oneri che, in base alla disciplina di vigilanza, gravano sulle imprese di assicurazione per quanto concerne, tra l'altro, le informazioni contabili, le relazioni sull'andamento, le partecipazioni, la separazione di patrimoni o di classi di attivi, nonché per il rispetto del segreto professionale da parte dei dipendenti dell'impresa.

Il corretto e continuativo adempimento delle suddette disposizioni è senz'altro importante strumento di salvaguardia, ma non può considerarsi sufficiente ancorché ne sia aumentata la specifica attenzione.

Di seguito sono elencate le attività che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati di cui al D.Lgs. 231/2001:

- Gestione e divulgazione delle informazioni e delle comunicazioni verso l'esterno (a titolo esemplificativo ma non esaustivo IVASS, banche d'investimento, azionisti, giornalisti) o provenienti da fonti esterne, ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato;
- Impartizione di ordini di acquisto e/o di vendita.

## CAPITOLO E.3

## Regole e principi procedurali specifici

### E.3.1 Principi di comportamento

Obiettivo della presente Parte Speciale è che i Dipendenti e gli Organi Sociali – nei limiti delle rispettive competenze e nella misura in cui siano coinvolti nello svolgimento delle attività nelle Attività Sensibili individuate in precedenza – a regole di condotta conformi a quanto prescritto in tale Parte Speciale e nelle *policy* e procedure cui la stessa fa riferimento diretto o indiretto, al fine di prevenire la commissione dei Reati e illeciti Amministrativi di abuso di mercato.

In particolare, i soggetti destinatari della presente Parte Speciale dovranno attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati e illeciti Amministrativi di abuso di mercato;
2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato o di illecito amministrativo rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. adoperarsi affinché le comunicazioni all'esterno siano veritiere e corrette;
4. astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false o non corrette (anche mediante l'utilizzo di strumenti di intelligenza artificiale), idonee a provocare una sensibile alterazione del prezzo di strumenti finanziari quotati o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, codici di comportamento, *policy* e procedure aziendali.

Tali *policy* e procedure e loro eventuali successive integrazioni o modifiche si considerano parte integrante del Modello e, pertanto, si devono intendere come recepite nella loro configurazione.

### E.3.2 Regole comportamentali

Ai fini dell'attuazione delle regole elencate, devono altresì rispettarsi i seguenti principi riferibili alla Attività Sensibili di cui al precedente paragrafo E.2.

a. *Gestione e divulgazione delle informazioni e delle comunicazioni verso l'esterno (a titolo esemplificativo ma non esaustivo IVASS, banche d'investimento, azionisti, giornalisti) o provenienti da fonti esterne, ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato.*

Con riferimento a tale Attività Sensibile è espressamente vietato ai Destinatari di:

1) utilizzare o comunicare informazioni privilegiate relative a strumenti finanziari o emittenti strumenti finanziari, quotati, comunque ottenute (*i.e.* in qualsiasi modo e per qualsiasi via), anche al di fuori della propria attività lavorativa;

2) partecipare a gruppi di discussione o chat-room su internet aventi ad oggetto strumenti finanziari o emittenti strumenti finanziari, quotati e nei quali vi sia uno scambio di informazioni concernenti strumenti finanziari quotati, o società quotate in genere o strumenti finanziari emessi da tali soggetti, a meno che si tratti di incontri istituzionali per i quali è già stata compiuta una verifica di legittimità da parte delle funzioni competenti e/o non vi sia scambio di informazioni il cui carattere non privilegiato sia evidente;

3) sollecitare l'ottenimento di informazioni privilegiate su strumenti finanziari o emittenti strumenti finanziari quotati;

4) comunicare qualsiasi informazione all'interno della Società, dei comitati, degli organi sociali di tipo collegiale senza il puntuale e metodico rispetto della normativa vigente in materia di informazioni privilegiate;

5) lasciare documentazione contenente informazioni privilegiate in luoghi in cui potrebbe facilmente essere letta da persone che non sono autorizzate a conoscere tali informazioni secondo quanto previsto dalla normativa vigente;

6) effettuare comunicazioni all'esterno nel mancato rispetto delle procedure interne in materia e senza il preventivo coordinamento con le funzioni preposte a tale compito;

7) rivelare a terzi informazioni privilegiate (in qualunque modo siano state ottenute) relative a strumenti finanziari o emittenti strumenti finanziari, quotati o non quotati, se non nei casi in cui tale rivelazione sia richiesta da leggi, da altre disposizioni regolamentari o da specifici accordi contrattuali con cui le controparti si siano impegnate a utilizzare dette informazioni privilegiate esclusivamente per i fini per i quali dette informazioni sono trasmesse e a mantenere la riservatezza sulle stesse;

8) comunicare o diffondere all'esterno analisi o valutazioni su uno strumento finanziario quotato (o indirettamente sul suo emittente) che possano influenzare i terzi, dopo aver preso precedentemente posizione su tale strumento finanziario, beneficiando di conseguenza dell'impatto della valutazione diffusa sul prezzo di detto strumento, senza avere allo stesso tempo comunicato al pubblico, in modo corretto ed efficace, l'esistenza di tale conflitto di interesse;

9) diffondere informazioni di mercato false o fuorvianti tramite mezzi di comunicazione, compreso internet, o tramite qualsiasi altro mezzo;

10) diffondere al pubblico valutazioni o una notizia su uno strumento finanziario o un emittente senza prima aver verificato l'attendibilità e il carattere non privilegiato dell'informazione;

11) consigliare ai terzi operazioni di investimento sulla base delle informazioni privilegiate in loro possesso;

12) discutere di informazioni privilegiate in presenza di estranei o, comunque, soggetti non autorizzati a conoscere tali informazioni sulla base della normativa vigente;

13) discutere di informazioni privilegiate al telefono in luoghi pubblici ovvero in ufficio con la modalità "viva voce", onde evitare che informazioni privilegiate possano essere ascoltate da estranei o comunque da soggetti non autorizzati a conoscere tali informazioni secondo quanto previsto dalla normativa vigente.

*b. Impartizione di ordini di acquisto e/o di vendita.*

Con riferimento a tale Attività Sensibile è espressamente vietato ai Destinatari, direttamente o indirettamente, di:

1) agire consultandosi con altri soggetti per acquisire una posizione dominante sull'offerta o sulla domanda di uno strumento finanziario che abbia l'effetto di fissare, direttamente o indirettamente, i prezzi di acquisto o di vendita o determinare altre condizioni commerciali non corrette;

2) impartire ordini di compravendita di uno strumento finanziario nella consapevolezza di un conflitto di interessi (a meno che esso non venga esplicitato nelle forme previste dalla normativa), allorquando tale operazione non sarebbe stata ragionevolmente effettuata in caso di assenza di conflitto di interessi;

3) operare creando inusuali concentrazioni di operazioni in accordo con altri soggetti su un particolare strumento finanziario;

4) impartire operazioni che hanno la finalità di aggirare gli accorgimenti previsti dai meccanismi di negoziazione (ad esempio, con riferimento ai limiti quantitativi, ai parametri relativi al differenziale tra le proposte di acquisto e di vendita, ecc.);

5) impartire ordini di compravendita prima o dopo che la stessa società o soggetti ad essa collegati abbiano diffuso studi, ricerche o raccomandazioni di investimento errate o tendenziose o manifestamente influenzate da interessi rilevanti;

6) impartire ordini di acquisto di partecipazioni di un emittente appartenente al c.d. "mercato sottile" realizzando poi operazioni volte a farne aumentare i prezzi così da consentire di ottenere performance superiori al *benchmark* di riferimento;

7) aprire una posizione lunga su uno strumento finanziario ed effettuare ulteriori acquisti e/o diffondere fuorvianti informazioni positive sullo strumento finanziario in modo da aumentarne il prezzo;

8) prendere una posizione ribassata su uno strumento finanziario ed effettuare un'ulteriore attività di vendita e/o diffondere fuorvianti informazioni negative sullo strumento finanziario in modo da ridurne il prezzo;

9) aprire una posizione su un determinato strumento finanziario e chiuderla immediatamente dopo che la posizione stessa è stata resa nota al pubblico;

10) realizzare un'inusuale operatività sugli strumenti finanziari di una società emittente prima dell'annuncio di informazioni privilegiate relative alla società, a meno che tale operatività non sia basata solo su analisi di mercato, su informazioni non privilegiate ovvero su altre notizie pubblicamente disponibili;

11) realizzare operazioni che hanno la finalità di aumentare il prezzo di uno strumento finanziario nei giorni precedenti all'emissione di uno strumento finanziario derivato collegato o di uno strumento finanziario convertibile.

## CAPITOLO E.4

## I controlli dell'OdV e i flussi informativi

### E.4.1 Il controllo in generale

L'OdV effettua dei periodici controlli diretti a verificare il corretto adempimento da parte dei destinatari, come meglio individuati al Paragrafo E.3.1, nei limiti dei rispettivi compiti e attribuzioni, delle regole e principi contenuti nella presente Parte Speciale e nelle procedure aziendali cui la stessa fa esplicito o implicito richiamo.

A tal riguardo, è compito dell'Organismo di Vigilanza:

- proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati e degli illeciti amministrativi di cui alla presente Parte Speciale;
- monitorare il rispetto delle procedure interne per la prevenzione dei reati e illeciti amministrativi di abuso di informazioni privilegiate e di manipolazione di mercato;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Societari, da terzi o da qualsiasi Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Per i flussi informativi si rimanda alla compilazione da parte delle funzioni competenti delle "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento) che costituiscono un allegato al Modello.

**PARTE SPECIALE – F –**

**Reati di omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro**

**Definizioni**

Si rinvia alle definizioni di cui alla Parte Generale, fatte salve le ulteriori definizioni contenute nella presente Parte Speciale.

- **Datore di Lavoro o DdL**: il soggetto titolare del rapporto di lavoro con il Lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il Lavoratore presta la propria attività, ha la responsabilità, in virtù di apposita delega, dell'organizzazione stessa o del singolo settore in quanto esercita i poteri decisionali e di spesa.

- **D.Lgs. 81/2008**: il decreto legislativo 9 aprile 2008, n. 81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro" e successive modifiche e integrazioni.

- **DUVRI o Documento Unico di Valutazione dei Rischi per le Interferenze**: il documento redatto dal Datore di Lavoro committente contenente una valutazione dei rischi che indichi le misure per eliminare o, ove ciò non risulti possibile, ridurre al minimo i rischi da interferenze.

- **DVR**: il documento redatto dal Datore di Lavoro contenente una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa e i criteri per la suddetta valutazione, l'indicazione delle misure di prevenzione e protezione attuate e dei dispositivi di protezione individuali adottati a seguito di tale valutazione, il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, l'indicazione del nominativo del RSPP, del RLS e del Medico Competente che ha partecipato alla valutazione del rischio, nonché l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

- **Formazione:** processo educativo attraverso il quale trasferire ai lavoratori e agli altri soggetti del sistema di prevenzione e protezione aziendale conoscenze e procedure utili alla acquisizione di competenze per lo svolgimento in sicurezza dei rispettivi compiti in azienda e alla identificazione, alla riduzione e alla gestione dei rischi (Art. 2 comma 1, lett. aa) del D.Lgs. 81/2008).

- **Informazione:** complesso delle attività dirette a fornire conoscenze utili alla identificazione, alla riduzione e alla gestione dei rischi in ambiente di lavoro (Art. 2 comma 1, lett.bb) del D.Lgs. 81/2008).
- **Lavoratori**: persone che, indipendentemente dalla tipologia contrattuale, svolgono un'attività lavorativa nell'ambito dell'organizzazione della Società.
- **Medico Competente**: il medico in possesso di uno dei titoli e dei requisiti formali e professionali indicati nel D.Lgs. 81/2008 che collabora con il Datore di Lavoro ai fini della valutazione dei rischi e al fine di effettuare la Sorveglianza Sanitaria e adempiere tutti gli altri compiti di cui al D.Lgs. 81/2008.
- **Reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro:** i reati di cui all'art. 25-*septies* del D.Lgs. 231/2001, ovvero l'omicidio colposo (art. 589 c.p) e le lesioni personali gravi o gravissime (art. 590 terzo comma c.p.) commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.
- **RLS o Rappresentante dei Lavoratori per la Sicurezza**: il soggetto eletto o designato per rappresentare i Lavoratori in relazione agli aspetti della salute e sicurezza durante il lavoro.
- **RSPP o Responsabile del Servizio di Prevenzione e Protezione**: il soggetto in possesso delle capacità e dei requisiti professionali indicati nel D.Lgs. 81/2008, designato dal Datore di Lavoro, a cui risponde, per coordinare il Servizio di Prevenzione e Protezione.
- **Sorveglianza Sanitaria**: l'insieme degli atti medici finalizzati alla tutela dello stato di salute e sicurezza dei Lavoratori in relazione all'ambiente di lavoro, ai fattori di rischio professionali, e alle modalità di svolgimento dell'attività lavorativa.
- **SPP o Servizio di Prevenzione e Protezione**: l'insieme delle persone, sistemi e mezzi esterni o interni alla Società finalizzati all'attività di prevenzione e protezione dei rischi professionali per i Lavoratori.
- **SSL**: Salute e Sicurezza dei Lavoratori.

## CAPITOLO F.1

## Le fattispecie dei reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (Art. 25-*septies*, D.Lgs. 231/2001)

Si provvede qui di seguito a fornire una breve descrizione dei reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro indicati all'art. 25-*septies* del Decreto.

Tale articolo, originariamente introdotto dalla legge 3 agosto 2007, n. 123, e successivamente sostituito ai sensi dell'art. 300 del D.Lgs. 81/2008, prevede l'applicazione di sanzioni pecuniarie e interdittive agli Enti i cui esponenti commettano i reati di cui agli artt. 589 (omicidio colposo) e 590 terzo comma (lesioni personali colpose gravi o gravissime) c.p., in violazione delle norme sulla tutela della salute e sicurezza sul lavoro. Le fattispecie delittuose inserite all'art. 25-*septies* riguardano unicamente le ipotesi in cui l'evento sia stato determinato non già da colpa di tipo generico (e dunque per imperizia, imprudenza o negligenza) bensì da "colpa specifica", ovverosia allorquando l'evento si sia verificato a causa della inosservanza delle norme sulla salute e sicurezza sul lavoro.

### OMICIDIO COLPOSO (ART. 589, COMMA 2, C.P.)

Il reato si configura ogni qualvolta un soggetto cagioni per colpa la morte di altro soggetto con violazione delle norme per la prevenzione degli infortuni sul lavoro.

### LESIONI PERSONALI COLPOSE GRAVI O GRAVISSIME (ART. 590, COMMA 3, C.P.)

Il reato si configura ogni qualvolta un soggetto, in violazione delle norme per la prevenzione degli infortuni sul lavoro, cagioni per colpa ad altro soggetto lesioni gravi o gravissime.

Si precisa che, ai sensi del comma 1 dell'art. 583 c.p., la lesione è considerata grave nei seguenti casi:

"*1) se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;*

*2) se il fatto produce l'indebolimento permanente di un senso o di un organo*".

Ai sensi del comma 2 dell'art. 583 c.p., la lesione è considerata invece gravissima se dal fatto deriva:

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

Al fine di garantire l'adozione di un valido presidio avverso la potenziale commissione dei Reati di cui all'art. 25-*septies* del Decreto, la Società ha deciso di dotarsi anche della presente Parte Speciale, in conformità a quanto disposto dall'art. 30 del D.Lgs. 81/2008.

Ai sensi del suddetto articolo "*in sede di prima applicazione i modelli di organizzazione aziendale definiti conformemente alle Linee Guida Uni-Inail per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti*"[6].

A tal proposito appare opportuno sottolineare che la Società ha predisposto un sistema di gestione della sicurezza sul lavoro ("**SGSL**") certificato allo standard ISO 45001 e, congiuntamente al presente Modello, costituisce un presidio conforme alle previsioni dell'art. 30 D.Lgs. 81/2008 e idoneo ad avere efficacia esimente della responsabilità amministrativa della Società.

[6] Per quanto concerne il riferimento al British Standard OHSAS 18001:2007, lo stesso è ora, per espressa previsione normativa, da intendersi operato allo standard di cui alla norma UNI ISO 45001.

## CAPITOLO F.2

### Attività Sensibili nell'ambito dei reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Partendo dall'assunto che tutte le aree e tutti gli ambienti fisici nei quali si svolge attività lavorativa per l'impresa in rapporto di dipendenza o di collaborazione, nonché le attività lavorative esterne svolte per conto dell'impresa, sono esposti al rischio infortunistico, si pone l'accento sulle attività di verifica degli adempimenti richiesti dalle normative in materia di salute e sicurezza nei luoghi di lavoro, nonché sulla predisposizione delle procedure informative relative alla gestione delle strutture (locali, arredi, macchine server e apparecchiature informatiche, ecc.) e sulla valutazione sanitaria degli ambienti di lavoro.
Di seguito sono elencate le attività che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati di cui al D.Lgs. 231/2001:

- adempimento degli obblighi normativi in materia di salute e sicurezza nei luoghi di lavoro;
- selezione e gestione degli appaltatori e subappaltatori.

## CAPITOLO F.3

## Regole e principi procedurali specifici

### F.3.1 Principi di comportamento nell'ambito dei reati in materia di salute e sicurezza nei luoghi di lavoro

Al fine di consentire l'attuazione dei principi finalizzati alla protezione della salute e della sicurezza dei Lavoratori così come individuati dall'art. 15 del D.Lgs. 81/2008 e in ottemperanza a quanto previsto dagli artt. 18, 19 e 20 del medesimo decreto si prevede quanto segue.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, i Destinatari del Modello sono tenuti, in generale, a conoscere e rispettare tutte le regole e i princìpi contenuti nei seguenti documenti:

a) organigramma aziendale;

b) CCNL;

c) DUVRI/DVR con i relativi documenti integrativi;

d) il SGSL e ogni procedura operativa o organizzativa in materia di salute e sicurezza sul lavoro.

La presente Parte Speciale prevede a carico dei Destinatari di cui sopra, in considerazione delle diverse posizioni e dei diversi obblighi che ciascuno di essi assume nei confronti della Società nell'ambito dell'espletamento delle attività considerate a rischio, l'espresso divieto di porre in essere, promuovere, collaborare, o dare causa a comportamenti tali da integrare fattispecie di Reati commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

### F.3.2 La politica per la sicurezza sul lavoro

La politica di sicurezza e salute sul lavoro (SSL) costituisce un riferimento fondamentale ed essenziale per tutti i partecipanti alla vita aziendale e per tutti coloro che, esterni all'azienda, hanno con essa rapporti.

Essa deve far comprendere, declinando anche gli obiettivi strategici, i principi cui si ispira ogni azione aziendale, nell'ottica della salute e sicurezza e benessere di tutti i partecipanti alla vita aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo e alle responsabilità assunte in azienda.

Il documento di politica indica in sostanza quale "missione" si è data l'azienda in tema di SSL, esprimendo le motivazioni che stanno alla base, la ferma volontà del vertice aziendale a perseguire gli obiettivi posti, la consapevolezza dei risultati auspicati cui tendere, le responsabilità da assumere.

Il successo di questa politica per la Sicurezza e la Salute sarà ottenuto con le azioni che seguono:

- la direzione aziendale si impegna affinché sia considerato una priorità il rispetto della legislazione vigente in materia di salute e sicurezza sul lavoro;
- la direzione aziendale si impegna nel recepimento di considerazioni attinenti alla sicurezza e la salute nelle decisioni economiche e nelle attività che la riguardano;
- la direzione aziendale tiene sotto controllo ciò che può pregiudicare la sicurezza, impegnandosi a far fronte con rapidità ed efficacia a necessità emergenti nel corso delle attività lavorative e a privilegiare le azioni preventive e le indagini interne a tutela della sicurezza e salute dei lavoratori, in modo da ridurre significativamente le probabilità di accadimento di incidenti, infortuni o altre non conformità;
- la direzione aziendale provvede affinché sia svolta una regolare manutenzione e pulitura dei luoghi, delle attrezzature, degli impianti e dei dispositivi di sicurezza e di protezione, in modo da salvaguardare la salute e la sicurezza dei lavoratori, dei terzi e più in generale della comunità in cui l'azienda opera;
- la direzione aziendale si impegna ad accertare le capacità degli addetti prima di affidare un incarico che comporti pericolo per la propria e l'altrui sicurezza, sviluppando ed erogando preventivamente programmi di addestramento e formazione che permettano ai lavoratori di identificare e gestire correttamente i rischi per la Sicurezza e la Salute, assicurare l'integrità dei beni e prevenire malattie professionali e infortuni nell'ambiente di lavoro; la formazione, l'informazione, l'addestramento e la sensibilizzazione sui rischi di cui sopra sono diffusi a tutti i lavoratori e ne viene gestito l'aggiornamento, il tutto con specifico riferimento alla mansione svolta dai singoli lavoratori stessi;
- la direzione aziendale mette a disposizione mezzi, tecnologie e sistemi per lavorare in sicurezza, istruendo i lavoratori all'impegno ad agire in spirito di collaborazione con i propri colleghi per salvaguardare la propria e l'altrui salute;

- la direzione aziendale si impegna a garantire la consultazione dei lavoratori, anche attraverso il rappresentante dei lavoratori per la sicurezza, in merito agli aspetti della sicurezza e salute sul lavoro; si impegna altresì a coinvolgere l'intera struttura aziendale affinché essa partecipi, secondo le proprie attribuzioni e competenze, al raggiungimento degli obiettivi di sicurezza assegnati;

- la direzione aziendale si impegna affinché siano riesaminati periodicamente la Politica, gli Obiettivi e l'attuazione del SGSL, allo scopo di ottenere un miglioramento continuo del livello di sicurezza e salute sul lavoro in azienda.

**F.3.3 Il processo di pianificazione**

Al fine di dare concreta attuazione alla politica di SSL ogni attività aziendale è analizzata, tenendo conto di tutte le possibili condizioni, e vengono definiti degli obiettivi coerenti con la politica di SSL, all'interno di uno specifico piano nell'ambito del SGSL.

La pianificazione costituisce uno dei cardini fondamentali del sistema.

Essa consente inoltre di avere esatta conoscenza dei compiti che sono affidati a ciascuno e delle relative responsabilità.

Primi elementi considerati nella pianificazione delle attività per la SSL sono l'individuazione dei requisiti legali cui l'azienda deve attenersi e l'individuazione dei pericoli per la SSL, la valutazione del rischio e il controllo del rischio.

La Società, con cadenza periodica:

- definisce gli obiettivi finalizzati al mantenimento e/o miglioramento delle misure di prevenzione e protezione così come l'adeguamento della struttura alla normativa applicabile;

- individua le figure/strutture coinvolte nel raggiungimento dei suddetti obbiettivi e l'attribuzione dei relativi compiti e responsabilità;

- definisce le risorse, anche economiche, necessarie;

- prevede le modalità di verifica dell'effettivo ed efficace raggiungimento degli obiettivi.

**F.3.2 Compiti e responsabilità**

Nella definizione dei compiti organizzativi ed operativi devono essere esplicitati e resi noti anche quelli relativi alle attività di sicurezza di loro competenza, nonché le responsabilità

connesse all'esercizio delle stesse e i compiti di ispezione, verifica e sorveglianza in materia di SSL.

L'attribuzione di compiti e responsabilità compete esclusivamente al Datore di Lavoro, fatti salvi i limiti previsti dalle norme di legge.

Si riportano qui di seguito gli adempimenti che, in attuazione dei principi sopra descritti e della normativa applicabile, sono posti a carico delle figure rilevanti e fungono da presidio alle Attività Sensibili indicate al par. F.2.1.

**Il Datore di Lavoro**

Al Datore di Lavoro della Società sono attribuiti tutti gli obblighi in materia di salute e sicurezza sul lavoro, tra cui i seguenti **compiti non delegabili** ai sensi dell'art. 17 del D.Lgs. 81/2008:

1) valutare tutti i rischi per la sicurezza e per la salute dei lavoratori ed elaborare, all'esito di tale valutazione, un DVR (da custodirsi presso l'azienda) contenente tra l'altro:

   - una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante il lavoro, nella quale siano specificati i criteri adottati per la valutazione stessa;
   - l'indicazione delle eventuali misure di prevenzione e di protezione attuate e degli eventuali dispositivi di protezione individuale adottati a seguito della suddetta valutazione dei rischi (artt. 74 - 79 D.Lgs. 81/2008);
   - il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
   - l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere;
   - l'indicazione del nominativo del RSPP, del RLS e del Medico Competente che abbiano partecipato alla valutazione del rischio.

   L'attività di valutazione e di redazione del documento deve essere compiuta in collaborazione con il RSPP e con il Medico Competente. La valutazione dei rischi è oggetto di consultazione preventiva con il Rappresentante dei Lavoratori per la Sicurezza;

2) designare il Responsabile del Servizio di Prevenzione e Protezione dai rischi.

Al Datore di Lavoro sono attribuiti numerosi altri **compiti** dallo stesso **delegabili** a soggetti qualificati. Tali compiti, sono previsti dall'art. 18 del D.Lgs. 81/2008 e riguardano, tra l'altro: a) la nomina del Medico Competente per l'effettuazione della Sorveglianza Sanitaria; b) l'individuazione (tramite apposito atto di nomina) del preposto/preposti per l'effettuazione delle attività di vigilanza di cui all'art. 19 del D.Lgs. 81/2008; c) la designazione preventivamente dei 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 delle emergenze; d) l'adempimento degli obblighi di informazione, formazione e addestramento; e) la convocazione della riunione periodica di cui all'art. 35 D.Lgs. 81/2008; f) l'aggiornamento delle misure di prevenzione in relazione ai mutamenti organizzativi che hanno rilevanza ai fini della salute e sicurezza del lavoro, ecc.

Al fine di garantire l'attuazione di un modello di sicurezza aziendale sinergico e compartecipativo, il Datore di Lavoro fornisce al Servizio di Prevenzione e Protezione e al Medico Competente informazioni in merito a:

- la natura dei rischi;
- l'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive;
- la descrizione dei luoghi di lavoro;
- i dati relativi agli infortuni e quelli relativi alle malattie professionali.

Il Datore di Lavoro è tenuto a svolgere attività formativa nella materia in oggetto secondo quanto stabilito dall'Accordo Stato-Regioni attuativo della normativa in materia di salute e sicurezza sul lavoro.

**Il Delegato**

In relazione ai compiti delegabili da parte del Datore di Lavoro, la relativa delega nei confronti del Delegato è ammessa, ai sensi dell'art. 16 del D.Lgs. 81/2008, con i seguenti limiti e condizioni:

- che essa risulti da atto scritto recante data certa;
- che il Delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;

- che essa attribuisca al Delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;
- che essa attribuisca al Delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate;
- che la delega sia accettata dal Delegato per iscritto.

Ai sensi del comma 2 dell'art. 16 del D.Lgs. 81/2008 è, inoltre, previsto che alla delega debba essere data adeguata e tempestiva pubblicità.

I Delegati possono a loro volta, previa intesa con il Datore di Lavoro delegante, sub-delegare specifiche funzioni in materia di salute e sicurezza sul lavoro alle medesime condizioni di cui sopra. Siffatta sub-delega di funzioni non esclude l'obbligo di vigilanza in capo al delegante in ordine al corretto espletamento delle funzioni trasferite. Il soggetto al quale sia conferita tale sub-delega non può, a sua volta, delegare le funzioni delegate.

**Il Servizio di Prevenzione e Protezione (SPP)**

Nell'adempimento degli obblighi in materia di salute e sicurezza sul lavoro, il Datore di Lavoro si avvale, ricorrendo anche a soggetti esterni alla Società, del Servizio di Prevenzione e Protezione dei rischi professionali che provvede:

- 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;
- ad elaborare, per quanto di competenza, le misure preventive e protettive a seguito della valutazione dei rischi e i sistemi di controllo di tali misure;
- ad elaborare le linee guida, alert e indicazioni operative relative alle varie attività aziendali;
- a proporre attività di informazione e formazione dei Lavoratori;
- a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro nonché alla riunione periodica di cui all'art. 35, D.Lgs. 81/2008;
- a fornire ai Lavoratori ogni informazione in tema di tutela della salute e sicurezza sul lavoro che si renda necessaria.

Qualora nell'espletamento dei relativi compiti, il RSPP della Società verificasse la sussistenza di eventuali criticità nell'attuazione delle azioni di recupero prescritte dal Datore di Lavoro, il RSPP coinvolto dovrà darne immediata comunicazione all'OdV.

L'eventuale sostituzione del RSPP dovrà altresì essere comunicata all'OdV con l'espressa indicazione delle motivazioni a supporto di tale decisione.

Il RSPP deve avere le capacità e i requisiti professionali in materia di prevenzione e sicurezza che sono specificamente indicati dall'art. 32 del D.Lgs. 81/2008 e che sono accertati dal Datore di Lavoro prima della nomina attraverso documentazione che ne comprovi il possesso.

Il RSPP è coinvolto regolarmente ed è invitato alle riunioni dell'OdV relativamente alle materie di sua competenza.

**Il Medico Competente**

Il Medico Competente provvede tra l'altro a:

- collaborare con il Datore di Lavoro e con il Servizio di Prevenzione e Protezione alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della Sorveglianza Sanitaria, alla predisposizione della attuazione delle misure per la tutela della salute e dell'integrità psicofisica dei lavoratori e all'attività di formazione e informazione nei loro confronti, per la parte di competenza considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro;
- programmare ed effettuare la Sorveglianza Sanitaria;
- istituire, aggiornare e custodire sotto la propria responsabilità una cartella sanitaria e di rischio per ogni Lavoratore sottoposto a Sorveglianza Sanitaria;
- fornire informazioni ai lavoratori sul significato degli accertamenti sanitari a cui sono sottoposti e informandoli sui relativi risultati;
- comunicare per iscritto in occasione della riunione periodica di cui all'art. 35 D.Lgs. 81/2008 i risultati anonimi collettivi della Sorveglianza Sanitaria effettuata, fornendo indicazioni sul significato di detti risultati ai fini dell'attuazione delle misure per la tutela della salute e della integrità psicofisica dei lavoratori;
- visitare gli ambienti di lavoro almeno una volta l'anno o a cadenza diversa in base alla valutazione di rischi.

Il Medico Competente deve essere in possesso di uno dei titoli *ex* art. 38, D.Lgs. 81/2008, che vengono accertati dal Datore di Lavoro prima di provvedere alla relativa nomina.

**Il Rappresentante dei Lavoratori per la Sicurezza (RLS)**

È il soggetto eletto o designato, in conformità a quanto previsto dagli accordi sindacali in materia, per rappresentare i lavoratori per gli aspetti di salute e sicurezza sui luoghi di lavoro.

Il RLS riceve, a cura del Datore di Lavoro o di un suo delegato, la prevista formazione specifica in materia di salute e sicurezza.

Il RLS:

- accede ai luoghi di lavoro;
- è consultato preventivamente e tempestivamente in merito alla valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive;
- è consultato sulla designazione del RSPP e degli incaricati dell'attuazione delle misure di emergenza e di pronto soccorso e del Medico Competente;
- è consultato in merito all'organizzazione delle attività formative;
- promuove l'elaborazione, l'individuazione a l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei lavoratori;
- partecipa alla "riunione periodica di prevenzione e protezione dai rischi";
- riceve informazioni inerenti la valutazione dei rischi e le misure di prevenzione relative e, ove ne faccia richiesta e per l'espletamento della sua funzione, copia del DVR e del DUVRI.

Il RLS dispone del tempo necessario allo svolgimento dell'incarico, senza perdita di retribuzione, nonché dei mezzi necessari per l'esercizio delle funzioni e delle facoltà riconosciutegli; non può subire pregiudizio alcuno a causa dello svolgimento della propria attività e nei suoi confronti si applicano le stesse tutele previste dalla legge per le rappresentanze sindacali.

**I Lavoratori**

È cura di ciascun Lavoratore – come, peraltro, chiaramente indicato dall'art. 20 del D.Lgs. 81/2008 – porre attenzione alla propria sicurezza e salute e a quella delle altre persone

presenti sul luogo di lavoro su cui possono ricadere gli effetti delle sue azioni ed omissioni, in relazione alla formazione e alle istruzioni ricevute e alle dotazioni fornite.

I Lavoratori devono in particolare:

- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro o dal suo Delegato ai fini della protezione collettiva e individuale;
- utilizzare correttamente le apparecchiature da lavoro nonché gli eventuali dispositivi di sicurezza, ove presenti;
- segnalare immediatamente al Datore di Lavoro o ai soggetti incaricati le deficienze dei mezzi e dispositivi dei punti precedenti, nonché le altre eventuali condizioni di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli;
- non rimuovere né modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- partecipare ai programmi di formazione e di addestramento organizzati dal Datore di Lavoro;
- sottoporsi ai controlli sanitari previsti nei loro confronti;
- contribuire, insieme al Datore di Lavoro o al suo Delegato all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

I lavoratori di aziende che svolgono per la Società attività in regime di appalto e subappalto devono esporre apposita tessera di riconoscimento.

### F.3.4.2 Informazione e formazione

**Informazione**

Il SGSL deve definire e mantenere attive le modalità per assicurare che il personale sia ad ogni livello consapevole:

- dell'importanza della conformità delle proprie azioni rispetto alla politica e ai requisiti del SGSL;
- delle conseguenze che la loro attività ha nei confronti della SSL;

- delle possibili conseguenze dovute a uno scostamento da quanto fissato in materia di SSL.

Ciò premesso, il Datore di Lavoro è responsabile dell'informazione, della formazione e dell'addestramento dei Lavoratori, nonché dell'informazione delle persone presenti od operanti nell'insediamento, mentre il RSPP è responsabile di proporre i Piani di informazione e formazione dei Lavoratori.

L'informazione che la Società riserva ai Destinatari deve essere facilmente comprensibile e deve consentire agli stessi di acquisire la necessaria consapevolezza in merito a:

a) le conseguenze derivanti dallo svolgimento della propria attività non conformemente alle regole adottate dalla Società in tema di salute e sicurezza sul lavoro;

b) il ruolo e le responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità con la politica aziendale e le procedure in materia di sicurezza e ogni altra prescrizione relativa al sistema di salute e sicurezza sul lavoro adottato dalla Società, nonché ai principi indicati nella presente Parte Speciale.

Pertanto, la Società, in considerazione dei diversi ruoli, responsabilità e capacità e dei rischi cui è esposto ciascun Lavoratore, cura che:

- i Lavoratori siano sensibilizzati in merito al tema della sicurezza con continuità e periodicità attraverso apposite riunioni periodiche;
- sia fornita adeguata informazione ai Lavoratori e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro., ecc.) circa i rischi specifici dell'impresa, per quanto limitati, sulle conseguenze di questi e sulle misure di prevenzione e protezione adottate;
- sia data evidenza dell'informativa erogata in merito alla gestione del pronto soccorso, emergenza, evacuazione e prevenzione incendi e siano verbalizzati gli eventuali incontri;
- sia fornita informazione ai Lavoratori e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro.) sulla presenza di delegati e subdelegati per la SSL, sulla nomina del RSPP, sul Medico Competente e sugli addetti ai compiti specifici per il pronto soccorso, salvataggio, evacuazione e prevenzione incendi;
- sia formalmente documentata l'informazione e l'istruzione per l'uso delle attrezzature di lavoro messe a disposizione dei Lavoratori;

- il RSPP e/o il Medico Competente sia/siano coinvolto/i nella definizione delle informazioni;

Di tutta l'attività di informazione sopra descritta deve essere data evidenza su base documentale.

**Formazione**

Datore di Lavoro[7] e dirigenti ai sensi dell'art. 2 del D.Lgs. 81/2008 sono tenuti a frequentare appositi corsi di formazione.

In relazione alla formazione, La Società cura che:

- sia fornita adeguata formazione a tutti i Lavoratori in materia di sicurezza sul lavoro;
- il RSPP e/o il Medico Competente partecipino alla stesura del piano di formazione;
- la formazione erogata preveda questionari di valutazione;
- la formazione sia adeguata ai rischi della mansione cui il Lavoratore è in concreto assegnato;
- gli addetti a specifici compiti in materia di prevenzione e protezione (addetti prevenzione incendi, addetti all'evacuazione, addetti al pronto soccorso) ricevano specifica formazione;
- vengano effettuate periodiche esercitazioni di evacuazione.

Tutta l'attività di formazione sopra descritta deve essere ripetuta periodicamente e della stessa deve essere data evidenza su base documentale.

### F.3.4.3 Comunicazione, flusso informativo e cooperazione

L'organizzazione razionalizzata del flusso informativo deve essere tale da consentire il trasferimento delle informazioni utili attraverso comunicazioni pluridirezionali, mirate e sintetiche, in grado di rendere partecipi tutti i Lavoratori, per la parte di loro interesse ai fini della SSL, sull'evoluzione delle proprie attività.

Il flusso è quindi biunivoco:

- verticale: dall'alta dirigenza verso la base e viceversa;

[7] Come anticipato sopra, l'attività formativa nei confronti del Datore di Lavoro nella materia in oggetto viene svolta secondo quanto stabilito dall'Accordo Stato-Regioni attuativo della normativa in materia di salute e sicurezza sul lavoro.

- orizzontale: da responsabile di processo a responsabile di processo, da lavoratore a lavoratore.

La cooperazione nasce dalla conoscenza delle altrui esigenze e dalla necessità di trovare le sinergie necessarie alla crescita comune.

Non va poi trascurata la comunicazione da e verso l'esterno, nella consapevolezza che l'azienda vive ed opera in un contesto sociale.

Al fine di dare maggior efficacia al sistema organizzativo adottato per la gestione della sicurezza e quindi alla prevenzione degli infortuni sul luogo di lavoro, la Società si organizza per garantire un adeguato livello di circolazione e condivisione delle informazioni tra tutti i Lavoratori.

A tal proposito la Società adotta un sistema di comunicazione interna che prevede due differenti tipologie di flussi informativi:

*a) dal basso verso l'alto*

Il flusso dal basso verso l'alto è garantito dalla Società ricevendo da parte dei Lavoratori segnalazioni, osservazioni, proposte ed esigenze di miglioria inerenti alla gestione della sicurezza in ambito aziendale; Tali segnalazioni vengo portate a conoscenza da parte dei Lavoratori ai propri superiori in linea gerarchica affinché siano trasmesse al Datore di Lavoro o al suo Delegato.

*b) dall'alto verso il basso*

Il flusso dall'alto verso il basso ha lo scopo di diffondere a tutti i Lavoratori la conoscenza del sistema adottato dalla Società per la gestione della sicurezza nel luogo di lavoro.

A tale scopo la Società garantisce ai Destinatari un'adeguata e costante informativa attraverso la predisposizione di comunicati da diffondere internamente e l'organizzazione di incontri periodici che abbiano ad oggetto:

- eventuali nuovi rischi in materia di salute e sicurezza dei Lavoratori;
- modifiche nella struttura organizzativa adottata dalla Società per la gestione della salute e sicurezza dei Lavoratori;
- contenuti delle procedure aziendali adottate per la gestione della sicurezza e salute dei Lavoratori;
- ogni altro aspetto inerente alla salute e alla sicurezza dei Lavoratori.

*c) comunicazione esterna: suddivisa in passiva e attiva.*

Passiva – Ogni rilievo, osservazione, richiesta, ecc. proveniente dall'esterno e relativa a temi di SSL deve essere convogliata al RSGSL attraverso i suoi assistenti o, in caso di sua assenza, ai Dirigenti presenti in azienda. Se si tratta di richiesta verbale deve essere tradotta in forma scritta dal ricevente.

Ogni richiesta deve essere archiviata.

Attiva - È responsabilità del Datore di Lavoro e riguarda essenzialmente:

- la politica e l'impegno dell'azienda verso la SSL;
- i risultati e i miglioramenti conseguiti;
- specifiche iniziative (ad esempio iniziative a premio, fabbriche aperte, ecc.).

I mezzi utilizzati possono comprendere:

- la diffusione di comunicati aziendali;
- articoli sulla rete intranet aziendale.

Tra i soggetti destinatari si possono individuare almeno:

- il personale esterno (committenti, Fornitori, collaboratori esterni);
- il pubblico (clienti e soggetti interessati).

**Documentazione**

Per documentazione della sicurezza si intende sia la documentazione del SGSL che la documentazione di SSL.

Pur avendo stabilito una distinzione tra i documenti della sicurezza, scorporandoli in quelli di tipo volontario (SGSL) e in quelli di tipo cogente (SSL), è possibile che taluni di questi siano difficilmente attribuibili in modo univoco all'uno o all'altro tipo, dal momento che possono contemplare temi od argomenti relativi ad obblighi di legge, ma al contempo essere anche conformati secondo regole di natura volontaria.

Il criterio seguito per la distinzione dei documenti si è basato sul fatto di preminenza della natura del contenuto.

Pur essendo possibile che alcune delle seguenti documentazioni elencate siano archiviate all'interno del SGSL per i motivi di sovrapposizione citati, a livello esemplificativo la documentazione di SSL comprende:

- leggi, regolamenti, norme antinfortunistiche attinenti all'attività dell'azienda;
- regolamenti e accordi aziendali;
- documentazione richiesta dalla normativa vigente in materia di SSL (esempio: DVR con relative parti integranti, elenco delle sostanze pericolose, rapporto di analisi delle esposizioni al rumore e alle vibrazioni, valutazioni di rischio specifiche, CPI, verbali ispettivi e manutentivi periodici obbligatori, comunicazioni obbligatorie sulla sicurezza agli Organismi di Vigilanza, verbali prescrittivi degli Organismi di Vigilanza, certificati e cartelle sanitarie emessi dal Medico Competente, ecc.);
- documentazione fornita dai costruttori (esempio: manuali, istruzioni per l'uso di macchine, attrezzature e DPI, schede tecniche delle sostanze pericolose utilizzate);
- informazioni sui processi produttivi.

In ogni caso, la Società dovrà provvedere alla conservazione, sia su supporto cartaceo che informatico, i seguenti documenti:

- la cartella sanitaria, la quale deve essere istituita e aggiornata dal Medico Competente e custodita dal Datore di Lavoro;
- il DVR che indica la metodologia con la quale si è proceduto alla valutazione dei rischi e contiene il programma delle misure di mantenimento e di miglioramento.

La Società è altresì chiamata a garantire che:

- il RSPP, il Medico Competente, gli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, vengano nominati formalmente;
- venga data evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate dal RSPP e dal Medico Competente;
- venga adottato e mantenuto aggiornato il registro delle pratiche delle malattie professionali riportante data, malattia, data emissione certificato medico e data inoltro della pratica;
- venga conservata la documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti all'attività aziendale;
- vengano conservati, ove previsti, i manuali e le istruzioni per l'uso di macchine, attrezzature ed eventuali dispositivi di protezione individuale forniti dai costruttori;

- venga conservata ogni procedura adottata dalla Società per la gestione della salute e sicurezza sui luoghi di lavoro;
- tutta la documentazione relativa alle attività di informazione e formazione venga conservata a cura del RSPP e messa a disposizione dell'OdV.

**F.3.5 Integrazione nei processi aziendali e gestione operativa**

Il successo di un SGSL sta nella sua piena integrazione con il sistema di pianificazione, azione e controllo più generale dell'azienda, nel senso che ogni processo, ogni procedura deve contemplare gli aspetti di SSL.

Ciò in linea con la politica generale dell'azienda di cui la "politica" per la SSL è parte integrante e determinante e con gli obiettivi strategici verso cui è proiettata.

Questa impostazione porta ad una continua revisione e aggiornamento, in tal senso, delle analisi dei processi e procedure, della definizione dei compiti e responsabilità e dei rilevamenti connessi al controllo operativo.

**F.3.6 L'attività di controllo – monitoraggio.**

Il monitoraggio costituisce una fase fondamentale del sistema perché consente ad ogni operatore, prima di ogni altro, di tenere sotto controllo la propria attività, riscontrando eventuali anomalie rispetto agli standard di processo, non solo in termini di SSL ma anche in termini produttivi e qualitativi.

La conoscenza degli eventuali scostamenti dagli obiettivi pianificati può evidenziare le eventuali carenze e far comprendere dove e come intervenire per assicurare il raggiungimento degli obiettivi preposti.

La Società deve assicurare un controllo periodico delle misure di prevenzione e protezione adottate sui luoghi di lavoro.

A tale scopo la Società:

- assicura un controllo periodico delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro;
- assicura un controllo periodico dell'adeguatezza e della funzionalità di tali misure a raggiungere gli obiettivi prefissati e della loro corretta applicazione;

- compie approfondita analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere.

Il monitoraggio si pone l'obiettivo di misurare in modo affidabile e ripetibile il funzionamento del SGSL, in tutte le sue parti componenti, nonché il miglioramento o il mantenimento delle condizioni di SSL.

Il monitoraggio di 1° livello ha lo scopo di tenere sotto controllo le misure preventive e protettive predisposte dall'azienda in materia di SSL.

Il monitoraggio di 2° livello ha lo scopo di stabilire se il sistema è conforme a quanto pianificato e consente di raggiungere gli obiettivi, e se è correttamente applicato e mantenuto attivo.

Al fine di adempiere adeguatamente all'attività di controllo ora descritta, la Società, laddove la specificità del campo di intervento lo richiedesse, farà affidamento a risorse esterne con elevato livello di specializzazione.

La Società garantisce che gli eventuali interventi correttivi necessari (cosiddette "non conformità"), vengano predisposti nel più breve tempo possibile.

**F.3.7 Gli interventi successivi alle attività di controllo**

Al termine di detta attività di controllo di cui al precedente paragrafo, la Società pianifica gli interventi necessari per eliminare le criticità rilevate, al fine di accertare che il sistema di salute e sicurezza sia adeguatamente attuato e siano raggiunti gli obiettivi prefissati.

Il corretto trattamento delle non conformità costituisce l'indispensabile presupposto al funzionamento nel tempo del SGSL.

Le non conformità riscontate nel monitoraggio di 1° livello richiedono un intervento più o meno immediato per il ripristino delle condizioni corrette, sia da parte dell'operatore, se questo rientra nelle sue competenze e capacità, sia da parte del superiore gerarchico.

Le non conformità riscontrate nel monitoraggio previsto dalle procedure o istruzioni di SSL richiedono l'immediata segnalazione al superiore gerarchico per l'opportuno intervento per la rimozione del problema tecnico o organizzativo riscontrato.

Le non conformità riscontrate nel monitoraggio di 2° livello richiedono un riesame della correttezza delle procedure o istruzioni di SSL, della loro effettiva applicazione e delle azioni

di informazione, formazione e sensibilizzazione attuate, anche per l'applicazione dei provvedimenti correttivi previsti

## CAPITOLO F.4

### I contratti di appalto

La Società disciplina, tramite apposita documentazione, la gestione, le attività da svolgere e le responsabilità dei soggetti coinvolti in ambito di salute e sicurezza sul lavoro, nel caso di affidamento di lavori in appalto, o prestazione d'opera, o somministrazione (escluse le mere forniture di materiali o attrezzature).

Le modalità di gestione e di coordinamento dei lavori in appalto devono essere formalizzate in contratti scritti nei quali siano presenti espressi riferimenti agli adempimenti di cui all'art. 26, D.Lgs. 81/2008. Al riguardo, è necessario:

- verificare l'idoneità tecnico-professionale delle imprese appaltatrici in relazione ai lavori da affidare in appalto attraverso i) acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato ii) acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico professionale ai sensi dell'art. 4, D.P.R. 28 dicembre 2000, n. 445;
- fornire informazioni dettagliate agli appaltatori circa gli eventuali rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- evitare qualsiasi ingerenza nell'organizzazione del lavoro dell'appaltatore, assicurando che quest'ultimo mantenga piena autonomia nella gestione delle risorse, dei mezzi e delle modalità esecutive della prestazione, nonché nella pianificazione dei tempi e nell'organizzazione delle attività, nel rispetto degli obblighi contrattuali assunti;
- cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
- coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori;
- predisporre un unico DVR che indichi le misure adottate al fine di eliminare, o quanto meno ridurre al minimo, i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva (cosiddetto DUVRI); tale documento deve allegarsi al contratto di appalto o d'opera. Tale adempimento non è necessario in caso di appalto di servizi di natura intellettuale, di

mere forniture di materiali o attrezzature nonché di lavori o servizi la cui durata non sia superiore ai due giorni.

Nei contratti di somministrazione, di appalto e di subappalto, devono essere specificamente indicati i costi relativi alla sicurezza del lavoro. A tali dati può accedere, su richiesta, il Rappresentante per la Sicurezza dei Lavoratori.

Nei contratti di appalto deve essere chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto (che deve essere preventivamente approvato dalla Società).

L'imprenditore committente risponde in solido con l'appaltatore, nonché con ciascuno degli eventuali ulteriori subappaltatori, per tutti i danni per i quali il lavoratore, dipendente dall'appaltatore o dal subappaltatore, non risulti indennizzato ad opera dell'Istituto nazionale per l'assicurazione contro gli infortuni sul lavoro.

La Società si riserva, anche per il tramite di apposite clausole contrattuali, di svolgere specifiche verifiche (in autonomia o mediante terzi) presso gli appaltatori e subappaltatori. Tali verifiche avranno ad oggetto anche il rispetto dei princìpi previsti dalla presente Parte Speciale e dalla Parte Speciale D relativa ai reati contro la personalità individuale e l'impiego di cittadini di paesi terzi il cui soggiorno è irregolare. Nel caso di riscontrate non conformità, la Società potrà dare al Fornitore il tempo necessario per porre in essere le azioni di rimedio ovvero fornire la documentazione necessaria. Le conseguenze della mancata ottemperanza devono essere formalizzate nei relativi contratti.

***

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, codici di comportamento, policy e procedure aziendali.

Tali *policy* e procedure e loro eventuali successive integrazioni o modifiche si considerano parte integrante del Modello e, pertanto, si devono intendere come recepite nella loro configurazione.

## CAPITOLO F.5

### I controlli dell'OdV e i flussi informativi

Fermo restando il potere discrezionale dell'OdV di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute (per le quali si rinvia a quanto esplicitato nella Parte Generale), l'OdV può:

a. partecipare agli eventuali incontri organizzati dalla Società tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;

b. accedere a tutta la documentazione aziendale disponibile in materia di SSL.

La Società istituisce altresì a favore dell'Organismo di Vigilanza flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli infortuni, delle criticità nonché notizie di eventuali malattie professionali accertate o presunte.

L'Organismo di Vigilanza, nell'espletamento delle attività di cui sopra, può avvalersi di tutte le risorse competenti in azienda (ad esempio: il Delegato *ex* art. 16 del D.Lgs. 81/2008, il RSPP; il Rappresentante dei Lavoratori per la Sicurezza; il Medico Competente; gli incaricati dell'attuazione delle misure di emergenza e primo soccorso; ecc.) e organizzare specifici incontri con le stesse.

Per i flussi informativi si rimanda alla compilazione da parte delle funzioni competenti delle "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento) che costituiscono un allegato al Modello.

**PARTE SPECIALE – G –**

**Delitti informatici e in materia di violazione del diritto d'autore**

## CAPITOLO G.1

### G.1.1. Le fattispecie dei delitti informatici e (art. 24-*bis* del Decreto 231) e dei delitti in materia di violazione del diritto d'autore (art. 25-*novies* del Decreto 231)

La presente Parte Speciale si riferisce ai delitti informatici e (art. 24-*bis,* di seguito, per brevità, i "**Delitti Informatici**") in materia di violazione del diritto d'autore introdotti dalla Legge 99/2009 tra i reati presupposto sanzionabili ai sensi del Decreto 231 (art. 25-*novies*).

A tal riguardo si sottolinea che, nonostante le due tipologie di reati tutelino interessi giuridici differenti, si è ritenuto opportuno trattarli un'unica Parte Speciale in quanto:

- entrambe le fattispecie presuppongono un corretto utilizzo delle risorse informatiche;
- le Attività Sensibili risultano, in virtù di tale circostanza, in parte sovrapponibili;
- i principi procedurali mirano, in entrambi i casi, a garantire la sensibilizzazione dei Destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

Si provvede a descrivere qui di seguito le fattispecie di reato punibili ai sensi dell'art. 24-bis del Decreto 231 e ritenute, a seguito dell'analisi dei rischi, astrattamente applicabili alla Società.

### G.1.2.Delitti informatici

***FALSITÀ IN DOCUMENTI INFORMATICI (ART. 491-BIS C.P.)***

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti, tra i quali rientrano sia le falsità ideologiche che le falsità materiali in atti pubblici sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico.

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

Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, comma 1, lett. p), D.Lgs. 82/2005, salvo modifiche ed integrazioni).

A titolo esemplificativo, integrano il delitto di falsità in documenti informatici la condotta di inserimento fraudolento di dati falsi nelle banche dati pubbliche oppure la condotta dell'addetto alla gestione degli archivi informatici che proceda, deliberatamente, alla modifica di dati in modo da falsificarli.

Inoltre, il delitto potrebbe essere integrato tramite la cancellazione o l'alterazione di informazioni a valenza probatoria presenti sui sistemi dell'ente, allo scopo di eliminare le prove di un altro reato.

***ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (ART. 615-TER C.P.)***

Tale reato si realizza quando un soggetto "*abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto ad escluderlo*".

La pena è aumentata:

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 totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

La pena è aumentata anche qualora il delitto in oggetto riguardi 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.

Il delitto di accesso abusivo al sistema informatico rientra tra i delitti contro la libertà individuale. Il bene che viene protetto dalla norma è il domicilio informatico seppur vi sia chi sostiene che il bene tutelato è, invece, l'integrità dei dati e dei programmi contenuti nel sistema informatico. L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema.

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

Il delitto di accesso abusivo a sistema informatico si integra, ad esempio, nel caso in cui un soggetto accede abusivamente ad un sistema informatico e procede alla stampa di un documento contenuto nell'archivio del PC altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).

Il delitto potrebbe essere astrattamente commesso da parte di qualunque dipendente della Società accedendo abusivamente ai sistemi informatici di proprietà di terzi (*outsider hacking*), ad esempio, per prendere cognizione di dati riservati di un'impresa concorrente, ovvero tramite la manipolazione di dati presenti sui propri sistemi come risultato dei processi di business allo scopo di produrre un bilancio falso o, infine, mediante l'accesso abusivo a sistemi aziendali protetti da misure di sicurezza, da parte di utenti dei sistemi stessi, per attivare servizi non richiesti dalla clientela.

### *DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE, CODICI E ALTRI MEZZI ATTI ALL'ACCESSO A SISTEMI INFORMATICI O TELEMATICI (ART. 615-*QUATER *C.P.)*

Tale reato si realizza quando un soggetto, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

La pena è aumentata se il danno 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.

Il legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accessi abusivi a sistemi informatici. Per mezzo dell'art. 615-*quater* c.p., pertanto, sono punite le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.

I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, *password* o schede informatiche (ad esempio, *badge*, carte di credito, bancomat e *smart card*).

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

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

Risponde, ad esempio, del delitto di diffusione abusiva di codici di accesso, il dipendente della Società autorizzato ad un certo livello di accesso al sistema informatico che ottenga illecitamente il livello di accesso superiore, procurandosi codici o altri strumenti di accesso mediante lo sfruttamento della propria posizione all'interno della Società oppure carpisca in altro modo fraudolento o ingannevole il codice di accesso.

***INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-QUATER C.P.)***

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

La norma tutela la libertà e la riservatezza delle comunicazioni informatiche o telematiche durante la fase di trasmissione al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi.

La fraudolenza consiste nella modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione.

Perché possa realizzarsi questo delitto è necessario che la comunicazione sia attuale, vale a dire in corso, nonché personale ossia diretta ad un numero di soggetti determinati o determinabili (siano essi persone fisiche o giuridiche). Nel caso in cui la comunicazione sia

rivolta ad un numero indeterminato di soggetti la stessa sarà considerata come rivolta al pubblico.

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

Il reato si integra, ad esempio, con il vantaggio concreto dell'ente, nel caso in cui un dipendente esegua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di un concorrente.

***DENTENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE E DI ALTRI MEZZI ATTI A INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-*QUINQUIES *C.P.)***

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

La condotta vietata dall'art. 617-*quinquies* è, pertanto, costituita dalla detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi, a prescindere dalla circostanza che le stesse siano o meno utilizzate. Si tratta di un reato che mira a prevenire quello precedente di intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche.

Anche la semplice installazione di apparecchiature idonee all'intercettazione viene punita dato che tale condotta rende probabile la commissione del reato di intercettazione. Ai fini della condanna il giudice dovrà, però, limitarsi ad accertare se l'apparecchiatura installata abbia, obbiettivamente, una potenzialità lesiva.

Qualora all'installazione faccia seguito anche l'utilizzo delle apparecchiature per l'intercettazione, interruzione, impedimento o rivelazione delle comunicazioni, si applicheranno nei confronti del soggetto agente, qualora ricorrano i presupposti, più fattispecie criminose.

Il reato si integra, ad esempio, a vantaggio dell'ente, nel caso in cui un dipendente, direttamente o mediante conferimento di incarico ad un investigatore privato (se privo delle necessarie autorizzazioni) si introduca fraudolentemente presso la sede di un concorrente o di un cliente insolvente al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche. Così come per la fattispecie, dianzi analizzata, di cui all'art. 617-*quater* c.p., la pena è aumentata:

1) se il fatto è commesso in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente esercizi pubblici o di pubblica necessità;
2) se il fatto è commesso da un pubblico ufficiale o da un incaricato di 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) se il fatto è commesso da chi esercita, anche abusivamente, la professione di investigatore privato.

***ESTORSIONE INFORMATICA (ART. 629, COMMA 3, C.P.)***

Il reato di "estorsione informatica" punisce chiunque, mediante le condotte di cui agli articoli 615-*ter*, 617-*quater*, 617-*sexies*, 635-*bis*, 635-*quater* e 635-*quinquies* c.p. ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

***DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (ART. 635-BIS C.P.)***

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

La pena aumentata se il fatto è commesso con violenza alla persona o con minaccia o se è commesso abusando della qualità di operatore del sistema.

Il reato, ad esempio, si integra nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

Il danneggiamento potrebbe essere commesso a vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano

poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento delle obbligazioni da parte del fornitore.

***DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI PUBBLICI O DI INTERESSE PUBBLICO (ART. 635-TER C.P.)***

Tale reato si realizza quando un soggetto "*commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici 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 aumentata nelle seguenti ipotesi:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di 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 minaccia o violenza ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.

Questo delitto si distingue da quello dianzi analizzato poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati alla soddisfazione di un interesse di natura pubblica.

Perché il reato si integri è sufficiente che si tenga una condotta finalizzata al deterioramento o alla soppressione del dato.

***DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (ART. 635-QUATER C.P.)***

Questo reato di realizza quando un soggetto "*mediante le condotte di cui all'art. 635-bis (danneggiamento di dati, informazioni e programmi informatici), ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento*".

La pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema.

Si tenga conto che qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-*bis*.

Il reato si integra in caso di danneggiamento o cancellazione dei dati o dei programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio, attraverso l'inserimento nel sistema di un *virus*).

***DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO (ART. 635-QUATER.1 C.P.)***

Tale reato si realizza qualora qualcuno, "*allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero 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, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici*".

Questo delitto è integrato, ad esempio, nel caso in cui ci si procuri un virus idoneo a danneggiare un sistema informatico o qualora si producano o si utilizzino delle smart card che consentono il danneggiamento di apparecchiature o di dispositivi elettronici.

Tali condotte sono punibili nel caso in cui un soggetto persegua lo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati oppure i programmi in essi contenuti o, ancora, miri a favorirne l'interruzione parziale o totale o l'alterazione del funzionamento. Ciò si verificherebbe, ad esempio, qualora un dipendente introducesse un virus idoneo a danneggiare o a interrompere il funzionamento del sistema informatico di un concorrente.

***DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICO INTERESSE (ART. 635-QUINQUIES C.P.)***

Questo reato si configura nei confronti di chiunque "mediante le condotte di cui *all'art. 635-quater (Danneggiamento di sistemi informatici o telematici) ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare, rendere, in tutto o in parte*

*inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento*".

La pena è aumentata nelle seguenti ipotesi:

a) 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;
b) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;
c) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblico interesse, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità (art. 635-*ter*), quel che rileva è che il sistema sia utilizzato per il perseguimento di pubblico interesse indipendentemente dalla proprietà privata o pubblica del sistema stesso.

Il reato si può configurare nel caso in cui un Dipendente cancelli file o dati, relativi ad un'area per cui sia stato abilitato ad operare, per conseguire vantaggi interni (ad esempio, far venire meno la prova del credito da parte di un ente o di un fornitore) ovvero che l'amministratore di sistema, abusando della sua qualità, ponga in essere i comportamenti illeciti in oggetto per le medesime finalità già descritte.

### G.1.3. Delitti in materia di violazione del diritto d'autore

La Legge 23 luglio 2009, n. 99, introducendo nell'ambito del Decreto 231 l'art 25-*novies* concernente i "*delitti in materia di violazione del diritto d'autore",* ha esteso la responsabilità amministrativa degli enti anche ai reati di cui alla Legge 22 aprile 1941, n. 633 relativa alla protezione del diritto d'autore e di altri diritti connessi al suo esercizio (di seguito "*Legge sul Diritto d'Autore*").

Si provvede a descrivere qui di seguito le fattispecie di reato punibili ai sensi dell'art. 25-*novies* del Decreto 231 e ritenute, a seguito dell'analisi dei rischi e suggerimenti, *prima facie* applicabili alla Società.

***DIVULGAZIONE TRAMITE RETI TELEMATICHE DI UN'OPERA DELL'INGEGNO PROTETTA (art. 171 comma 1 lett. a-bis e comma 3. Legge sul Diritto d'Autore)***

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

(i) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa;

(ii) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore o alla reputazione dell'autore.

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

Tale reato potrebbe ad esempio essere commesso nell'interesse della Società qualora venissero caricati sulla rete aziendale dei contenuti coperti dal diritto d'autore affinché gli stessi potessero essere utilizzati nell'ambito dell'attività lavorativa.

***DUPLICAZIONE, A FINI DI LUCRO, DI PROGRAMMI INFORMATICI O IMPORTAZIONE, DISTRIBUZIONE, VENDITA, DETENZIONE PER FINI COMMERCIALI DI PROGRAMMI CONTENUTI IN SUPPORTI NON CONTRASSEGNATI DALLA SIAE O DA ALTRI ORGANISMI DI GESTIONE COLLETTIVA OVVERO DA ENTITÀ DI GESTIONE INDIPENDENTI (art. 171-bis Legge sul Diritto d'Autore)***

La norma in esame è volta a tutelare il corretto utilizzo dei *software* e delle banche dati.

Per ciò che concerne i *software*, è prevista la rilevanza penale dell'abusiva duplicazione nonché dell'importazione, distribuzione, vendita e detenzione a scopo commerciale o imprenditoriale e locazione di programmi "pirata".

Il reato in ipotesi si configura nel caso in cui 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 SIAE o da altri organismi di gestione collettiva o da entità di gestione indipendenti.

Il fatto è punito anche se la condotta ha ad oggetto 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.

Il secondo comma della stessa norma punisce inoltre chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE o da altri organismi di gestione collettiva o da entità di gestione indipendenti, riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui alla Legge sul Diritto d'Autore.

Sul piano soggettivo, per la configurabilità del reato è sufficiente lo scopo di lucro, sicché assumono rilevanza penale anche tutti quei comportamenti che non sono sorretti dallo specifico scopo di conseguire un guadagno di tipo prettamente economico (come nell'ipotesi dello scopo di profitto).

Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora venissero utilizzati, per scopi lavorativi, programmi non originali ai fine di risparmiare il costo derivante dalla licenza per l'utilizzo di un *software* originale.

***DUPLICAZIONE, RIPRODUZIONE, TRASMISSIONE – PER USO NON PERSONALE E A SCOPO DI LUCRO – DI UN'OPERA DELL'INGEGNO DESTINATA AL CIRCUITO TELEVISIVO, CINEMATOGRAFICO, DELLA VENDITA O DEL NOLEGGIO (art. 171-ter Legge sul Diritto d'Autore)***

La lunga disposizione tende alla tutela di una serie numerosa di opere dell'ingegno: opere destinate al circuito radiotelevisivo e cinematografico, incorporate in supporti di qualsiasi tipo contenenti fonogrammi e videogrammi di opere musicali, ma anche opere letterarie, scientifiche o didattiche.

A restringere l'ambito di applicabilità della disposizione, però, vi sono due requisiti.

Il primo è che le condotte siano poste in essere per fare un uso non personale dell'opera dell'ingegno, e il secondo è il dolo specifico di lucro, necessario per integrare il fatto tipico.

## CAPITOLO G.2

### G.2.1 Attività Sensibili nell'ambito dei delitti informatici

A seguito di una approfondita analisi della realtà aziendale, le principali Attività Sensibili che la Società ha individuato al proprio interno riguardano il corretto utilizzo e l'idonea protezione dei sistemi informatici, come di seguito indicate:

a) strutturazione del sistema informatico aziendale, gestione ed evoluzione della piattaforma tecnologica e applicativa *IT* e pianificazione della sicurezza informatica;

b) utilizzo della rete aziendale, del servizio di posta elettronica e accesso ad *internet*;

c) gestione di informazioni, dati e programmi informatici e della documentazione informatica (anche nei rapporti con la pubblica amministrazione).

### G.2.2. Attività Sensibili nell'ambito dei delitti in violazione del diritto d'autore

In relazione ai delitti in violazione del diritto d'autore, sono state individuate le seguenti Attività Sensibili:

a) utilizzo degli applicativi informatici aziendali, in considerazione del potenziale utilizzo senza licenza di *software* coperti da altrui diritto d'autore;

b) gestione dei contenuti multimediali sulla rete aziendale e in particolare sul sito internet aziendale, in considerazione, tra l'altro, del possibile illegittimo utilizzo all'interno di quest'ultimo di composizioni musicali, immagini o altre opere dell'ingegno coperte da altrui diritto d'autore;

c) riproduzione, duplicazione e divulgazione di opere dell'ingegno coperte dal diritto d'autore.

## CAPITOLO G.3

### Regole e principi generali

Obiettivo della presente Parte Speciale è che i Dipendenti, gli Organi Sociali e i soggetti che operano a livello periferico (Consulenti, service provider ecc.) nella misura in cui gli stessi possano essere coinvolti nelle Attività Sensibili, si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire e impedire il verificarsi dei Delitti Informatici e di Delitti in violazione del Diritto d'Autore.

Nell'espletamento delle attività aziendali e, in particolare, nelle Attività Sensibili, è espressamente vietato ai soggetti sopra indicati, anche in relazione al tipo di rapporto posto in essere con la Società, di porre in essere, collaborare o dare causa alla realizzazione di comportamenti, anche omissivi, tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente Parte Speciale (art. 24-*bis* e 25-*novies* del Decreto).

In particolare non è ammesso:

- porre in essere quei comportamenti che (i) integrano le fattispecie di reato o, (ii) sebbene non costituiscano di per sé un'ipotesi di reato, possano esserne il presupposto (ad esempio, mancato controllo);
- divulgare informazioni relative ai sistemi informatici aziendali che possano rivelare carenze e/o modalità di utilizzo distorte e non consentite degli stessi;
- utilizzare i sistemi informatici della Società per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico e al presente Modello;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di terze parti, comprensivo di archivi, dati e programmi;
- installare autonomamente nel PC in dotazione per uso aziendale *software* non autorizzati dalla Società;
- utilizzare illecitamente materiale tutelato da altrui diritto d'autore.

Nell'espletamento delle rispettive attività/funzioni oltre alle regole di cui al Modello e alla presente Parte Speciale, i Destinatari sono tenuti a conoscere e osservare tutte le regole e i principi contenuti nelle procedure aziendali relative a:

- gestione degli accessi logici a reti, sistemi, dati e applicazioni,
- gestione delle credenziali personali (*username* e *password*); e
- corretta gestione delle informazioni di cui si viene a conoscenza per ragioni operative;
- sicurezza informatica.

Al fine di mitigare il rischio di commissione dei Delitti Informatici e dei Delitti in violazione del Diritto d'Autore e, di conseguenza, anche di assicurare il corretto adempimento degli obblighi connessi alla normativa di riferimento, la Società, in relazione alle operazioni inerenti lo svolgimento della propria attività, assolve i seguenti adempimenti:

1. fornisce, ai Destinatari, un'adeguata informazione circa il corretto utilizzo degli strumenti informatici aziendali e delle credenziali d'accesso per accedere ai principali sottosistemi informatici utilizzati presso la Società;
2. limita, attraverso abilitazioni di accesso differenti, l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;
3. effettua, per quanto possibile, nel rispetto della normativa sulla *privacy*, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare fenomeni anomali sulla rete aziendale;
4. predispone e mantiene adeguate difese fisiche a protezione dei *server* della Società;
5. predispone e mantiene adeguate difese, fisiche e logiche, a protezione degli ulteriori sistemi informatici aziendali;
6. effettua periodici inventari dei *software* e delle banche dati in uso presso l'azienda e verifica che l'utilizzo degli stessi sia legittimato da apposita licenza;
7. effettua, per quanto possibile, controlli periodici sui contenuti del sito *internet* aziendale.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, codici di comportamento, policy e procedure aziendali.

Tali *policy* e procedure e loro eventuali successive integrazioni o modifiche si considerano parte integrante del Modello e, pertanto, si devono intendere come recepite nella loro configurazione.

## CAPITOLO G.4

### Principi procedurali specifici

Ai fini dell'attuazione delle regole e del rispetto dei divieti elencati nel precedente Capitolo, devono essere ottemperati i principi procedurali qui di seguito descritti, oltre alle Regole e ai Principi Generali già contenuti nella Parte Generale del presente Modello.

In particolare, si descrivono qui di seguito le regole che devono essere rispettate dai destinatari della presente Parte Speciale, meglio individuati nel Capitolo precedente, nell'ambito delle Attività Sensibili.

### G.4.1. Principi procedurali specifici relativi ai Delitti Informatici

1. *Strutturazione del sistema informatico aziendale, gestione ed evoluzione della piattaforma tecnologica e applicativa IT e pianificazione della sicurezza informatica*

   a. La Società si è dotata di una struttura di sistemi informatici e telematici nonché di sicurezza informatica e *governance* dei dati, presidiata da specifiche funzioni aziendali, nell'ambito delle quali sono stati assegnati specifici ruoli e responsabilità;
   b. La Società adotta un piano nel quale sono specificate le attività di strutturazione, monitoraggio, difesa del patrimonio informatico e telematico aziendale. In particolare:
      - sono stati stabiliti e prefissati i requisiti dei sistemi ICT;
      - sono stati identificati i soggetti che utilizzano e hanno accesso agli stessi;
      - sono state quantificate le risorse economiche e finanziarie da assegnare alla gestione e sviluppo della struttura stessa;
      - sono previste attività di manutenzione e di evoluzione degli strumenti informatici e telematici aziendali;
      - sono stati adottati sistemi di protezione da eventuali accessi esteri e da eventuali manomissioni da parte degli utenti interni;
      - sono state stabilite e divulgate le regole di utilizzo degli strumenti informatici aziendali;
      - sono previste le attività relative alla sicurezza e alla mitigazione dei rischi connessi alla gestione dei sistemi, con particolare riferimento ai temi della *cybersecurity*, in conformità con le disposizioni di cui al Regolamento IVASS n. 38/2018.
   c. La Società declina quanto previsto dal suddetto piano,

- definendo risorse, tempi e livelli di qualità per ogni progetto;
- selezionando i Fornitori esterni più adatti ai requisiti stabiliti per ogni progetto e controllandone l'operato;
- monitorando avanzamenti e criticità.

d. Con particolare riferimento alla struttura informatica aziendale, le procedure aziendali vietano agli utenti, *inter alia*, di:
   - modificare, salvo particolari eccezioni, la configurazione di postazioni di lavoro fisse o mobili, senza l'autorizzazione di amministratori di sistema o della funzione competente;
   - utilizzare strumenti *software* e/o *hardware* che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le *password*, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.);
   - ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla Società;
   - effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici della compagnia o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi;
   - divulgare a soggetti terzi le proprie credenziali di accesso per l'utilizzo dei sistemi informatici aziendali;
   - comunicare a persone non autorizzate, interne o esterne alla Società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
   - navigare in siti *internet* per ragioni non attinenti allo svolgimento delle mansioni assegnate.

e. La Società ha adottato i seguenti presidi volti ad evitare che il sistema informatico aziendale sia strumentalizzato per la commissione di delitti informatici:
   - le postazioni informatiche sono impostate in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;

- il processo di abilitazione, disabilitazione, modifica e sospensione delle utenze è regolato da apposita procedura e prevede la collaborazione, a livello informativo, della funzione Risorse Umane, *Property* e *Mobility Management*;
- gli accessi alla stanza *server* sono consentiti unicamente al personale autorizzato;
- per quanto possibile, ogni sistema informatico societario è protetto dall'illecita installazione di dispositivi *hardware* in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;
- è previsto un procedimento di autenticazione mediante *username* e *password* al quale corrisponde un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei Dipendenti e degli altri soggetti eventualmente autorizzati;
- è previsto che le *password* utilizzate per l'accesso ai sistemi informatici aziendali debbano rispettare determinati requisiti e ne è richiesta la modifica periodica;
- sono previsti sistemi di blocco automatico delle utenze in caso di ripetuti tentativi di accesso nei sistemi informatici aziendali con credenziali errate;
- tutti gli accessi ai sistemi aziendali sono tracciati tramite specifici file di *log*;
- viene limitato l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Dipendenti e degli altri soggetti eventualmente autorizzati;
- viene verificata periodicamente la corrispondenza tra i *software* installati nei singoli sistemi informatici aziendali e il numero di licenze ottenute per il relativo utilizzo;
- vengono regolarmente e periodicamente effettuati gli aggiornamenti e gli interventi evolutivi e di potenziamento necessari a garantire la sicurezza dei sistemi informatici in uso.

f. Con particolare riferimento ai temi della *cybersecurity*, la Società:

- diffonde la cultura della sicurezza informatica, effettuando campagne di sensibilizzazione degli utenti, (consistenti, ad esempio, in corsi *online*, distribuzione di materiale informativo, sessioni di aggiornamento in occasione di sessioni di formazione);
- individua la figura dell'ITSO (*Information Technology Security Officer*), che in stretto coordinamento con il CISO di Gruppo garantisce gli standard di *cybersecurity*

richiesti dal Gruppo, gestendo e implementando i presìdi di sicurezza informatica necessari;

- garantisce la segregazione dei servizi gestiti in ambito informatico.

g. Nei rapporti contrattuali con i service provider e le società di *software house*, la Società:
   - prevede una dettagliata descrizione delle funzionalità e dei requisiti tecnici dei software commissionati;
   - richiede che sia garantita la sicurezza dei dati gestiti dal *software* o in *outsourcing* dal service *provider*;
   - richiede che sia mantenuta assoluta riservatezza sui sistemi informatici forniti e sulle relative credenziali di accesso;
   - vieta che il sistema informatico aziendale sia strumentalizzato per il compimento di reati informatici;
   - prevede la risoluzione immediata della Società dal contratto qualora vengano poste in essere azioni che possano, direttamente o indirettamente, configurare un delitto informatico o esporre la Società a tale rischio.

h. La Società sensibilizza i propri Dipendenti e i soggetti terzi eventualmente autorizzati all'utilizzo degli strumenti informatici e dei dispositivi portatili aziendali attraverso le seguenti azioni:
   - viene fatto sottoscrivere ai Dipendenti e agli altri soggetti eventualmente autorizzati uno specifico documento con il quale gli stessi si impegnano al corretto utilizzo delle risorse informatiche aziendali;
   - le regole comportamentali di utilizzo degli strumenti informatici e dei dispositivi portatili aziendali sono riassunte in un'apposita procedura;
   - ai Dipendenti che operano su sistemi aziendali di *Partner* (ad esempio, quelli dell'intermediario bancario) viene fatta sottoscrivere una specifica informativa sul corretto utilizzo degli stessi;
   - i Dipendenti e gli altri soggetti eventualmente autorizzati sono informati, tramite sessioni formative o comunicazioni interne, in merito alla necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;

- i Dipendenti e gli altri soggetti eventualmente autorizzati vengono informati dell'importanza di mantenere i propri codici di accesso (*username* e *password*) confidenziali e di non divulgare gli stessi a soggetti terzi;
- i Dipendenti vengono richiamati periodicamente in modo inequivocabile, anche attraverso apposita attività di formazione, ad un corretto utilizzo degli strumenti informatici in proprio possesso.

2. *Utilizzo della rete aziendale, del servizio di posta elettronica e accesso ad internet*

   a. La Società si è dotata di procedure volte a disciplinare l'utilizzo della rete aziendale, con particolare riferimento al servizio di posta elettronica e all'accesso a *internet*. In particolare, tali procedure prevedono:
      - disposizioni specifiche in merito agli usi consentiti della rete *Internet* aziendale e della posta elettronica messa a disposizione;
      - il divieto di divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso alla rete aziendale o di clienti o di terze parti;
      - il divieto di distorcere, oscurare sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti *virus* o altri programmi in grado di danneggiare o intercettare dati.

   b. La Società, al fine di prevenire il rischio di strumentalizzazione della rete aziendale per la commissione di delitti informatici ha adottato i seguenti presidi:
      - l'accesso da e verso l'esterno (connessione alla rete *Internet*) viene fornito esclusivamente ai sistemi informatici dei Dipendenti o di eventuali soggetti terzi che ne abbiano la necessità ai fini lavorativi o connessi all'amministrazione societaria;
      - ogni postazione informatica viene fornita di adeguato *software* e *antivirus;* sono inoltre presenti sistemi *firewall*;
      - fa in modo che, ove possibile, i *software* di sicurezza informatica (*antivirus* e *firewall*) non possano essere disattivati dagli utenti;
      - viene limitato l'accesso alle aree e ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (*virus*) capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti;

- viene mantenuta traccia di tutti gli accessi effettuati alla rete aziendale e in particolare dei siti internet consultati attraverso file di *log*;
- qualora per la connessione alla rete *Internet* si utilizzino collegamenti *wireless* (ossia senza fili, mediante *routers* dotati di antenna *WiFi*), gli stessi vengono protetti impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete Internet tramite i *routers* della stessa e compiere illeciti ascrivibili ai Dipendenti;
- vengono effettuate, qualora le esigenze lo richiedano, in presenza di accordi sindacali che autorizzino in tale senso e ove possibile ai sensi di legge, controlli *ex ante* ed *ex post*, in forma aggregata e senza identificazione dell'utente, sulle attività effettuate dal personale sulle reti.

3. *Gestione di informazioni, dati e programmi informatici e della documentazione informatica (anche nei rapporti con la pubblica amministrazione)*

   a. Al fine di consentire una corretta gestione dei dati aziendali la Società ha previsto quanto segue:
      - l'istituzione di un comitato *Data Governance*;
      - la predisposizione di una Politica di *Data Governance* e *Data Quality*;
      - il monitoraggio dei dati aziendali da parte delle funzioni competenti;
      - l'adozione di adeguati presidi volti a prevenire il rischio di manipolazione di dati informatici e assicurare quindi la correttezza, veridicità e accuratezza dei dati.

   b. In particolare, la Società ha adottato procedure volte a disciplinare il corretto utilizzo da parte dei Dipendenti e dei soggetti terzi autorizzati dei dati informatici. In particolare tali procedure prevedono:
      - che i dati e le informazioni non pubbliche, relative anche a clienti e terze parti (commerciali, organizzative, tecniche), incluse le credenziali di accesso ai sistemi informatici aziendali, devono essere gestiti come riservati;
      - il divieto di accedere ad un sistema informatico altrui (anche di un collega) e di manomettere o alterarne i dati ivi contenuti;
      - il divieto di installazione e di utilizzo, sui sistemi informatici della Società, di *software* (c.d. "P2P", di *files sharing* o di *istant messaging*) mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni

tipologia di file (quali filmati, documenti, canzoni, *virus*, ecc.) senza alcuna possibilità di controllo da parte della Società.

c. La Società, al fine di garantire che eventuali malfunzionamenti improvvisi dei sistemi aziendali non danneggino o determinino la perdita dei dati informatici aziendali:
   - adotta piani di *Business Continuity* e *Disaster Recovery*;
   - prevede la revisione e l'aggiornamento degli stessi;
   - sensibilizza gli *outsourcer* in merito alla tematica in oggetto.

### G.4.2. Principi procedurali specifici relativi ai delitti in materia di violazione del diritto d'autore

Si elencano qui di seguito le regole che devono essere rispettate dai destinatari della presente Parte Speciale, meglio individuati nel Capitolo precedente, nell'ambito delle Attività Sensibili relative ai delitti in materia di violazione del diritto d'autore.

1. *Utilizzo degli applicativi informatici aziendali, in considerazione del potenziale utilizzo senza licenza di* software *coperti da altrui diritto d'autore*

   a. le attività di installazione, gestione e monitoraggio delle licenze *software* acquistate dalla Società sono state affidate a specifica funzione;
   b. tale funzione verifica periodicamente la corrispondenza tra le banche dati e i software in uso rispetto ai relativi termini e condizioni di licenza.

2. *Gestione dei contenuti multimediali sulla rete aziendale e in particolare sul sito internet aziendale, in considerazione, tra l'altro, del possibile illegittimo utilizzo all'interno di quest'ultimo di composizioni musicali, immagini o altre opere dell'ingegno coperte da altrui diritto d'autore*

   a. la Società, anche tramite i propri Consulenti, effettua ricerche di anteriorità sui contenuti e i materiali che intende pubblicare sul sito internet e su altri canali (come i social media) e che potrebbero essere protetti dall'altrui diritto d'autore;
   b. la Società provvede a disciplinare attraverso procedure o policy aziendali le modalità attraverso le quali modificare il sito internet aziendale. In particolare tali procedure o policy aziendali:
      - indicano specificatamente le aree aziendali coinvolte nella modifica del sito internet aziendale;
      - prevedono che l'accesso al sito Internet aziendale a fini di modifica sia attuabile solo in possesso di specifiche *password* a tale scopo generate;
      - prevedono verifiche periodiche in merito all'eventuale pubblicazione sul proprio sito internet aziendale di materiale non lecito.
   c. La Società si impegna, inoltre, a fornire alle figure aziendali interessate adeguata informazione circa le potenziali rischiosità in materia di responsabilità amministrativa degli enti connesse all'attività di configurazione del sito internet aziendale.

3. *Riproduzione, duplicazione e divulgazione di opere dell'ingegno coperte dal diritto d'autore*

   a. A tutti i Dipendenti è fatto divieto di:

- utilizzare immagini, video, composizioni musicali, banche dati ovvero qualsiasi opera dell'ingegno protetta dal diritto d'autore senza aver ottenuto le necessarie licenze e permessi;
- utilizzare immagini, video o composizioni musicali al fine di pubblicizzare o promuovere prodotti assicurativi al di fuori delle attività svolte dalla funzione Commerciale e Marketing e dalla funzione Comunicazione;
- riprodurre opere dell'ingegno (quali, ad esempio, libri o manuali) se non nei limiti del 15% per sola finalità di agevolare la lettura e l'esame delle tematiche ivi trattate.

b. I contenuti di articoli o altri contributi per riviste o testate giornalistiche predisposti da Dipendenti o Esponenti Aziendali su tematiche che coinvolgono o sono di interesse per la Società vengono verificati da più funzioni (compresa la funzione *Compliance*) prima della relativa pubblicazione.
c. Tutti i Dipendenti devono essere sensibilizzati sui rischi legati all'utilizzo di opere protette dal diritto d'autore.

## CAPITOLO G.5

## I controlli dell'OdV e i flussi informativi

### G.5.1 Il controllo in generale

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'art. 24-*bis* e all'art. 25-*novies,* D.Lgs. 231/2001 sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare regolarmente la sua efficacia a prevenire la commissione dei delitti di cui all'art. 24-*bis* e all'art. 25-*novies* del Decreto 231; con riferimento a tale punto, l'OdV conduce controlli a campione sulle attività potenzialmente a rischio di Delitti Informatici e Delitti in violazione del Diritto d'Autore, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;
- proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei Delitti Informatici e dei Delitti in violazione del Diritto d'Autore di cui alla presente Parte Speciale, anche in considerazione del progresso e dell'evoluzione delle tecnologie informatiche;
- proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Attività Sensibili individuate nella presente Parte Speciale;
- monitorare il rispetto delle procedure e la documentazione interna per la prevenzione dei Delitti Informatici e dei Delitti in violazione del Diritto d'Autore in costante coordinamento con le funzioni IT, *Infrastructure e Digital innovation*, *IT Security* e *Data Governance*, Commerciale e *Marketing*, Comunicazione, *Compliance* e *Internal Audit,* e con il *comitato Data Governance*; a tal fine, l'OdV invita periodicamente a relazionare i relativi responsabili alle proprie riunioni;
- esaminare le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari o opportuni;
- conservare traccia dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti.

A tal fine, all'OdV, viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Per i flussi informativi si rimanda, in particolare, alla compilazione da parte delle funzioni

competenti delle "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento) che costituiscono un allegato al Modello.

**PARTE SPECIALE – H –**

**Delitti di criminalità organizzata**

## CAPITOLO H.1

### Le fattispecie dei delitti di criminalità organizzata (art. 24-*ter* Decreto 231)

La legge 15 luglio 2009 n. 94, recante disposizioni in materia di sicurezza pubblica ha introdotto nel Decreto 231 l'art. 24-*ter* (di seguito i "**Delitti di Criminalità Organizzata**") che richiama le seguenti fattispecie criminose:

- "*associazione per delinquere*" di cui all'art 416 c.p.;
- "*associazione per delinquere finalizzata alla riduzione o mantenimento in schiavitù o in servitù (*ex *art. 600 c.p.) alla tratta di persone (*ex *art. 601 c.p.) o all'acquisto e alienazione di schiavi (*ex *art. 602 c.p.)*" di cui all'art. 416, comma 6 c.p.;
- "*associazione di stampo mafioso anche straniere*" di cui all'art. 416-*bis* c.p.;
- "*scambio elettorale politico-mafioso*" di cui all'art. 416-*ter* c.p.;
- "*sequestro di persona a scopo di rapina o di estorsione*" di cui all'art. 630 c.p.;
- "*associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope*" di cui all'art. 74 del D.P.R. n. 309/1990;
- "*delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra, di esplosivi e di armi clandestine*" di cui all'art. 407 comma 2, lett. a) n. 5 c.p.p.

Da un'analisi preliminare dei rischi relativi alle attività poste in essere dalla Società è emerso che il rischio di commissione dei reati di cui agli articoli 416, comma 6 c.p., 416 *bis*, 416-*ter* c.p., 630 c.p. nonché all'art. 74 del D.P.R. n. 309/1990 e all'art. 407 comma 2, lett. a) n. 5 c.p.p. è remoto e solo astrattamente ipotizzabile.

Si fornisce, invece, qui di seguito una breve descrizione della fattispecie di cui all'art. 24-*ter* del Decreto ritenuta *prima facie* rilevante per la Società e prevista dall'art. 416 c.p.

#### *ASSOCIAZIONE PER DELINQUERE (ART. 416 C.P.)*

La condotta sanzionata dall'art. 416 c.p. è integrata mediante la costituzione e la conservazione di un vincolo associativo continuativo con fine criminoso tra tre o più persone, allo scopo di commettere una serie indeterminata di delitti, con la predisposizione di mezzi necessari per la realizzazione del programma criminoso e con la permanente consapevolezza di ciascun associato di far parte di un sodalizio e di essere disponibile ad operare per l'attuazione del programma delinquenziale.

Il reato associativo è caratterizzato, pertanto, dai seguenti elementi fondamentali:

1) *stabilità e permanenza*: il vincolo associativo deve essere tendenzialmente stabile e destinato a durare anche oltre la realizzazione dei delitti concretamente programmati;

2) *indeterminatezza del programma criminoso*: l'associazione per delinquere non si configura se i partecipanti si associano al fine di compiere un solo reato; lo scopo dell'associazione deve essere quello di commettere più delitti, anche della stessa specie (in tal caso l'indeterminatezza del programma criminoso ha riguardo solo all'entità numerica);

3) *esistenza di una struttura organizzativa*: l'associazione deve prevedere un'organizzazione di mezzi e di persone che, seppure in forma rudimentale, siano adeguati a realizzare il programma criminoso e a mettere in pericolo l'ordine pubblico.

In particolare, sono puniti coloro che promuovono, costituiscono o organizzano l'associazione, oltre a coloro che regolano l'attività collettiva da una posizione di superiorità o supremazia gerarchica, definiti dal testo legislativo come "capi".

Sono puniti altresì con una pena inferiore tutti coloro che partecipano all'associazione.

Il reato in questione assume rilevanza ai fini della responsabilità amministrativa degli enti anche se commesso a livello "*transnazionale*" ai sensi dell'art. 10 della Legge 16 marzo 2006, n. 146 (legge di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale).

A tal riguardo giova sottolineare che ai sensi dell'art. 3 della suddetta legge si considera "transnazionale" il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

- sia commesso in più di uno Stato;
- ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
- ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

* * *

Come emerge dalla descrizione del reato in esame, attraverso lo strumento del reato associativo potrebbero essere commessi anche reati espressamente previsti dal Decreto 231, analizzati e approfonditi nelle relative Parti Speciali (cui occorre rinviare), indipendentemente dalla circostanza che la loro esecuzione avvenga in forma associativa o meno.

## CAPITOLO H.2

### Attività Sensibili

In relazione ai reati e alle condotte criminose sopra esplicitate, le attività ritenute più specificamente a rischio risultano essere, ai fini della presente Parte Speciale, le seguenti:

1. *Selezione, assunzione e gestione del personale*: si tratta di attività finalizzate all'assunzione di personale dipendente e consistenti nell'accertamento dei requisiti di onorabilità e affidabilità in capo ai candidati. Tali attività si svolgono attraverso l'attribuzione di specifico incarico a società di *head hunting* o attraverso la selezione diretta da parte dei responsabili di funzione interessati all'integrazione della risorsa.

   L'Attività Sensibile in esame è legata ai profili di rischiosità connessi – nell'ottica della possibile commissione dei reati associativi – all'impiego in azienda di personale con precedenti penali o giudizi pendenti.

2. *Selezione delle controparti contrattuali*: si tratta di attività finalizzate all'accertamento della sussistenza dei requisiti di onorabilità e affidabilità in capo a:

   - *Intermediari*, ossia ai soggetti operanti nella rete distributiva con i quali la Società stipula accordi di distribuzione dei propri prodotti assicurativi.
   - *Partner*, Fornitori, Consulenti e altri enti con i quali la Società potrebbe intraprendere forme di collaborazione contrattualmente regolate (ad esempio associazioni temporanee di impresa – ATI, *joint venture*, consorzi, ecc.).

   La selezione delle controparti contrattuali rileva in quanto l'instaurazione di rapporti con le stesse potrebbe rappresentare un fondamentale presupposto fattuale per la successiva commissione dei reati associativi.

## CAPITOLO H.3

## Regole e principi generali

### H.3.1 Il sistema in linea generale

Obiettivo della presente Parte Speciale è che i Destinatari del Modello si attengano – nella misura in cui gli stessi siano coinvolti nello svolgimento delle Attività Sensibili o di attività alle stesse connesse, nonché in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti della Società – a regole di condotta conformi a quanto prescritto nella stessa al fine di prevenire e impedire il verificarsi dei Delitti di Criminalità Organizzata.

In particolare, la presente Parte Speciale ha la funzione di fornire:

- un elenco dei principi generali nonché dei principi procedurali specifici cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- all'OdV e ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, i principi e gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica agli stessi demandati.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, i Destinatari sono tenuti, in generale, a rispettare tutte le regole e i principi disposti dalla Società e dal Gruppo alla quale la stessa appartiene.

### H.3.2 Principi generali di comportamento

I seguenti principi di carattere generale si applicano a tutti i Destinatari.

In via generale, è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate; sono altresì proibite le violazioni ai principi e alle procedure aziendali richiamate nella presente Parte Speciale.

Al fine di prevenire eventuali infiltrazioni criminali nell'esercizio dell'attività aziendale sono previsti a carico degli Esponenti Aziendali e dei Dipendenti, ciascuno per le attività di propria competenza, i seguenti obblighi:

- non sottostare a richieste di qualsiasi tipo contrarie alla legge e darne, comunque, informativa al proprio diretto superiore il quale, a sua volta, dovrà darne comunicazione all'Amministratore Delegato e all'Organismo di Vigilanza;
- consentire l'accesso alle aree aziendali soltanto a persone autorizzate.

È in ogni caso fatto obbligo a ciascun Esponente Aziendale, anche per il tramite di propri superiori gerarchici, segnalare all'OdV qualsiasi elemento da cui possa desumersi il pericolo di interferenze criminali in relazione all'attività aziendale e la Società si impegna a tal riguardo a garantire la riservatezza a coloro che adempiano ai suddetti obblighi di segnalazione o denuncia con un pieno supporto, anche in termini di eventuale assistenza legale.

In generale, in relazione ai reati di associazione per delinquere:

- è fatto divieto di procedere all'assunzione di personale dipendente senza aver rispettato le procedure di assunzione adottate dalla Società e senza aver prima constatato la sussistenza di requisiti di onorabilità e affidabilità in capo ai candidati; è inoltre fatto divieto di favorire candidati per il solo fatto che gli stessi siano legati da rapporti di parentela, affinità o amicizia con soggetti operanti all'interno della Società;
- è fatto divieto di instaurare rapporti con soggetti terzi – persone fisiche o giuridiche, italiane o straniere – senza aver rispettato i criteri e le metodologie di selezione previsti dalle procedure aziendali.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, codici di comportamento, *policy* e procedure aziendali.

Tali *policy* e procedure e loro eventuali successive integrazioni o modifiche si considerano parte integrante del Modello e, pertanto, si devono intendere come recepite nella loro configurazione.

## CAPITOLO H.4

## Principi procedurali specifici

### H.4.1 Principi procedurali specifici generalmente applicabili

Ai fini dell'attuazione dei principi e regole generali e dei divieti elencati al precedente cap. H.3, devono rispettarsi gli specifici principi procedurali qui di seguito descritti, oltre alle regole e principi generali già contenuti nella Parte Generale del Modello. Le regole qui di seguito descritte devono essere rispettate sia nell'esplicazione dell'attività della Società in territorio italiano sia eventualmente all'estero.

1) *Selezione, assunzione e gestione del personale:*

a. La Società adotta specifiche procedure di selezione e assunzione del personale dipendente di qualsiasi livello e di collaboratori a progetto che garantiscano un criterio di trasparenza sulla base dei seguenti parametri:

   - professionalità adeguata rispetto all'incarico o alle mansioni da assegnare;
   - uguaglianza di trattamento tra i diversi candidati;
   - affidabilità rispetto al rischio di infiltrazione criminale.

b. La Società conserva la documentazione esibita in sede di assunzione da parte del dipendente anche al fine di consentirne la consultazione da parte dell'OdV nell'espletamento della consueta attività di vigilanza e controllo.

c. La Società mette a disposizione dei neoassunti copia del Modello 231 e del Codice Etico con la richiesta di prenderne visione e di impegnarsi al rispetto dei principi contenuti negli stessi.

d. La Società prevede contrattualmente che il datore di lavoro somministrante accerti la sussistenza dei requisiti di onorabilità dei propri dipendenti, consentendo alla Società di risolvere con effetto immediato il contratto di somministrazione di attività lavorativa qualora il dipendente somministrato risultasse indagato o condannato per reati di cui al D.Lgs. 231/2001.

d) Il processo di inserimento della risorsa all'interno della Società deve avvenire nel rispetto degli obblighi di formazione e aggiornamento previsti dalle procedure aziendali in base al ruolo e all'attività svolta all'interno dell'azienda.

e) Eventuali avanzamenti interni di carriera e riconoscimenti di premi (ivi compresa l'eventuale previsione, nel trattamento retributivo, di una componente variabile legata al raggiungimento di specifici obiettivi) devono essere assegnati secondo criteri oggettivi basati sulla parità di trattamento, sulla valorizzazione del merito e della professionalità nonché sul rispetto della normativa aziendale.

2) *Selezione delle controparti contrattuali:*

a. La Società verifica l'attendibilità commerciale e professionale dei Fornitori, *Partner*, Consulenti e intermediari.

b. La Società adotta procedure o *policy* aziendali volte a garantire che il processo di selezione delle controparti contrattuali avvenga nel rispetto dei criteri di trasparenza, pari opportunità di accesso, professionalità, affidabilità ed economicità, fermo restando la prevalenza dei requisiti di legalità rispetto a tutti gli altri.

c. La Società tiene traccia dei Consulenti, Fornitori e altre controparti con i quali siano già intercorsi rapporti contrattuali.

d. La Società si impegna, in occasione di ogni rinnovo contrattuale con Fornitori, *Partner* e Consulenti, a richiedere la sottoscrizione da parte di questi ultimi di un'autodichiarazione circa la persistenza dei requisiti di onorabilità che in fase di selezione iniziale hanno permesso l'instaurazione del rapporto.

i. I rapporti tra la Società e i Consulenti, i Fornitori, i *Partner* e gli intermediari devono essere definiti per iscritto in tutte le loro condizioni e termini e rispettare quanto indicato ai successivi punti.

j. Tali contratti devono contenere (anche in caso di rinnovo) una clausola standard (cosiddetta "**Clausola 231**"), con cui le controparti contrattuali della Società:

- dichiarino di conoscere la disciplina di cui al Decreto 231 e le sue implicazioni in termini di adempimenti e responsabilità;
- si impegnino al rispetto delle disposizioni in esso contenute e dichiarino di non essere mai stato coinvolto in procedimenti giudiziari relativi ai reati contemplati nella suddetta normativa;
- dichiarino di essere a conoscenza (avendone presa visione) del contenuto del Codice Etico e del Modello della Società ed – eventualmente – di aver adottato a loro volta un codice etico e un modello di organizzazione, gestione e controllo;

- si impegnino a rispettare il contenuto del Codice Etico e del Modello della Società.

k. In conformità con le indicazioni fornite a livello di Gruppo, i contratti con i Consulenti, i Fornitori e i *Partner* prevedono, inoltre, il rispetto da parte dei medesimi di normative nazionali e/o internazionali applicabili e rilevanti.

e. Ad integrazione dei principi sopra esposti, nel caso di instaurazione di rapporti continuativi con controparti contrattuali, la Società si impegna ad attuare efficacemente controlli periodici circa

    - la persistenza in capo a questi ultimi dei requisiti che in fase di selezione iniziale hanno permesso l'instaurazione del rapporto;
    - l'effettiva esecuzione della consulenza/fornitura e la congruità del prezzo pattuito.

## CAPITOLO H.5

## I controlli dell'OdV e i flussi informativi

### H.5.1 Il controllo in generale

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati di cui alla presente Parte Speciale sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente l'efficacia della stessa a prevenire la commissione dei Reati quivi previsti. Con riferimento a tale punto l'OdV – avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia – condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà alle funzioni competenti eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle previsioni contenute nella presente Parte Speciale;
- proporre e collaborare nella predisposizione delle istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle Attività Sensibili individuate nella presente Parte Speciale; tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di adempiere adeguatamente ai propri compiti, l'OdV può:

a) organizzare specifici incontri con i Responsabili delle funzioni Legale e Affari Societari e/o Risorse Umane, *Property* e *Mobility Management* in merito ad eventuali segnalazioni di procedimenti penali in corso che vedano coinvolti Esponenti Aziendali o altri Destinatari per reati associativi o per altri reati rilevanti ai fini della responsabilità amministrativa degli enti (ad esempio riciclaggio, reati societari, ecc.).

b) accedere o richiedere ai propri delegati di accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

Al fine di dare attuazione ai principi che precedono, la Società prevede l'istituzione di flussi informativi nei confronti dell'OdV. Tali flussi informativi dovranno essere idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio delle anomalie rilevanti ai sensi della presente Parte Speciale e delle criticità rilevate in tale ambito.

Fermo restando quanto appena indicato, l'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verifichino violazioni ai principi procedurali specifici contenuti nel Capitolo H.4 della presente Parte Speciale ovvero alle procedure*, policy* e normative aziendali attinenti alle Attività Sensibili sopra individuate.

Per i flussi informativi si rimanda, in particolare, alla compilazione da parte delle funzioni competenti delle "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento) che costituiscono un allegato al Modello.

**PARTE SPECIALE – I –**

**Delitti contro l'industria e il commercio e delitti di contraffazione**

## CAPITOLO I.1

### A) Delitti contro l'industria e il commercio

La Legge 23 luglio 2009, n. 99 ha esteso la responsabilità amministrativa degli enti prevista dal Decreto 231 ai "*delitti contro l'industria e il commercio*" (art. 25-*bis* 1.) configurabili ogni qualvolta venga commesso nell'interesse o a vantaggio dell'ente una delle seguenti fattispecie di reati:

- *turbata libertà dell'industria o del commercio* (art. 513 c.p.);
- *illecita concorrenza con minaccia o violenza* (art. 513-*bis* c.p.);
- *frodi contro le industrie nazionali* (art. 514 c.p.);
- *frode nell'esercizio del commercio* (art. 515 c.p.);
- *vendita di sostanze alimentari non genuine come genuine* (art. 516 c.p.);
- *vendita di prodotti industriali con segni mendaci* (art. 517 c.p.);
- *fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale* (art. 517-*ter* c.p.);
- *contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari* (art. 517-*quater* c.p.).

Si provvede a fornire qui di seguito una breve descrizione dei reati che sono risultati astrattamente configurabili in relazione all'attività aziendale svolta dalla Società.

***TURBATA LIBERTÀ DELL'INDUSTRIA E DEL COMMERCIO (ART. 513 C.P.)***

Risponde del delitto di turbata libertà dell'industria e del commercio ai sensi dell'art. 513 c.p. chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di una industria o di un commercio.

Tale norma ha ad oggetto la tutela del libero esercizio dell'industria, ossia di qualsiasi forma di organizzazione che tenda a concentrare l'attività produttiva, e del commercio, inteso come esercizio abituale dell'acquisto e della rivendita dei beni a scopo di guadagno: rientrano, pertanto, nell'ambito di protezione della norma tutti i tipi di attività economica che rispettino i requisiti di organizzazione, economicità e professionalità stabiliti dall'art. 2082 c.c. per l'esercizio dell'attività imprenditoriale.

In particolare la condotta dell'intermediario deve essere concretamente idonea a:

- *impedire*, ossia a contrastare anche temporaneamente o parzialmente l'esercizio

dell'attività industriale o commerciale;

- *turbare*, ossia alterare il regolare e libero svolgimento dell'attività industriale o commerciale.

La fattispecie in oggetto prevede alternativamente l'uso della violenza sulle cose o di mezzi fraudolenti. In relazione alla prima, deve farsi riferimento all'art. 392, comma 2, c.p. il quale prevede in generale che "*agli effetti della legge penale si ha «violenza sulle cose» allorché la cosa venga danneggiata o trasformata o ne è mutata la destinazione*".

Con riferimento alla definizione di mezzi fraudolenti, invece, non essendo previsto alcunché dalle norme del codice penale, devono intendersi tali tutti i mezzi che sono in concreto idonei a trarre in inganno la vittima (ad esempio artifizi, raggiri e menzogne).

La condotta tipica nella prassi si manifesta attraverso atti di concorrenza sleale, intendendosi per tali quelli commessi da colui che ai sensi dell'art. 2598 c.c.:

a. usa nomi o segni distintivi idonei a produrre confusione con nomi o segni distintivi legittimamente usati da altri o imita servilmente i prodotti di un concorrente, o compie con qualsiasi altro mezzo atti idonei a creare confusione con i prodotti o con altre attività di un concorrente;

b. diffonde notizie e apprezzamenti sui prodotti e sull'attività di un concorrente, idonei a determinarne il discredito, o si appropria di pregi dei prodotti o dell'impresa di un concorrente;

c. si avvale direttamente o indirettamente di ogni altro mezzo non conforme ai principi della correttezza professionale e idoneo a danneggiare l'altrui azienda.

Ai fini della rilevanza penale e, quindi, delle configurabilità del reato è comunque necessario che i suddetti comportamenti siano idonei concretamente a impedire o turbare l'esercizio dell'attività industriale o commerciale e che siano posti in essere con violenza o quantomeno con mezzi fraudolenti. In caso contrario rimangono sanzionabili solo ai sensi dell'art. 2599 c.c. e 2600 c.c. attraverso un provvedimento giudiziario volto ad inibire il comportamento sleale, a eliminarne gli effetti e a liquidare il risarcimento dei danni provocati (con possibile pubblicazione della sentenza).

Il suddetto reato potrebbe configurarsi in astratto qualora la Società adotti politiche di commercializzazione o pubblicizzazione particolarmente aggressive e condotte attraverso raggiri o simulazioni al fine di sviare la clientela di un determinato *competitor* oppure nel caso in cui utilizzi mezzi fraudolenti diretti nei confronti di un intermediario assicurativo che

collabora con un *competitor* al fine di indurlo a cessare la propria attività di promozione dei prodotti assicurativi concorrenti e, quindi, di conquistare la quota di mercato.

***ILLECITA CONCORRENZA CON MINACCIA O CON VIOLENZA (ART. 513-BIS C.P.)***

L'art. 513-*bis* punisce chiunque nell'esercizio di una attività commerciale, industriale o comunque produttiva, compie atti di concorrenza con violenza o minaccia.

Gli atti di concorrenza previsti dalla norma non sono di per sé illeciti e consistono in un insieme di attività compiute al fine di produrre o vendere di più rispetto agli altri esercenti la stessa attività o attività simile. Tali atti diventano illeciti e integrano, quindi, il suddetto reato solo nel caso in cui vengano compiuti con violenza, ossia impiegando energia fisica sulla persona o sulle cose, o con minaccia ossia prospettando ad una persona un male ingiusto e futuro il cui verificarsi dipenderà dalla volontà del minacciante.

L'intermediario tende attraverso le suddette condotte a eliminare i concorrenti, reprimendo la loro capacità di autodeterminarsi.

**B) I reati di contraffazione**

La Legge 23 luglio 2009, n. 99 ha introdotto, altresì, all'interno dei reati di "*falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento*" di cui all'art. 25-*bis* del Decreto 231 le fattispecie di "*contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni*" (di seguito, i "**delitti di contraffazione**") e di "*introduzione nello Stato e commercio di prodotti con segni falsi*", previste rispettivamente dagli art. 473 c.p. e art. 474 c.p.

Si provvede a fornire qui di seguito una breve descrizione del reato di cui all'art. 473 c.p., in quanto ritenuto *prima facie* rilevante in relazione all'attività svolta dalla Società.

***CONTRAFFAZIONE, ALTERAZIONE O USO DI MARCHI O SEGNI DISTINTIVI OVVERO DI BREVETTI, MODELLI E DISEGNI (ART. 473 C.P.)***

L'art. 473 c.p. sanziona penalmente:

a) chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, contraffà o altera marchi o segni distintivi, nazionali o esteri, di prodotti industriali;

b) chiunque, senza essere incorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati.

La norma ha ad oggetto la tutela di segni distintivi o di prodotti industriali, ossia di:

- *marchi*: segni (emblema, figura, denominazione ecc.) destinati a distinguere merci o prodotti di una determinata impresa;
- *brevetti*: attestati con i quali è concesso il diritto all'uso esclusivo di una invenzione o di una scoperta;
- *disegni industriali*: rappresentazione figurativa di qualsiasi bene o prodotto industriale;
- *modello industriale*: archetipo di una scoperta o di una nuova applicazione industriale (ad esempio modelli ornamentali e modelli di utilità).

La condotta criminosa consiste nella falsificazione del segno distintivo in modo tale da ingenerare confusione nella distinzione dei segni e può quindi consistere nella:

- *contraffazione*, ossia nella creazione di cosa del tutto simile ad un'altra in modo da trarre in inganno sulla sua essenza;
- *alterazione*, ossia nella modificazione dell'aspetto, della sostanza o della natura di una cosa.

La condotta viene penalmente sanzionata anche nel caso di utilizzo commerciale o industriale dei marchi o dei segni distintivi già falsificati e, quindi, anche non di contraffazione o alterazione *strictu sensu*.

Il reato potrebbe configurarsi in relazione all'utilizzo da parte della Società di segni distintivi già registrati da altre società operanti nello stesso ambito di attività e per commercializzare un prodotto assicurativo avente peculiari caratteristiche. Tale condotta, creando confusione nei prodotti assicurativi, potrebbe avvantaggiare la Società inducendo gli assicurati a sottoscrivere polizze assicurative che già ritengono di conoscere.

## CAPITOLO I.2

### Attività Sensibili nell'ambito dei delitti contro l'industria e il commercio e dei reati di contraffazione

Dall'analisi dei rischi e suggerimenti è emerso che i delitti contro l'industria e il commercio sono difficilmente configurabili da parte della Società ma, tuttavia, non possono essere sottovalutati. A tal proposito, la Società ha individuato nel proprio ambito di operatività le seguenti Attività Sensibili che risultano maggiormente esposte al rischio di commissione dei Reati in oggetto:

a. attività di sviluppo e commercializzazione di prodotti assicurativi (anche con riferimento ai rapporti commerciali con gli intermediari che operano anche per altre compagnie assicurative non appartenenti al Gruppo Crédit Agricole);
b. pubblicizzazione e comunicazioni relative ai prodotti assicurativi (nuovi ovvero già esistenti).

## CAPITOLO I.3

### Regole e principi generali

Sebbene la commissione di delitti contro l'industria e il commercio sia solo astrattamente ipotizzabile, con la presente Parte Speciale la Società intende disporre regole di condotta uniformi destinate a tutti i Dipendenti e agli Organi Sociali della Società al fine di prevenire e impedire il verificarsi di condotte criminose che possano integrare i reati di turbata libertà dell'industria e del commercio o illecita concorrenza con minaccia o con violenza nonché i delitti di contraffazione.

Nell'espletamento delle attività aziendali e, in particolare, nelle Attività Sensibili, è espressamente vietato ai soggetti sopra indicati, anche in relazione al tipo di rapporto posto in essere con la Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente Parte Speciale (artt. 25-*bis* e 25-*bis*.1 del Decreto).

In particolare:

1. è ammesso intrattenere rapporti d'affari con intermediari che operano anche per altre compagnie assicurative concorrenti nel rispetto della legge e dei principi a tutela della libera concorrenza;
2. è vietato utilizzare minaccia, violenza o mezzi fraudolenti al fine di indurre un intermediario assicurativo a cessare o ridurre o modificare a vantaggio della Società l'attività di promozione dei prodotti assicurativi di un *competitor;*
3. non è ammesso usare nomi o segni distintivi per la commercializzazione dei prodotti assicurativi che siano idonei a produrre confusione con nomi o segni distintivi legittimamente usati da altre compagnie assicurative;
4. non è ammesso imitare servilmente i prodotti di un concorrente che abbiano caratteristiche peculiari e specifiche tali da poter essere considerate proteggibili dalla normativa oggetto della presente Parte Speciale;
5. non è ammesso compiere qualsiasi atto idoneo a creare confusione tra i prodotti assicurativi della Società e i prodotti di un concorrente;
6. non è ammesso diffondere notizie e/o apprezzamenti sui prodotti e sull'attività di un concorrente che siano anche solo potenzialmente idonei a determinarne il

discredito;

7. non è ammesso partecipare a gare d'appalto o *beauty contest* qualora tale attività non rientri nella propria *job description* ovvero, in tale ultima ipotesi, senza preventiva autorizzazione da parte delle funzioni competenti;
8. non è ammesso utilizzare marchi diversi da quelli espressamente autorizzati dalla Società per la commercializzazione e pubblicizzazione dei prodotti assicurativi;
9. non è ammesso utilizzare segni distintivi già registrati da altre società per commercializzare e pubblicizzare i prodotti assicurativi.

Al fine di mitigare il rischio di commissione dei Delitti di contraffazione e, di conseguenza, anche di assicurare il corretto adempimento degli obblighi connessi alla normativa di riferimento, la Società, in relazione alle operazioni inerenti allo svolgimento della propria attività, assolve i seguenti adempimenti:

1. tiene traccia di tutti i marchi e dei segni distintivi registrati dalla medesima o concessi in uso alla Società da parte di altre società (anche del Gruppo di appartenenza) o da altri soggetti che ne sono titolari;
2. accerta l'inconfondibilità dei segni distintivi utilizzati per commercializzare e pubblicizzare i prodotti assicurativi attraverso ricerche di anteriorità;
3. a tal fine, prevede la necessaria consultazione delle banche dati messe a disposizione dall'Ufficio Italiano Marchi e Brevetti – anche tramite consulenti esterni – prima dell'utilizzo a scopi commerciali di segni o simboli grafici che possano costituire marchi già registrati.

La particolare attenzione che la Società ripone nel presidiare le fattispecie in oggetto è rappresentata anche dai princìpi ad esse dedicate all'interno del Codice Etico, della Carta Etica e Codice di Condotta.

In generale, nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, codici di comportamento, *policy* e procedure aziendali.

Tali *policy* e procedure e loro eventuali successive integrazioni o modifiche si considerano parte integrante del Modello e, pertanto, si devono intendere come recepite nella loro configurazione.

## CAPITOLO I.4

### Principi procedurali specifici

Ai fini dell'attuazione delle regole e del rispetto dei divieti elencati nel precedente Capitolo, devono essere ottemperati i principi procedurali qui di seguito descritti, oltre alle Regole e ai Principi Generali già contenuti nella Parte Generale del presente Modello.

In particolare, si elencano qui di seguito le regole e i presidi che devono essere rispettati dai destinatari della presente Parte Speciale, meglio individuati nel Capitolo precedente, nell'ambito delle Attività Sensibili.

1. *Attività di sviluppo e commercializzazione di prodotti assicurativi (anche con riferimento ai rapporti commerciali con gli intermediari che operano anche per altre compagnie assicurative non appartenenti al Gruppo Crédit Agricole)*

a. Nell'ambito dell'attività in oggetto, è fatto divieto di:

   1. utilizzare nomi o segni distintivi per la commercializzazione dei prodotti assicurativi che non siano stati previamente oggetto di valutazione da parte delle funzioni competenti a svolgere indagini relative alla potenziale idoneità degli stessi a confondere la clientela;

   2. denigrare un concorrente o, comunque, convincere fraudolentemente un appaltatore a scegliere la Società preferendola ad altre nell'ambito di una gara d'appalto o di un *beauty contest*;

b. è prevista l'istituzione di appositi comitati interni con il compito di valutare e approvare le proposte di nuove attività e nuovi prodotti provenienti da funzioni di *business*, con specifico riferimento alla conformità alle leggi, regolamenti e procedure vigenti (nell'ambito delle comunicazioni relative ai prodotti è sempre previsto il coinvolgimento della funzione *Compliance*);

c. nessun prodotto o attività nuovi possono essere commercializzati senza l'autorizzazione del comitato di cui al punto b).

d. la Società, inoltre:

   1. prevede linee guida di comportamento nei rapporti d'affari con gli intermediari assicurativi;
   2. prevede specifica attività informativa e formativa prima del lancio di nuovi prodotti;

3. predispone presidi volti ad accertare l'inconfondibilità dei segni distintivi utilizzati per commercializzare i prodotti assicurativi;
4. garantisce la diffusione e, comunque, la disponibilità per tutti i soggetti interessati, della procedura relativa al processo autorizzativo per i nuovi prodotti e le nuove attività;
5. nell'ambito delle attività prodromiche allo sviluppo e alla commercializzazione dei prodotti assicurativi, procede alla consultazione delle banche dati messe a disposizione dall'Ufficio Italiano Marchi e Brevetti da attuarsi ogni volta che si intendano utilizzare nuovi segni o simboli grafici;
6. tiene traccia di tutti i marchi e dei segni distintivi utilizzati (e, pertanto, utilizzabili) dalla Società per la commercializzazione dei prodotti assicurativi e fornisce specifiche istruzioni sull'utilizzo di nuovi marchi o segni distintivi;
7. prevede controlli a campione in relazione ai canali attraverso i quali sono commercializzati i prodotti assicurativi.

2. *Pubblicizzazione e comunicazioni relative ai prodotti assicurativi (nuovi ovvero già esistenti)*

Nell'ambito dell'attività in oggetto, è fatto divieto di:

a. diffondere notizie su compagnie assicurative concorrenti, attraverso la stampa, internet ovvero qualsiasi altro mezzo di comunicazione senza preventiva autorizzazione;

b. inserire nella carta intestata, nei documenti contenenti le polizze assicurative, nelle brochure pubblicitarie, nel sito internet e in qualsiasi altro supporto cartaceo o informatico simboli o segni grafici prima che:

   - sia stata verificata la non registrazione dei medesimi nonché l'inconfondibilità degli stessi attraverso indagini e consultazioni di banche dati messe a disposizione dall'Ufficio Italiano Marchi e Brevetti;
   - sia stata ottenuta espressa autorizzazione dalle funzioni competenti.

Inoltre, la Società:

a. informa i propri Esponenti e i Dipendenti – anche tramite specifica attività formativa – in merito al divieto di diffondere informazioni o apprezzamenti che possano essere lesivi delle attività dei *competitors* o che siano tali da trarre in inganno un cliente;

b. prevede linee guida rivolte ai propri Esponenti, ai Dipendenti e ai distributori in

merito alle comunicazioni relative ai prodotti (anche per quanto riguarda l'attività di telemarketing);

c. prevede controlli sui contenuti del sito internet, dei social media nonché su altri canali attraverso i quali sono pubblicizzati i prodotti assicurativi;

d. prevede presidi volti ad accertare l'inconfondibilità dei segni distintivi utilizzati per la pubblicizzazione dei prodotti assicurativi;

e. prevede, anche al di fuori delle riunioni dei comitati istituiti, il coinvolgimento della funzione Compliance nelle valutazioni relative alle comunicazioni sui prodotti.

## CAPITOLO I.5

### I controlli dell'OdV e i flussi informativi

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'art. 25-*bis*.1 D.Lgs. 231/2001 sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare regolarmente la sua efficacia a prevenire la commissione dei delitti di cui all'artt. 25 *bis* e 25-*bis*.1 del Decreto 231;
- consultarsi con i responsabili delle funzioni coinvolte ogni qualvolta sorga nell'area di loro competenza il sospetto di violazione dei principi comportamentali previsti dalla presente Parte Speciale.

A tal fine, all'OdV, viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Per i flussi informativi si rimanda, in particolare, alla compilazione da parte delle funzioni competenti delle "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento) che costituiscono un allegato al Modello.

**PARTE SPECIALE – L –**

**Fattispecie di corruzione tra privati**

## CAPITOLO L.1

### Le fattispecie di reato di corruzione tra privati (Art. 25-*ter*, comma 1, lettera s-*bis*, del D.Lgs. 231/2001)

La Legge 6 novembre 2012, n. 190, recante "*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*", ha introdotto nel nostro ordinamento, attraverso la modifica dell'art. 2635 c.c. – fattispecie che originariamente puniva l'"*infedeltà a seguito di dazione o promessa di utilità*" – il reato di "*corruzione tra privati*".

L'Articolo in parola è poi stato oggetto di ulteriori modifiche, l'ultima delle quali intervenuta con L. 9 gennaio 2019, n. 3. A seguito di detta modifica, l'art. 2635 c.c. recita come segue:

"*1. Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni. Si applica la stessa pena se il fatto è commesso da chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo.*

*2. Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.*

*3. Chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuti alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste.*

*4. Le pene stabilite nei commi precedenti sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'art. 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.*

*5. Fermo quanto previsto dall'articolo 2641, la misura della confisca per valore equivalente non può essere inferiore al valore delle utilità date, promesse e offerte*".

In precedenza, il D.Lgs. 15 marzo 2017, n. 38 aveva introdotto nell'ordinamento una nuova fattispecie di reato, denominata "*istigazione alla corruzione tra privati*", prevista e punita dall'art. 2635-*bis* c.c., che – anch'essa oggetto di modifica ad opera della L. 9 gennaio 2019, n. 3 – recita come segue:

"*1. Chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo.*

*2. La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per sé o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata*".

Le fattispecie in esame sono state, inoltre, inserite nel catalogo dei reati presupposto.

In particolare, ai fini dell'applicazione della responsabilità amministrativa degli enti *ex* Decreto 231 rileva la fattispecie di corruzione tra privati cosiddetta "attiva", in virtù del richiamo che l'art. 25-*ter*, lett. s-*bis*, del Decreto 231 fa al terzo comma dell'art. 2635 ("*Chi, anche per interposta persona, offre, promette o dà* […]") e al primo comma dell'art. 2635-*bis* c.c. ("*Chiunque offre o promette* […]").

Si segnala come l'attuale formulazione dell'art. 25-*ter*, lett. s-*bis* del Decreto 231, con riferimento alla pena per la violazione delle norme in parola, preveda, oltre alla sanzione pecuniaria, l'applicabilità delle sanzioni interdittive.

***

Occorre rilevare, per completezza, come la promessa o la dazione di denaro o altra utilità come corrispettivo per il compimento o l'omissione di un atto, costituisca condotta astrattamente idonea ad integrare ulteriori e diverse fattispecie di reato. L'art. 2635 c.c. non trova applicazione, per espressa previsione normativa, quando il fatto costituisce un più grave reato.

Esistono, poi, incriminazioni che, apparentemente simili alla "*corruzione tra privati*", hanno un ambito applicativo distinto. Gli articoli 27 e 28 del D.Lgs. 39/2010, fattispecie non ricomprese tra i reati presupposto della responsabilità amministrativa degli enti, ad esempio, sanzionano condotte, *lato sensu* "corruttive", poste in essere nei confronti della società di revisione.

***FALSITÀ NELLE RELAZIONI O NELLE COMUNICAZIONI DEI RESPONSABILI DELLA REVISIONE LEGALE (ART. 27, D.LGS. 39/2010)***

Art. 27 del citato D.Lgs. 39/2010 prevede che "*I responsabili della revisione legale i quali, al fine di conseguire per sè 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, attestano il falso od occultano 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, sono puniti, se la condotta non ha loro cagionato un danno patrimoniale, con l'arresto fino a un anno*".

Con particolare riferimento agli "*Enti di Interesse Pubblico*", la medesima disposizione prevede delle pene superiori rispetto a quelle previste in caso di corruzione tra privati. In particolare, l'art. 27, commi 3 e 4, prevede che:

- se il fatto previsto dal comma 1 (falsità od occultamento) è commesso dal responsabile della revisione legale di uno di tali enti, la pena prevista è da uno a cinque anni;
- se il fatto previsto dal comma 1 (falsità od occultamento) è commesso dal responsabile della revisione legale di un ente di interesse pubblico per denaro o altra utilità data o promessa, ovvero in concorso con gli amministratori, i direttori generali o i sindaci della società assoggettata a revisione, la pena è aumentata fino alla metà.

Anche la fattispecie di cui all'art. 27 del D.Lgs. 39/2010 prevede la punizione sia della condotta passiva, sia della condotta attiva. In particolare, il quinto comma della medesima disposizione dispone che le stesse pene previste a carico di chi commette la falsità o l'occultamento siano applicate anche "*a chi dà o promette l'utilità nonché ai direttori generali e ai componenti dell'organo di amministrazione e dell'organo di controllo dell'ente di interesse pubblico assoggettato a revisione legale, che abbiano concorso a commettere il fatto*".

La linea di *discrimen* rispetto al reato di "corruzione tra privati" è tracciata dalla norma stessa, la quale limita il proprio perimetro applicativo all'atto, specificamente individuato nella falsa attestazione o nell'occultamento di informazioni concernenti la situazione economica,

patrimoniale o finanziaria della società, compiuto da un soggetto qualificato, ossia il responsabile della revisione legale[8].

Pertanto, anche nel caso in cui concorrano alla commissione del fatto, unitamente al responsabile della revisione legale, i medesimi soggetti indicati dalla norma sulla "corruzione tra privati" (amministratori, direttori generali e sindaci), non sarà configurabile, se l'atto compiuto si sostanzia nella falsa attestazione o nell'occultamento descritti, tale ultima fattispecie, ma quella di cui all'art. 27 del D.lgs. 39/2010.

***CORRUZIONE DEI REVISORI (ART. 28, D.LGS. 39/2010)***

L'art. 28 del D.Lgs. 39/2010 prevede che "*i responsabili della revisione legale, i quali, a seguito della dazione o della promessa di utilità, per sé o per un terzo, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio, cagionando nocumento alla società, sono puniti con la reclusione sino a tre anni. La stessa pena si applica a chi dà o promette l'utilità*".

Il secondo comma dello stesso articolo prevede che "*il responsabile della revisione legale e i componenti dell'organo di amministrazione, i soci, e i dipendenti della società di revisione legale, i quali, nell'esercizio della revisione legale dei conti degli enti di interesse pubblico o delle società da queste controllate* [...] *per denaro o altra utilità data o promessa, compiono od omettono atti in violazione degli obblighi inerenti all'ufficio, sono puniti con la reclusione da uno a cinque anni. La stessa pena si applica a chi dà o promette l'utilità*".

La struttura del reato previsto dall'art. 28 del D.Lgs. 39/2010 è molto simile a quella di corruzione tra privati prevista dall'art. 2635 c.c., ma, anche in questo caso, distinto è l'ambito applicativo. Il primo comma, infatti, individua il destinatario della dazione o della promessa di utilità nel responsabile della revisione legale, mentre il secondo comma definisce chiaramente il contesto in cui deve essere posta in essere la condotta penalmente rilevante, ossia "l'esercizio della revisione legale dei conti".

Anche il reato di corruzione dei revisori legali è escluso dall'ambito di applicazione del D.Lgs. 231/2001.

Considerata l'omogeneità dei comportamenti previsti dalle suddette fattispecie di reato rispetto al reato di corruzione tra privati, sono state considerate a rischio anche le attività relative ai rapporti con la società di revisione.

[8] Si tratta, come spiega l'art. 1, comma 1, lett. i, del "*revisore legale cui è stato conferito l'incarico*" oppure, nel caso in cui l'incarico sia conferito ad una società di revisione legale, del soggetto "responsabile dello svolgimento dell'incarico".

## CAPITOLO L.2

### Attività Sensibili e Attività Strumentali

In relazione ai reati e alle condotte criminose sopra esplicitate, le attività ritenute più specificamente a rischio risultano essere, ai fini della presente Parte Speciale, le seguenti:

1. *Gestione degli acquisti*: l'attività ha ad oggetto l'acquisto di beni e servizi da soggetti terzi, costituiti in forma societaria. Tale attività presenta potenziali profili di rischiosità nella misura in cui la Società, al fine di ottenere forniture a prezzi fuori mercato ponga in essere comportamenti, direttamente o indirettamente, corruttivi nei confronti di esponenti della società fornitrice dei beni o dei servizi richiesti.

2. *Gestione dei clienti*: l'attività ha a oggetto la gestione dei rapporti contrattuali con potenziali clienti, costituiti in forma societaria. Sebbene la Società intrattenga rapporti contrattuali con la clientela solo indirettamente, per il tramite delle banche intermediarie, l'attività in oggetto potrebbe comunque essere esposta al rischio di commissione del reato di corruzione tra privati. Ciò nel caso in cui, ad esempio, la Società ponga in essere – anche indirettamente, tramite il proprio intermediario bancario – comportamenti corruttivi nei confronti di esponenti di una società o altro ente privato (presumibilmente cliente, o potenziale tale, dell'intermediario bancario medesimo) al fine di procurarsi la sottoscrizione di polizze assicurative da parte di tutti i dipendenti della stessa.

3. *Partecipazione a gare indette da soggetti privati*: l'attività ha ad oggetto la partecipazione a procedure di gara, *beauty contest*, organizzate da soggetti privati al fine di selezionare la fornitura di prodotti assicurativi. L'attività in oggetto si presenta potenzialmente a rischio sia in relazione ai rapporti con il soggetto che promuove e/o gestisce la procedura di gara, sia nei confronti dei competitor partecipanti alla medesima gara. Nel primo caso, infatti, potrebbero essere poste in essere condotte corruttive nei confronti di esponenti operanti per il promotore o per il gestore della gara (solitamente advisor), al fine di ottenerne l'aggiudicazione. Nel secondo caso invece le condotte corruttive potrebbero essere poste in essere nei confronti di esponenti operanti per un *competitor* al fine di escludere quest'ultimo dalla gara medesima e, quindi, avvantaggiare la Società nella competizione.

4. *Gestione dei rapporti con la società di revisione*: l'attività ha ad oggetto tutti i rapporti con la società di revisione, sia in relazione alle attività proprie dell'organo di controllo, sia in relazione all'assegnazione alla medesima di eventuali incarichi consulenziali.

In particolare, l'attività si presenta a rischio in considerazione della possibilità che la Società, attraverso i propri rappresentanti, corrompa i revisori al fine di falsificare o occultare alcune informazioni concernenti la situazione economica, patrimoniale o finanziaria della stessa, promettendo denaro o altre utilità (tra cui l'assegnazione di nuovi incarichi consulenziali).

5. *Gestione dei contenziosi*: l'attività consiste nella gestione di tutte le controversie giudiziali e stragiudiziali con assicurati o altre controparti contrattuali, costituiti in forma societaria o, comunque, in forma di ente. In particolare l'attività si presenta a rischio in considerazione della possibilità che la Società, attraverso un proprio rappresentante, corrompa un Soggetto Corruttibile operante nella struttura societaria della controparte al fine di ottenere un vantaggio nella gestione della lite (ad esempio, rinuncia, transazioni a condizioni particolarmente favorevoli ecc.).

6. *Liquidazione sinistri*: l'attività si presenta a rischio in considerazione della possibilità che un rappresentante della Società corrompa un esponente della società cliente assicurata affinché quest'ultimo ometta di denunciare un sinistro coperto da polizza assicurativa o accetti, per conto della medesima, un indennizzo notevolmente inferiore rispetto a quello effettivamente dovuto.

7. *Gestione dei rapporti infragruppo*: la Società fa parte di un Gruppo societario di livello internazionale. L'attività Sensibile in oggetto, pertanto, comprende tutte le attività di gestione e di controllo sulle operazioni compiute dalla medesima con altre società del Gruppo. Nell'ambito dell'attività in oggetto è stato rilevato il rischio astratto di corruzione (anche solo attraverso l'esercizio di pressioni o influenze illecite) di rappresentanti di altre società del Gruppo al fine di ottenere particolari vantaggi a favore della Società stessa.

8. *Richiesta e gestione di finanziamenti*: la presente attività ha ad oggetto la richiesta e la gestione di finanziamenti da parte della Società a banche e istituti di credito. Non sono compresi finanziamenti e garanzie richieste a istituti bancari o ad altre società appartenenti al Gruppo poiché tali attività rientrerebbero nell'Attività Sensibile relativa alle operazioni infragruppo.

9. *Rapporti con le imprese di riassicurazione*: la presente attività si presenta a rischio in relazione alla possibilità che la Società, attraverso i propri rappresentanti e responsabili di funzione, pongano in essere atti corruttivi nei confronti di esponenti operanti per l'impresa di riassicurazione al fine ottenere, nell'ambito della

stipulazione dei trattati riassicurativi, delle condizioni particolarmente favorevoli rispetto a quelle medie del mercato.

Nell'ambito delle attività di analisi dei rischi sono state individuate, oltre alle suddette Attività Sensibili, anche **Attività c.d. "Strumentali"** alla configurazione del medesimo reato. Queste ultime, pur non essendo direttamente esposte al rischio di commissione del reato di corruzione tra privati, costituiscono comunque attività strumentali e accessorie alla configurazione dello stesso, in quanto necessarie alla realizzazione della provvista utile al soggetto corruttore per porre in essere la condotta corruttiva (promessa o dazione di denaro o altra utilità).

Sono state individuate le seguenti Attività Strumentali alla commissione del reato di corruzione tra privati:

1. *Gestione degli omaggi, delle sponsorizzazioni ed effettuazione di altri atti di liberalità e correntezza*: il riconoscimento di omaggi o altre liberalità costituisce il tipico strumento di corruzione sia pubblica, sia privata. Tra queste rientrano anche le attività c.d. di "*caring*" del cliente o di *Partner* (quali ad esempio le colazioni o viaggi di lavoro). Inoltre (come evidenziato nella Parte Speciale A), qualsiasi prestazione gratuita erogata dalla Società a favore della clientela presenta profili di rischio in relazione alle fattispecie corruttive; in particolare, mentre gli atti di correntezza possono essere motivati da considerazioni di ordine tecnico, quelli di liberalità potrebbero essere mossi da valutazioni di opportunità commerciale e/o aziendale.
2. *Definizione delle politiche di remunerazione e incentivazione*: gli amministratori e i *manager* che sono intenzionati a porre in essere condotte corruttive potrebbero ricorrere a risorse economiche apparentemente non societarie, ma proprie. Un tipico esempio di risorse finanziarie non societarie utilizzate per corrompere soggetti terzi sono i bonus e le remunerazioni riconosciute dall'azienda: la corresponsione di remunerazioni particolarmente elevate agli amministratori e ai manager potrebbe, infatti, nascondere la "provvista" necessaria a questi ultimi per porre in essere condotte corruttive concordate a livello aziendale.
3. *Gestione dei rimborsi spese*: una modalità di utilizzo di risorse proprie per porre in essere condotte corruttive consiste nel sostenere personalmente le spese, salvo poi chiederne il relativo rimborso. È da ritenersi infatti responsabile per il reato in oggetto anche la società che dovesse consentire o agevolare il rimborso di spese

effettuate personalmente da amministratori e manager per porre in essere condotte corruttive.

4. *Selezione, assunzione e gestione del personale*: la selezione, l'assunzione e la gestione di personale dipendente sono attività tipicamente strumentalizzate per porre in essere condotte corruttive. La promessa di assunzione al soggetto corrotto o ad altro soggetto dal medesimo raccomandato costituisce infatti una merce di scambio tipicamente utilizzata dai corruttori per ottenere prestazioni a proprio vantaggio.
5. *Selezione di Consulenti, Fornitori,* Partner *e gestione dei rapporti con gli stessi*: l'assegnazione di consulenze, forniture a professionisti esterni ovvero di incarichi a *Partner* costituisce un tipico strumento per creare fondi neri da poter utilizzare per porre in essere condotte corruttive.
6. *Gestione della contabilità e dei flussi finanziari*: nell'ambito della gestione della contabilità e dei flussi finanziari potrebbero essere realizzate operazioni volte a costituire fondi neri da utilizzare a scopi corruttivi. L'attività in oggetto, inoltre, potrebbe essere utilizzata per celare (o dissimulare) eventuali dazioni passate, dando alle stesse parvenza di liceità. Il corruttore, infatti, per porre in essere la condotta corruttiva deve poter disporre di risorse finanziarie adeguate, attingendo quindi dal patrimonio aziendale. Un adeguato sistema di controlli sui flussi finanziari della Società consente di prevenire il rischio di formazione di provviste potenzialmente utili a porre in essere condotte corruttive.

## CAPITOLO L.3

## Regole e principi generali

### L.3.1 Il sistema in linea generale

Obiettivo della presente Parte Speciale è che i Destinatari del Modello si attengano – nella misura in cui gli stessi siano coinvolti nello svolgimento delle Attività Sensibili o di attività alle stesse connesse nonché in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti della Società – a regole di condotta conformi a quanto prescritto nella stessa al fine di prevenire e impedire il verificarsi del reato di corruzione tra privati.

In particolare, la presente Parte Speciale ha la funzione di fornire:

- un elenco dei principi generali nonché dei principi procedurali specifici cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- all'OdV e ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, i principi e gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica agli stessi demandati.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, i Destinatari sono tenuti, in generale, a rispettare tutte le regole e i principi disposti dalla Società e dal Gruppo alla quale la stessa appartiene.

### L.3.2 Principi generali di comportamento

In generale, è vietato a tutti i Destinatari del presente Modello porre in essere condotte che possano, direttamente o indirettamente, configurare il reato di corruzione tra privati. In particolare, è fatto divieto a tutti i Destinatari del presente Modello di:

a. promettere, concedere o autorizzare qualunque remunerazione indebita o ogni altro vantaggio a favore di esponenti, a qualsiasi titolo, di società, consorzi o altri enti privati;
b. effettuare pagamenti in favore di soggetti che, rispetto ai contratti stipulati, non hanno alcun ruolo specifico nell'erogazione della prestazione resa alla Società, senza preventiva autorizzazione da parte delle funzioni competenti;
c. servirsi di intermediari, quali agenti, Fornitori, Consulenti o altri terzi al fine di convogliare i pagamenti da destinare, a scopo corruttivo, a esponenti di società o enti privati, a loro amici o familiari nonché a società, partiti politici, associazioni no *profit*, dipendenti o *Partner* degli stessi.

Tutti i Destinatari del presente Modello e in particolare coloro che intrattengono rapporti commerciali con clienti (attuali o potenziali tali), *Partner*, Consulenti e qualsiasi altra controparte contrattuale, sono tenuti ad adottare condotte trasparenti, virtuose, leali e corrette, nel pieno rispetto della normativa nazionale, regolamentare e aziendale vigente, anche a tutela della libera e corretta concorrenza tra imprese.

Inoltre, tutti i Destinatari del presente Modello si impegnano a comunicare all'OdV, secondo le modalità specificamente previste nella Parte Generale del presente Modello, qualsiasi comportamento che possa direttamente o indirettamente configurare un'ipotesi di reato di corruzione tra privati o istigazione alla corruzione tra privati.

La Società, a sua volta, al fine di prevenire condotte di tipo corruttivo:

a. assicura che i poteri di spesa siano adeguati ai ruoli e alle responsabilità ricoperte nell'organigramma aziendale, nonché alle esigenze di operatività ordinaria della Società;
b. adotta politiche di remunerazione in coerenza con le disposizioni regolamentari vigenti e piani di incentivazione per il *management* in linea con gli obiettivi strategici, la redditività e l'equilibrio dell'impresa nel lungo termine, evitando politiche basate in modo esclusivo o prevalente su risultati difficilmente raggiungibili e/o tali da indurre i destinatari ad esporsi a tenere comportamenti illeciti;
c. nella gestione delle finanze e della contabilità, adotta procedure aziendali idonee ad assicurare che tutti i flussi finanziari in entrata e in uscita siano correttamente e regolarmente tracciati e che non siano creati conti segreti o scritture non registrate;
d. assicura che la selezione e l'assunzione del personale dipendente avvenga nel rispetto delle procedure aziendali che prevedono criteri di valutazione basati sulla professionalità e sul merito dei candidati;
e. vieta il conferimento di incarichi consulenziali a soggetti terzi che abbiano come unico scopo quello di utilizzarli come canale per qualsiasi pratica corruttiva nonché l'effettuazione di prestazioni in favore dei Consulenti e dei *Partner* che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi ovvero il riconoscimento di compensi in favore dei medesimi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti nel settore;
f. è fatto divieto di distribuire omaggi al di fuori di quanto previsto dalle *policy* aziendali (vale a dire ogni forma di omaggio offerto eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione

di qualsiasi attività aziendale). Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore e, pertanto, non potranno essere superiori a Euro 150 annuali per singolo destinatario, salvo deroghe approvate per iscritto (a livello generale per categorie di omaggi o in modo specifico per singoli omaggi) dall'Amministratore Delegato con l'indicazione della motivazione sottesa al compimento dell'atto di liberalità;

g. è fatto divieto di accettare qualsiasi tipo di regalo d'affari e/o di vantaggio che possa compromettere l'indipendenza, l'imparzialità e l'integrità dei dipendenti (o dei componenti degli Organi Sociali) della Società. A questo fine, la Società ha fissato un importo pari a Euro 150 quale limite massimo di valore per gli omaggi ricevuti sia da clienti sia da Fornitori sia da terzi in genere. Tale limite si intende su base annua;
h. per i contratti di assicurazione contro i danni, è vietato ricevere denaro contante a titolo di pagamento di premi di importo superiore a Euro 750,00 annui (Euro settecentocinquanta) per ciascun contratto; il limite di incasso di premi in contanti per il ramo r.c. auto è invece quello stabilito *ex lege* dal D.Lgs. 21 novembre 2007, n. 231.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, codici di comportamento, *policy* e procedure aziendali.

Tali *policy* e procedure e loro eventuali successive integrazioni o modifiche si considerano parte integrante del Modello e, pertanto, si devono intendere come recepite nella loro configurazione.

## CAPITOLO L.4

## Principi procedurali specifici

### L.4.1 Principi procedurali specifici generalmente applicabili

Ai fini dell'attuazione dei principi e regole generali e dei divieti elencati al precedente cap. L.3, devono rispettarsi gli specifici principi procedurali qui di seguito descritti, oltre alle regole e principi generali già contenuti nella Parte Generale del Modello. Le regole qui di seguito descritte devono essere rispettate sia nell'esplicazione dell'attività della Società in territorio italiano sia eventualmente all'estero.

1. *Gestione degli acquisti*

a. La Società prevede:

- la definizione di ruoli e responsabilità nel processo di selezione e assegnazione degli incarichi e delle forniture ai Consulenti o ai Fornitori;
- la valutazione comparativa di almeno tre offerte contrattuali da parte di Consulenti e Fornitori diversi, salvo deroghe espressamente previste nelle procedure interne;
- la selezione dei Fornitori e dei Consulenti sulla base del possesso di adeguati requisiti di professionalità e onorabilità, richiedendo eventualmente anche la documentazione idonea a comprovarne la sussistenza.

b. Nell'ambito dei rapporti con i Consulenti e i Fornitori, la Società prevede:

- che vi sia un contratto scritto che regoli condizioni e termini del rapporto;
- che i contratti con i Consulenti e i Fornitori contengano (anche in caso di rinnovo) la Clausola 231.
- che, in conformità con le indicazioni fornite a livello di Gruppo, i contratti con i Consulenti e i Fornitori prevedano il rispetto da parte dei medesimi delle normative nazionali e/o internazionali applicabili;
- che i pagamenti a titolo di corrispettivo per le prestazioni svolte dai Consulenti siano effettuati solo ed esclusivamente su conti correnti intestati ai Consulenti medesimi presso istituti di credito;
- che gli anticipi di pagamento siano riconosciuti solo se adeguatamente motivati nel contratto di consulenza o di fornitura;

- il divieto di porre in essere qualsiasi comportamento che, direttamente o indirettamente, possa configurare Reati Presupposto (tra cui i reati di corruzione tra privati), pena la risoluzione del relativo contratto.

c. La Società istituisce inoltre un sistema di controlli ex-post sulla conformità del prezzo pagato rispetto al preventivo autorizzato, nonché sulla effettiva esecuzione del servizio contrattualmente pattuito.

2. *Gestione dei clienti*

a. In relazione all'attività di business development e in particolare ai rapporti con la clientela, attuale o potenziale tale, la Società adotta procedure e/o policy aziendali e/o circolari interne dispositive che prevedono:

- l'obbligo di tenere comportamenti trasparenti, leali e virtuosi in tutti i rapporti con la clientela, dalla prima fase di promozione e vendita dei prodotti assicurativi alla successiva fase di gestione dei rapporti contrattuali con i clienti già acquisiti, soprattutto in fase di rimborso e liquidazione e, con particolare riguardo alla clientela corporate (società);

- controlli sul rispetto delle procedure aziendali nei casi di autorizzazione ad operare oltre i poteri negoziali prestabiliti.

b. Con particolare riguardo ai rapporti intrattenuti dagli intermediari con la clientela, la Società stabilisce contrattualmente:

- il divieto di porre in essere qualsiasi comportamento che possa, direttamente o indirettamente, configurare un reato di corruzione tra privati nell'interesse o vantaggio della Società, pena la facoltà per quest'ultima di risolvere di diritto il rapporto contrattuale vigente;

- obblighi di correttezza, chiarezza e trasparenza a carico degli intermediari, affinché questi ultimi non pongano in essere alcuna condotta corruttiva a favore e/o nell'interesse della Società;

- compensi provvigionali adeguati all'attività svolta dagli intermediari e conformi alle disposizioni normative e regolamentari vigenti, affinché non siano in alcun modo corrisposti, direttamente o indirettamente, compensi a titolo di incentivo per il compimento di condotte corruttive nell'interesse o vantaggio della Società;

- attività di controllo da parte della Società sulle modalità di gestione dei rapporti con la clientela "*corporate*" da parte degli intermediari medesimi.

3. *Partecipazione a gare indette da soggetti privati*

a. Nell'ambito delle attività di partecipazione a gare private per l'assegnazione di forniture di prodotti assicurativi, la Società si attiene strettamente ai regolamenti emessi dai promotori della gara e adotta i seguenti presidi procedurali:

- ogni decisione concernente la partecipazione a gare private per la stipulazione di polizze assicurative è preceduta da una valutazione oggettiva sull'effettiva capacità della Società medesima a soddisfare le richieste dei promotori / committenti. Tale valutazione è effettuata dalle funzioni competenti tenendo in considerazione le dimensioni della Società, i prodotti e le condizioni di assicurazione che la stessa è in grado di offrire;

- in caso di partecipazione ad una gara privata: a) vengono individuati i soggetti coinvolti nella relativa attività e un referente con funzioni di coordinamento; b) vengono attribuiti a ciascun soggetto coinvolto specifici compiti e responsabilità relativi alla predisposizione della documentazione e alla partecipazione ad eventuali incontri con le commissioni di gara; c) viene mantenuta traccia scritta delle attività svolte; d) a conclusione della procedura di gara il referente relaziona all'Amministratore Delegato ed, eventualmente, al Consiglio di Amministrazione le attività svolte; e) in caso di aggiudicazione, la Società conserva copia del verbale di assegnazione.

b. è vietato, infine, intraprendere qualsiasi tipo di rapporto, formale o informale, diretto o indiretto, con i competitor partecipanti alla medesima gara.

4. *Gestione dei rapporti con la società di revisione*

a. Nell'ambito dei rapporti con i revisori legali, la Società:

- collabora con gli organi di controllo fornendo tutte le informazioni necessarie allo svolgimento dell'incarico assegnato;

- individua all'interno della propria organizzazione i soggetti, appartenenti alle diverse funzioni, incaricati di relazionarsi con i revisori legali al fine di fornire le informazioni necessarie allo svolgimento dell'incarico assegnato;

- verifica che nel caso siano attribuiti alla Società di revisione, ai revisori e a qualsiasi altra entità appartenente alla sua rete, incarichi diversi dalla revisione legale, che questi non influenzino – direttamente e indirettamente – la relativa indipendenza.

5. *Gestione dei contenziosi*:

a. Nella gestione del contenzioso giudiziale e stragiudiziale la Società adotta specifiche procedure aziendali volte a stabilire:

- i ruoli e le responsabilità dei soggetti incaricati di gestire il contenzioso medesimo;
- i criteri per definire le controversie in sede giudiziale o stragiudiziale;
- le modalità di gestione delle stesse nei rapporti con i difensori e le controparti. In particolare:

  - nella gestione del contenzioso giudiziale o arbitrale la Società affida il mandato alle liti a difensori, selezionati sulla base delle procedure in vigore, e che si impegnino contrattualmente a non porre in essere alcun tipo di condotta, direttamente o indirettamente, idonea, anche solo in via strumentale, a configurare un reato di corruzione tra privati, a pena di revoca del mandato stesso.
  - nella gestione del contenzioso stragiudiziale, la negoziazione di accordi transattivi o conciliativi viene seguita da almeno due soggetti e viene mantenuta traccia di ogni fase della stessa.

b. La Società tiene un elenco di tutti contenziosi pendenti e dei mandati conferiti ai difensori.

6. *Liquidazione sinistri*:

a. La liquidazione dei sinistri deve essere eseguita nel rispetto delle procedure aziendali che ne regolano l'*iter* e che garantiscono parità di trattamento tra tutti gli assicurati.

b. In relazione alla liquidazione dei sinistri, la Società deve prevedere:

- l'individuazione dei soggetti incaricati a raccogliere le richieste di liquidazione dei sinistri, a gestire le pratiche stesse, ad autorizzare e ad effettuare i pagamenti, garantendo il rispetto del principio di separazione dei ruoli;
- l'adozione di strumenti informatici che prevedono il calcolo automatico degli importi da rimborsare e liquidare, assicurando quindi oggettività nella

determinazione di tali importi e parità di trattamento tra tutti i soggetti destinatari dei pagamenti in oggetto;

- la formalizzazione scritta e/o informatizzata di tutti i flussi informativi intercorrenti tra i soggetti coinvolti nella gestione dei sinistri, nonché della corrispondenza intercorrente con gli assicurati.

7. *Gestione dei rapporti infragruppo*

a. in relazione alle operazioni poste in essere con altre società del Gruppo, la Società:

- rispetta le disposizioni regolamentari previste in materia di operazioni infragruppo e di operazioni con parti correlate, adottando linee guida che, nel rispetto del principio della sana e prudente gestione, vietino l'attuazione di operazioni che possano produrre effetti negativi o arrecare pregiudizi agli interessi della controparte;
- in qualsiasi caso di dubbio, prevede l'obbligo di verificare con le funzioni competenti se le controparti contrattuali – persone fisiche e persone giuridiche – possano considerarsi appartenenti al Gruppo o comunque parti correlate;
- adotta sistemi di autorizzazione delle operazioni con parti correlate che prevedano:
  1) verifica di congruità del prezzo dell'operazione rispetto alle condizioni di mercato;
  2) approvazione dell'operazione da parte di soggetti specificamente individuati e dotati di poteri autorizzativi proporzionali alla tipologia di operazioni e al valore delle stesse.

*8.* *Richiesta e gestione di finanziamenti*:

*a*) la Società nell'ambito dei rapporti bilaterali con istituti di credito per l'ottenimento di finanziamenti prevede un sistema autorizzativo e organizzativo che:

- definisca i ruoli e le responsabilità delle principali funzioni coinvolte e
- assicuri la tracciabilità dei contatti intrapresi con le controparti al fine di monitorare eventuali condotte volte a: (i) influenzare l'istruttoria posta in essere dall'istituto di credito, propedeutica all'erogazione del finanziamento e alla determinazione dei termini e condizioni del relativo rapporto contrattuale; (ii) richiedere modifiche indebite alle condizioni di restituzione del finanziamento contrattualmente stabilite.

8. *Rapporti con le imprese di riassicurazione*

a) In relazione ai rapporti con le imprese di riassicurazione, la Società adotta presidi idonei a garantire che:

- siano garantiti ruoli e responsabilità delle principali funzioni coinvolte;
- sia garantita la tracciabilità dei contratti intrapresi con le controparti.

Al fine di prevenire il rischio di commissione dei reati di corruzione tra privati la Società, inoltre, si impegna ad adottare e far rispettare i seguenti princìpi di comportamento specifici relativi alle Attività Strumentali:

1. *Gestione degli omaggi, delle sponsorizzazioni ed effettuazione di altri atti di liberalità e correntenzza*

a. La Società adotta specifici presidi volti a disciplinare le finalità, le modalità e i limiti per l'offerta di omaggi e sponsorizzazioni e per l'effettuazione di altri atti di liberalità e correntenzza. Ciò al fine di assicurare che le medesime non influenzino impropriamente o possano essere recepite come capaci di influenzare l'indipendenza di giudizio dei soggetti terzi beneficiari, quali – a titolo esemplificativo e non esaustivo – clienti, partiti politici, associazioni no profit ecc. In particolare, anche tramite l'adozione di procedure, la Società:

- vieta che siano effettuati – senza preventiva e specifica autorizzazione – omaggi, liberalità e ogni altra forma di elargizione a organizzazioni o a soggetti (familiari, parenti o amici) che siano, direttamente o indirettamente, correlati con soggetti corruttibili;
- prevede che gli omaggi, le liberalità e ogni altra forma di elargizione siano limitati a importi ragionevoli e legittimi – di valore tale da non poter essere percepiti come impropriamente influenti l'indipendenza di giudizio del beneficiario nei confronti del donatore – nonché supportati da motivazioni specifiche (espresse per iscritto) e da idonea documentazione;
- definisce – nel rispetto del principio di segregazione dei ruoli – le modalità, i compiti e le responsabilità dei soggetti coinvolti nel processo di richiesta, valutazione e autorizzazione a procedere all'esecuzione di omaggi, liberalità e ogni altra forma di elargizione;

- prevede l'istituzione di un elenco di tutti gli omaggi, le liberalità e le elargizioni effettuati a beneficio di soggetti terzi nonché ricevuti da amministratori, sindaci, dirigenti e dipendenti della Società medesima;
- prevede che tutti gli omaggi, le liberalità e le altre forme di elargizione debbano essere autorizzati nel rispetto dei *budget* assegnati alle funzioni che, di volta in volta, ne richiedono l'esecuzione;
- di tutte le elargizioni deve essere informato anche l'OdV; se ritenuto opportuno dal *manager* che ha proposto l'erogazione liberale / donazione / sponsorizzazione, di tale azione può essere informato anche il Comitato Esecutivo (o Comex);
- le sponsorizzazioni al pari degli omaggi e regali sono mappate in apposito registro tenuto dall'unita aziendale preposta.

  L'*iter* da seguire per l'effettuazione di una sponsorizzazione prevede le seguenti fasi: (i) fase di analisi della documentazione; (ii) fase contrattuale (gestita secondo le linee guida aziendali in base all'importo della sponsorizzazione); (iii) controllo dell'utilizzo dei fondi; (iv) tracciabilità delle singole operazioni.

b. Sull'ammissibilità di eventuali eccezioni a regole previste in materia di omaggi o regalie è previsto il coinvolgimento del vertice aziendale e (a livello informativo) dell'Organismo di Vigilanza.

c. La Società garantisce una reportistica periodica verso l'Organismo di Vigilanza circa le sponsorizzazioni, gli omaggi e le donazioni effettuate nel periodo di riferimento.

2. *Definizione delle politiche di remunerazione e incentivazione*

a. La Società adotta politiche di remunerazione degli amministratori e di incentivazione del management e del personale dipendente che siano in linea con gli obiettivi, le strategie economiche, i valori e gli obiettivi di lungo periodo. In particolare, la politica di remunerazione e i piani di incentivazione:

- sono approvati dall'assemblea dei soci e definiti per iscritto in modo chiaro e trasparente;
- prevedono un adeguato equilibrio tra componenti fisse e componenti variabili;
- prevedono che le componenti variabili degli incentivi e delle remunerazioni siano limitate a determinati importi e siano subordinate al raggiungimento di risultati predeterminati e quantitativamente / qualitativamente misurabili;

- evitano che i sistemi premianti dei soggetti con poteri di spesa o facoltà decisionali a rilevanza esterna siano basati su *target* di *performance* sostanzialmente irraggiungibili;
- includono una revisione delle competenze etiche aziendali nella valutazione e nella promozione di dirigenti e funzionari, misurando il raggiungimento degli obiettivi non soltanto rispetto al conseguimento di *target* finanziari ma anche rispetto alle modalità con cui tali obiettivi sono stati conseguiti e in particolare alla conformità dei comportamenti tenuti rispetto alla presente Parte Speciale e alla normativa aziendale;
- prevedono un aggiornamento periodico per assicurare che le remunerazioni e i piani di incentivazione siano adeguati ai mutamenti aziendali intervenuti;
- prevedono sistemi di controllo finalizzati a verificare la coerenza delle remunerazioni e delle incentivazioni riconosciute agli amministratori, ai dirigenti e ai dipendenti rispetto alla politica e ai piani aziendali, nonché l'effettivo raggiungimento degli obiettivi prestabiliti.

b. La definizione degli obiettivi assegnati a tutte le figure disciplinate dal Regolamento Ivass 38/2018 è effettuata in accordo con i Direttori delle Aree *Compliance* e *Risk Management* e Controlli Permanenti.

3. *Gestione dei rimborsi spese*

a. La Società garantisce la previsione di specifici limiti e modalità per il rimborso di spese anticipate da esponenti aziendali e dipendenti;

b. l'utilizzo di carte di credito aziendali o carte prepagate è consentito solo a soggetti specificamente individuati dal vertice aziendale;

c. tutte le spese di viaggio e di rappresentanza sostenute dal personale e dai Fornitori/Consulenti della Società devono essere comprovate da idonea documentazione e giustificate da stretta attinenza all'attività lavorativa;

d. il rimborso delle spese sostenute avviene con modalità tracciabili.

4. *Selezione, assunzione e gestione del personale*

a. La Società adotta procedure di selezione, assunzione e gestione del personale dipendente di qualsiasi livello e di collaboratori a progetto che garantiscono (anche nel caso in cui tali attività siano in parte affidate a società di *head hunting*):

- parità di accesso a tutti i candidati;

- modalità di scelta basate su criteri di meritocrazia, professionalità e onorabilità dei candidati.

b. La Società conserva la documentazione esibita in sede di assunzione anche al fine di consentirne la consultazione da parte dell'OdV nell'espletamento della consueta attività di vigilanza e controllo.

c. La Società mette a disposizione dei neoassunti copia del Modello 231 e del Codice Etico con la richiesta di prenderne visione e di impegnarsi al rispetto dei principi contenuti negli stessi.

c. La Società prevede contrattualmente che il datore di lavoro somministrante accerti la sussistenza dei requisiti di onorabilità dei propri dipendenti, consentendo alla Società di risolvere con effetto immediato il contratto di somministrazione di attività lavorativa qualora il dipendente somministrato risultasse indagato o condannato per reati di cui al D.Lgs. 231/2001.

d. La Società consente l'effettuazione di segnalazioni di candidature da parte di Dipendenti (cosiddetto "*referral*") nel rispetto di apposito regolamento interno e delle procedure di selezione e assunzione del personale.

e. Il processo di inserimento della risorsa all'interno della Società deve avvenire nel rispetto degli obblighi di formazione e aggiornamento previsti dalle procedure aziendali in base al ruolo e all'attività svolta all'interno dell'azienda.

f. Eventuali avanzamenti interni di carriera e riconoscimenti di premi (ivi compresa l'eventuale previsione, nel trattamento retributivo, di una componente variabile legata al raggiungimento di specifici obiettivi) devono essere assegnati secondo criteri oggettivi basati sulla parità di trattamento, sulla valorizzazione del merito e della professionalità nonché sul rispetto della normativa aziendale.

5. *Selezione di Consulenti, Fornitori e* Partner *e gestione dei rapporti con gli stessi*

a. La Società verifica l'attendibilità commerciale e professionale dei Fornitori, Partner e dei Consulenti.

b. La Società adotta procedure o *policy* aziendali volte a garantire che il processo di selezione dei Fornitori, dei *Partner* e del Consulenti avvenga nel rispetto dei criteri di trasparenza, pari opportunità di accesso, professionalità, affidabilità ed economicità, fermo restando la prevalenza dei requisiti di legalità rispetto a tutti gli altri.

c. La Società tiene traccia dei Consulenti, Fornitori, *Partner* e altre controparti con i quali siano già intercorsi rapporti contrattuali.

d. La Società si impegna, in occasione di ogni rinnovo contrattuale con Fornitori, *Partner* e Consulenti, a richiedere la sottoscrizione da parte di questi ultimi di un'autodichiarazione circa la persistenza dei requisiti di onorabilità che in fase di selezione iniziale hanno permesso l'instaurazione del rapporto.

e. I rapporti tra CAA e i Consulenti, i Fornitori e i *Partner* devono essere definiti per iscritto in tutte le loro condizioni e termini e rispettare quanto indicato ai successivi punti.

f. I contratti con i Consulenti, i Fornitori e i *Partner* devono contenere (anche in caso di rinnovo) la Clausola 231.

g. In conformità con le indicazioni fornite a livello di Gruppo, i contratti con i Consulenti, i Fornitori e i *Partner* prevedono, inoltre, il rispetto da parte dei medesimi delle normative nazionali e/o internazionali applicabili.

h. A integrazione dei principi sopra esposti, nel caso di instaurazione di rapporti continuativi con controparti contrattuali, la Società si impegna ad attuare efficacemente controlli periodici circa

   - la persistenza in capo a questi ultimi dei requisiti che in fase di selezione iniziale hanno permesso l'instaurazione del rapporto;
   - l'effettiva prestazione della consulenza/fornitura e la congruità del prezzo pattuito.

6. *Gestione della contabilità e dei flussi finanziari*

   a. La Società adotta procedure specificamente finalizzate a regolare i processi di tenuta della contabilità. In particolare, tale procedura prevede:

      - la registrazione a livello informatico di tutte le voci di spesa;
      - controlli specifici su: a) la coerenza delle dei pagamenti rispetto ai corrispettivi pattuiti contrattualmente; b) l'avvenuta esecuzione dei delle prestazioni rese da soggetti terzi all'organizzazione aziendale; c) il rispetto del *budget* assegnato a ciascuna funzione per l'esercizio delle attività di propria competenza.

   b. La Società adotta sistemi contabili idonei ad assicurare che:

- tutti i flussi finanziari in entrata e in uscita siano adeguatamente identificabili e tracciabili, nonché correttamente e regolarmente registrati in appositi libri e registri contabili;
- tutti i flussi finanziari in entrata e in uscita siano supportati da specifica documentazione giustificatrice, che riporti chiaramente e fedelmente le transazioni a cui fa riferimento;
- sia rispettato il principio di segregazione dei ruoli tra i soggetti che autorizzano, coloro che eseguono e coloro che controllano i flussi finanziari in entrata e in uscita;
- siano rispettati i limiti di spesa e i budget assegnati ai soggetti che richiedono l'esecuzione di flussi finanziari in uscita;
- non siano creati conti segreti o scritture non registrate e che non siano effettuati pagamenti per spese inesistenti o elementi di passività il cui oggetto non sia correttamente identificato;
- il denaro contante sia utilizzato solo per pagamenti di piccola cassa e supportati da documentazione idonea a comprovare l'effettivo pagamento.

## CAPITOLO L.5

## I controlli dell'OdV e i flussi informativi

### L.5.1 Il controllo in generale

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati di cui alla presente Parte Speciale sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati quivi previsti. Con riferimento a tale punto l'OdV - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà alle funzioni competenti eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative dei principi ivi previsti;
- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti, l'OdV può incontrare:

a) il responsabile delle funzioni Commerciale e *Marketing* al fine di verificare che le prassi commerciali siano in linea con i principi previsti nella presente Parte Speciale;

b) il Responsabile della Direzione Investimenti e ALM al fine di accertare che la gestione del patrimonio e tutti i flussi finanziari avvengano nel rispetto delle procedure aziendali e dei principi procedurali previsti nella Presente Parte Speciale al fine di prevenire la commissione del reato di corruzione tra privati;

c) il Responsabile della funzione Risorse Umane, *Property* e *Mobility Management* al fine di accertare che la selezione delle risorse umane non sia strumentalizzata per ottenere favori a vantaggio della Società;

d) qualsiasi altro Responsabile di funzione o dipendente che possa fornire informazioni utili in merito all'attuazione dei presidi previsti nella presente Parte Speciale per prevenire il rischio di commissione del reato di corruzione tra privati.

È altresì attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

Al fine di dare attuazione ai principi di cui alle lett. da a) a d) che precedono, la Società valuta l'istituzione di flussi informativi proceduralizzati nei confronti dell'OdV. Tali flussi

informativi dovranno essere idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio delle anomalie rilevanti ai sensi della presente Parte Speciale e delle criticità rilevate in tale ambito.

Fermo restando quanto appena indicato, l'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verifichino violazioni ai principi procedurali specifici contenuti nella presente Parte Speciale ovvero alle procedure, *policy* e normative aziendali attinenti alle aree sensibili sopra individuate.

Per i flussi informativi si rimanda alla compilazione da parte delle funzioni competenti delle "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento) che costituiscono un allegato al Modello.

**PARTE SPECIALE – M –**

**Reati tributari**

## CAPITOLO M.1

### Le fattispecie dei reati tributari

Il Decreto Legge 26 ottobre 2019, n. 124 recante "*Disposizioni urgenti in materia fiscale e per esigenze indifferibili*", convertito con modificazioni dalla Legge 19 dicembre 2019, n. 157 (entrata in vigore il 25 dicembre 2019) ha introdotto nel D.Lgs. 231/2001 l'art. 25-*quinquiesdecies* ("***Reati tributari***").

Al fine di assicurare una corretta comprensione della presente Parte Speciale da parte di tutti i Destinatari del presente Modello, vengono di seguito descritte le fattispecie previste dal D.Lgs. 5 novembre 2024, n. 173 (e in precedenza dal D. Lgs. 10 marzo 2000, n. 74[9]) che assumono rilevanza in relazione all'attività svolta dalla Società.

#### *DICHIARAZIONE FRAUDOLENTA MEDIANTE USO DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 74 D.LGS. 173/2024, GIÀ 2 D.LGS. 74/2000)*

Il reato in oggetto è commesso da chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indichi in una delle dichiarazioni relative a dette imposte elementi passivi fittizi. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria. È prevista una pena più mite se l'ammontare degli elementi passivi fittizi è inferiore a Euro centomila.

#### *DICHIARAZIONE FRAUDOLENTA MEDIANTE ALTRI ARTIFICI (ART. 75 D.LGS. 173/2024, GIÀ ART. 3 D.LGS. 74/2000)*

Fuori dai casi previsti dall'articolo precedente, il reato in oggetto è commesso da chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indichi in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi o crediti e ritenute fittizi,

[9] Si precisa che il D.Lgs. 5 novembre 2024, n. 173, recante il "*Testo unico delle sanzioni tributarie amministrative e penali*" raccoglie le disposizioni penali in materia tributaria e la disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto. In particolare, nella seconda parte del Testo Unico, è stato recepito (a far data dal 1° gennaio 2026) il testo del D.Lgs. 10 marzo 2000, n. 74, dedicato ai reati tributari.

quando, congiuntamente: *a)* l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a Euro trentamila; *b)* l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a Euro unmilionecinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a Euro trentamila. Anche per tale fattispecie, è previsto che il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria. Non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

***EMISSIONE DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 79 D.LGS. 173/2024, GIÀ ART. 8 D.LGS. 74/2000)***

Il reato in oggetto è commesso da chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emetta o rilasci fatture o altri documenti per operazioni inesistenti. Al comma 2, viene precisato che l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato. È prevista una pena più mite se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a Euro centomila.

***OCCULTAMENTO O DISTRUZIONE DI DOCUMENTI CONTABILI (ART. 81 D.LGS. 173/2024, GIÀ ART. 10 D.LGS. 74/2000)***

Il reato in oggetto è commesso da chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulti o distrugga, in tutto o in parte, le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

***SOTTRAZIONE FRAUDOLENTA AL PAGAMENTO DI IMPOSTE (ART. 85 D.LGS. 173/2024, GIÀ ART. 11 D.LGS. 74/2000)***

La fattispecie prevista al primo comma dell'articolo in oggetto è commessa da chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi

o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore a Euro cinquantamila, alieni simulatamente o compia altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. È prevista una pena più severa se l'ammontare delle imposte, sanzioni ed interessi è superiore a Euro duecentomila. La fattispecie prevista al secondo comma è commessa da chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indichi nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi per un ammontare complessivo superiore ad Euro cinquantamila. È prevista una pena più severa se l'ammontare delle imposte, sanzioni ed interessi è superiore a Euro duecentomila.

****

L'art. 25-*quinquiesdecies* del D. Lgs. 231/2001 è poi stato integrato dal D.Lgs. 14 luglio 2020, n. 75. In particolare, tale ultimo decreto ha aggiunto all'art. 25-*quinquiesdecies* un nuovo comma 1-*bis* (poi modificato dal D.Lgs. 4 ottobre 2022, n. 156), ai sensi del quale viene previsto il richiamo ai reati di dichiarazione infedele, di omessa dichiarazione e di indebita compensazione, che acquisiscono rilevanza, ai fini della responsabilità amministrativa degli enti, laddove siano commessi al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegua o possa conseguire un danno complessivo pari o superiore dieci milioni di euro.

Nonostante sulla base dell'analisi dei rischi condotta, la configurabilità di tali condizioni sia apparsa prettamente astratta e remota, la presente Parte Speciale prevede princìpi valevoli anche quale presidio del rischio di commissione di dette fattispecie.

## CAPITOLO M.2

### Attività Sensibili nell'ambito dei Reati tributari

Le principali Attività Sensibili, nell'ambito dei reati trattati nella presente Parte Speciale, che la Società ha individuato sono le seguenti:

1. **Predisposizione delle dichiarazioni e gestione degli adempimenti fiscali**: tale attività assume rilevanza in considerazione del possibile utilizzo di stratagemmi (come, ad esempio, l'interposizione fittizia di società), che determino la redazione di una dichiarazione fiscale inveritiera, al fine di evadere le imposte.

2. **Conservazione delle scritture contabili e degli altri documenti di cui sia obbligatoria la conservazione per fini fiscali**: tale attività assume rilevanza in relazione al reato di occultamento o distruzione di scritture rilevanti ai fini fiscali, che potrebbe essere configurabile – ad esempio – laddove la Società distruggesse le scritture contabili al fine di rendere impossibile per l'Agenzia delle Entrate la ricostruzione degli affari.

3. **Selezione dei Consulenti (in materia contabile e fiscale)**: l'attività in oggetto rileva per il caso in cui la gestione o il supporto nella gestione degli adempimenti contabili e fiscali vengano affidati a soggetti terzi, quali i Consulenti.

4. **Gestione dei rapporti con l'Amministrazione fiscale**: si tratta della gestione degli scambi informativi (ad esempio, le risposte a questionari inviati dall'Agenzia delle Entrate) e, in generale, dei rapporti tra la Società e le Autorità competenti in ambito fiscale.

5. **Contabilità e fatturazione (anche infragruppo)**: tali processi costituiscono un'attività sensibile per la commissione di Reati tributari, con riferimento – ad esempio – all'ipotesi di utilizzo in dichiarazione fiscale di una fattura per operazione inesistente.

## CAPITOLO M.3

### Regole e princìpi generali

Obiettivo della presente Parte Speciale, al fine di prevenire la commissione dei Reati nella stessa considerati, è che tutti i Destinatari del Modello si attengano al rispetto di tutte le procedure e dei princìpi che siano direttamente o indirettamente funzionali alla prevenzione di condotte idonee a integrare le fattispecie di reato tributario sopra richiamate.

I Destinatari dovranno attenersi ai seguenti princìpi di condotta:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le Attività Sensibili individuate nella presente Parte Speciale;
2. agevolare il monitoraggio del rispetto dei princìpi che regolano la compilazione, tenuta e conservazione delle dichiarazioni di natura contabile rilevanti ai fini fiscali;
3. attuare la cosiddetta "segregazione dei ruoli" nella gestione della contabilità aziendale e nel processo di predisposizione delle dichiarazioni fiscali;
4. garantire la massima correttezza nell'ambito dei rapporti con l'amministrazione fiscale e la massima trasparenza nella comunicazione di dati e informazioni alla stessa;
5. adottare modalità trasparenti e tracciabili per eventuali operazioni su *asset*;
6. non pregiudicare in alcun modo le ragioni dell'erario (anche in relazione alla soddisfazione di eventuali pagamenti di imposte ovvero di interessi o sanzioni amministrative relativi a dette imposte).

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, codici di comportamento, policy e procedure aziendali.

Tali *policy* e procedure e loro eventuali successive integrazioni o modifiche si considerano parte integrante del Modello e, pertanto, si devono intendere come recepite nella loro configurazione.

## CAPITOLO M.4

### Principi procedurali specifici

Ai fini dell'attuazione dei principi e regole generali e dei divieti elencati al precedente capitolo, devono rispettarsi gli specifici principi procedurali qui di seguito descritti, oltre alle regole e principi generali già contenuti nella Parte Generale del Modello.

1. *Predisposizione delle dichiarazioni e gestione degli adempimenti fiscali*

Nella predisposizione delle dichiarazioni annuali relative alle imposte sui redditi e sul valore aggiunto, la Società garantisce che:

a) vi sia segregazione dei ruoli tra i soggetti che predispongono le dichiarazioni fiscali e i soggetti deputati ai relativi controlli;

b) sia garantito sempre il controllo anche da parte della società di revisione e del collegio sindacale;

c) non vengano indicati elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi;

d) non venga indicata una base imponibile in misura inferiore a quella effettiva (ad esempio costi fittiziamente sostenuti e/o ricavi indicati in misura inferiore a quella reale) facendo leva su una falsa rappresentazione nelle scritture contabili obbligatorie e/o avvalendosi di mezzi idonei ad ostacolarne l'accertamento;

e) non vengano posti in compensazione crediti inesistenti e non spettanti;

f) non siano fatti decorrere inutilmente i termini previsti dalla normativa applicabile per la presentazione delle dichiarazioni fiscali così come per il successivo versamento delle imposte dovute.

2. *Conservazione delle scritture contabili e degli altri documenti di cui sia obbligatoria la conservazione per fini fiscali*

In un'ottica di massima trasparenza, la Società cura che le scritture contabili e fiscali nonché tutti i documenti alla base e a supporto delle stesse:

a) siano conservati per un congruo lasso di tempo, eventualmente anche su supporti informatici, a patto che sia garantita l'affidabilità del sistema di conservazione nonché l'immodificabilità della documentazione;

b) siano conservati in maniera tale da renderli prontamente disponibili in caso di verifica.

3. *Selezione dei Consulenti (in materia contabile e fiscale)*

La Società – oltre ai presidi previsti diffusamente nell'ambito di altre Parti Speciali – garantisce:

a) che i Consulenti siano scelti, nell'ambito delle deleghe/procure conferite al singolo procuratore, avendo riguardo unicamente alle competenze, esperienze, *curriculum* degli stessi e con contratto definito per iscritto;

b) che, in sede di selezione dei Consulenti, venga verificata – *inter alia* – la sussistenza del requisito di professionalità in capo agli stessi (ad esempio, domandando loro prova dell'iscrizione all'eventuale albo di riferimento);

c) che nei contratti con i Consulenti sia contenuta apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al Decreto 231 e delle sue implicazioni per la Società, di non essere mai stati implicati in procedimenti giudiziari relativi ai reati nello stesso contemplati (o se lo sono stati, devono comunque dichiararlo ai fini di una maggiore attenzione da parte della società in caso si addivenga all'instaurazione del rapporto di consulenza) e di impegnarsi al rispetto del Decreto 231.

4. *Gestione dei rapporti con l'Amministrazione fiscale*

La Società si impegna a garantire la massima collaborazione e trasparenza nell'ambito dei rapporti con l'Amministrazione fiscale.

In particolare, la Società si impegna a garantire che:

a) siano individuati espressamente i soggetti autorizzati a trasmettere comunicazioni nei confronti dell'Amministrazione fiscale (Agenzia delle Entrate, Guardia di Finanza) e a riscontrarne le richieste;

b) qualsivoglia comunicazione di informazioni/dati/notizie nei confronti dell'Amministrazione fiscale sia effettuata in maniera corretta esaustiva e tempestiva (in caso di indicazione di una scadenza);

c) la Società garantisce che i rapporti con funzionari pubblici in caso di ispezione vengano gestiti nel rispetto dei principi stabiliti all'interno di apposita procedura interna.

5. *Contabilità e fatturazione (anche infragruppo)*

Nella predisposizione e successiva tenuta delle scritture contabili rilevanti ai fini tributari, la Società pone in essere una serie di misure formalizzate idonee ad assicurare che tutti i Dipendenti, nell'ambito delle rispettive competenze, rispettino il divieto di:

a) emettere o utilizzare fatture o altri documenti contabili relativi ad operazioni inesistenti;

b) emettere o utilizzare fatture o altri documenti contabili per corrispettivi superiori agli importi reali;

c) emettere o utilizzare fatture o altri documenti contabili che indichino soggetti diversi da quelli tra cui è effettivamente intercorso il rapporto sotteso;

d) effettuare pagamenti a fronte dell'emissione di fatture relative ad attività mai ricevute.

La Società si impegna, altresì, a garantire l'attuazione del principio di segregazione dei ruoli in relazione alle attività di gestione delle contabilità aziendale e nella successiva trasposizione dei dati nelle dichiarazioni tributarie, con riferimento, a titolo esemplificativo, a:

a) la tracciabilità dei flussi e l'identificazione dei soggetti che alimentano la trasmissione dei dati contabili e finanziari necessari alla predisposizione delle scritture contabili;

b) il rispetto del principio di segregazione dei compiti e il coinvolgimento di soggetti differenti nello svolgimento delle principali attività previste (fatturazione, pagamento, archiviazione della documentazione);

c) controllo sull'effettività delle prestazioni rispetto alle fatture emesse;

d) verifica della veridicità delle dichiarazioni rispetto alle scritture contabili.

Con particolare riferimento alla tematica della fatturazione infragruppo, la Società:

a) impronta le attività e i rapporti con le altre società del Gruppo alla massima integrità e trasparenza e assicura, nel compimento di operazioni di significativo rilievo, la trasparenza e il rispetto dei criteri di correttezza sostanziale e procedurale;

b) garantisce, anche nella gestione dei rapporti infragruppo, il rispetto del principio di segregazione dei ruoli;

c) garantisce che i servizi resi tra le società del Gruppo siano regolati contrattualmente per iscritto e resi a condizioni di mercato.

## CAPITOLO M.5

### I controlli dell'OdV e i flussi informativi

L'OdV effettua periodici controlli diretti a verificare il corretto adempimento da parte dei Destinatari, nei limiti dei rispettivi compiti e attribuzioni, delle regole e princìpi contenuti nella presente Parte Speciale e nelle procedure aziendali cui la stessa fa esplicito o implicito richiamo.

In particolare, è compito dell'Organismo di Vigilanza:

- monitorare l'efficacia dei princìpi contenuti nelle *policy* aziendali adottate ai fini della prevenzione dei Reati previsti nella presente Parte Speciale;
- proporre eventuali modifiche delle Attività Sensibili in ragione di eventuali mutamenti nell'operatività della Società;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi Dipendente o Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti, l'OdV può incontrare, invitare a relazionare alle riunioni dell'OdV e consultarsi con:

a) il Responsabile del Servizio Fiscale;

b) il Responsabile dell'Area *Finance & Strategy*.

È altresì attribuito all'OdV il potere di accedere o di chiedere di avere accesso a tutta la documentazione rilevante per lo svolgimento dei propri compiti.

La Società valuta l'istituzione di flussi informativi proceduralizzati nei confronti dell'OdV da parte delle funzioni indicate ai punti a) e b) (anche congiuntamente tra loro). Tali flussi informativi dovranno essere idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio delle anomalie rilevanti ai sensi della presente Parte Speciale e delle criticità rilevate in tale ambito.

Fermo restando quanto appena indicato, l'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verifichino violazioni ai principi procedurali specifici contenuti nella presente Parte Speciale ovvero alle procedure, *policy* e normative aziendali attinenti alle Attività Sensibili sopra individuate.

Per i flussi informativi si rimanda, in particolare, alla compilazione da parte delle funzioni competenti delle "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento) che costituiscono un allegato al Modello.

**PARTE SPECIALE – N –**

**Reati Ambientali**

**CAPITOLO N.1**

**Le fattispecie dei reati ambientali previste dall'art. 25-*undecies* del Decreto 231**

Il Decreto Legislativo 7 luglio 2011, n. 121 recante "*Attuazione della direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della Direttiva 2009/123/CE che modifica la Direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni*" ha previsto, attraverso l'inserimento dell'articolo 25-*undecies* nel Decreto 231, l'estensione della responsabilità amministrativa delle società e degli enti ad una serie di reati ambientali previsti dal codice penale, dal D.Lgs. 152/2006 ("**Cod. Amb.**") e da altre leggi speciali ("**Reati Ambientali**").

Si descrivono qui di seguito le fattispecie risultate *prima facie* a rischio di commissione nell'ambito delle attività svolte dalla Società.

***ATTIVITÀ DI GESTIONE DI RIFIUTI NON AUTORIZZATA (ART. 256, COMMA 1, LETT. A COD. AMB.)***

L'art. 256 è la disposizione normativa più importante nel sistema sanzionatorio in materia di gestione dei rifiuti in quanto detta una disciplina per una molteplicità di attività tutte connesse alla nozione di gestione dei rifiuti (*i.e.* la raccolta, il trasporto, il recupero, lo smaltimento, il commercio e l'intermediazione) siano essi pericolosi oppure non pericolosi.

È prevista una circostanza aggravante nel caso in cui il fatto sia commesso nell'ambito dell'attività di un'impresa o comunque di un'attività organizzata.

Si osserva che, quanto all'elemento soggettivo che caratterizza la condotta, la struttura contravvenzionale della fattispecie rende punibili i reati di cui al primo comma del presente articolo sia a titolo di dolo sia a titolo di colpa. È prevista una circostanza attenuante laddove il fatto sia commesso per colpa.

A tal fine è opportuno richiamare il rigore della giurisprudenza nell'interpretare e nell'applicare la norma, in quanto è stato ritenuto che tutti i soggetti che intervengono nel circuito della gestione dei rifiuti sono responsabili non solo della regolarità delle operazioni da essi stessi posti in essere, ma anche di quelle dei soggetti che precedono o seguono il loro intervento mediante l'accertamento della conformità dei rifiuti a quanto dichiarato dal produttore o dal trasportatore, sia pure tramite la verifica della regolarità degli appositi formulari, nonché la verifica del possesso delle prescritte autorizzazioni da parte del soggetto al quale i rifiuti sono conferiti per il successivo smaltimento

.

***VIOLAZIONE DEGLI OBBLIGHI DI COMUNICAZIONE, DI TENUTA DEI REGISTRI OBBLIGATORI E DEI FORMULARI (ART. 258, COMMA 4, COD. AMB.)***

L'art. 258 stabilisce che siano punite le imprese che: non effettuano o la effettuano in modo incompleto o inesatto la comunicazione annuale dei rifiuti (MUD), omettono la tenuta (o incompleta tenuta) dei registri di carico e scarico rifiuti, effettuano il trasporto di rifiuti senza il formulario di cui all'art. 193 ovvero indicano nel formulario stesso dati incompleti o inesatti.

In particolare, l'art. 25-*undecies* richiama il comma 4, secondo periodo della disposizione in oggetto. Pertanto, la responsabilità in ambito 231 può sorgere (ed è punita secondo la disciplina in materia di falsità ideologica commessa dal privato in atti pubblici) in caso di predisposizione di un certificato di analisi di rifiuti, recante false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti stessi e a chi fa uso di un certificato falso durante il trasporto.

***SPEDIZIONE ILLEGALE DI RIFIUTI (ART. 259, COMMA 1, COD. AMB.)***

L'art. 259 stabilisce che sia punito chiunque effettua una spedizione di rifiuti costituente spedizione illegale ai sensi degli articoli 2, punto 35 del regolamento (CE) n. 1013/2006 del Parlamento europeo e del Consiglio, del 14 giugno 2006 e dell'articolo 3, punto 26 del regolamento (UE) n. 2024/1157 del Parlamento europeo e del Consiglio dell'11 aprile 2024, è punito con la reclusione da uno a cinque anni. La pena è aumentata in caso di spedizione di rifiuti pericolosi.

***FATTISPECIE DI REATO DI CUI ALL'ART. 260-BIS COD. AMB. - SISTEMA INFORMATICO DI CONTROLLO DELLA TRACCIABILITÀ DEI RIFIUTI***

L'art. 260-*bis* punisce la falsità, l'omissione o la fraudolenta alterazione della documentazione che consente la tracciabilità dei rifiuti (anche in fase di trasporto degli stessi) applicando l'estensione della disciplina in materia di falsità ideologica commessa dal privato in atti pubblici.

***IMPEDIMENTO DEL CONTROLLO (ART. 452-SEPTIES C.P.)***

Il reato in oggetto punisce chiunque, negando l'accesso, predisponendo ostacoli o mutando artificiosamente lo stato dei luoghi, impedisca, intralci o eluda l'attività di vigilanza e controllo ambientali e di sicurezza e igiene del lavoro, ovvero ne comprometta gli esiti.

***ATTIVITÀ ORGANIZZATE PER IL TRAFFICO ILLECITO DI RIFIUTI (ART. 452-QUATERDECIES C.P.[10])***

Il reato in esame è integrato da chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti.

La pena prevista per le suddette condotte è aumentata quando: a) dal fatto deriva pericolo per la vita o per l'incolumità delle persone ovvero pericolo di compromissione o deterioramento: 1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo; 2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna; b) il fatto è commesso in siti contaminati o potenzialmente contaminati ai sensi dell'articolo 240 del Cod. Amb., o comunque sulle strade di accesso ai predetti siti e relative pertinenze.

Per integrare la presente fattispecie occorrono, quindi, una pluralità di operazioni tra l'allestimento di mezzi e attività continuative organizzate, la condotta di cedere, ricevere, trasportare, esportare, importare, o comunque di gestione di rifiuti, l'ingente quantità di rifiuti, il carattere abusivo dell'attività di gestione.

Questo delitto ha natura di reato (i) necessariamente abituale, in quanto la sua integrazione richiede la realizzazione di più comportamenti della stessa specie; (ii) di pura condotta, in quanto è su di questa che si incentra tutto il disvalore penale; (iii) si caratterizza per il dolo specifico, consistente nel fine di perseguire un ingiusto profitto.

[10] Il reato è stato introdotto dal D.Lgs. 1 marzo 2018, n. 21 e sostituisce l'art. 260 del D.Lgs. 3 aprile 2006, n. 152, abrogato dal citato decreto. Come specificato, infatti, dall'art. 8 del D.Lgs. 21/2018, "*dalla data di entrata in vigore del presente decreto, i richiami alle disposizioni abrogate dall'articolo 7, ovunque presenti, si intendono riferiti alle corrispondenti disposizioni del codice penale*".

## CAPITOLO N.2

### Attività Sensibili nell'ambito dei Reati Ambientali

In relazione ai Reati Ambientali la Società ha individuato al proprio interno le seguenti Attività a Rischio:

- selezione e gestione dei rapporti con fornitori di prestazioni di trasporto e smaltimento dei rifiuti;
- gestione delle ispezioni.

## CAPITOLO N.3

### Principi generali di comportamento nell'ambito dei Reati Ambientali

La Società si impegna ad orientare le proprie scelte in modo da garantire la compatibilità tra le attività del *business* e il rispetto dell'ambiente, svolgendo un ruolo attivo nella promozione di comportamenti responsabili e nella gestione degli impatti ambientali.

In generale, la Società al fine di garantire un adeguato presidio avverso la commissione di Reati Ambientali, si impegna a svolgere le attività aziendali nel rispetto delle leggi e dei regolamenti applicabili in tema di tutela ambientale. A tal proposito, viene individuato un "*Delegato per la tutela dell'ambiente*" ai sensi della normativa vigente in materia, al quale, tramite apposita procura scritta, vengono conferiti i necessari poteri di attivazione, verifica, coordinamento e relativi poteri di spesa in materia ambientale.

La Società ha adottato un sistema di gestione ambientale certificato allo standard ISO 14001.

La certificazione ISO 14001 e le relative norme tecniche adottate in materia ambientale sono espressione dell'attenzione posta dalla Società ai temi dell'ambiente e della sostenibilità in generale.

Pertanto, la Società:

- adempie puntualmente alle disposizioni normative applicabili in materia ambientale;
- assicura la definizione e l'aggiornamento, in base ai cambiamenti nella struttura organizzativa ed operativa della Società, nonché nella normativa di riferimento, di procedure specifiche per la prevenzione dei potenziali impatti ambientali connessi con l'attività;
- assicura la formalizzazione e attuazione di piani di manutenzione;
- assicura il controllo e la vigilanza sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate in materia ambientale e della conformità allo *standard* ISO 14001;
- sulla base degli esiti delle attività di controllo e vigilanza, pianifica gli interventi necessari per eliminare le criticità rilevate: ciò al fine di assicurare che il sistema di gestione degli impatti ambientali sia adeguatamente attuato e siano raggiunti gli obiettivi prefissati;
- assicura un adeguato livello di informazione dei Dipendenti e dei

Fornitori/appaltatori sul sistema procedurale ambientale definito dalla Società;

- assicura la selezione dei Fornitori sulla base di criteri ambientali definiti e il successivo affidamento dei contratti e monitoraggio delle prestazioni, in modo tale da garantire che i Fornitori a cui vengono affidate attività rilevanti da un punto di vista ambientale siano idonei da un punto di vista tecnico, professionale e autorizzativo e siano vincolati contrattualmente al rispetto delle norme ambientali vigenti e ai requisiti specifici stabiliti dall'organizzazione.

## CAPITOLO N.4

### Principi procedurali specifici nell'Ambito dei Reati Ambientali

Nell'ambito delle attività d'ufficio, la Società è dotata di un sistema di gestione dei rifiuti orientato alla diminuzione della produzione e al recupero degli stessi, nel rispetto delle prescrizioni normative vigenti. A tal fine, la Società:

- definisce i principali adempimenti da adottare in ambito aziendale in merito alla gestione delle diverse tipologie di rifiuti prodotti (soprattutto in riferimento alla gestione di rifiuti speciali, quali toner e materiale elettronico e informatico);
- provvede alla raccolta e alla classificazione dei rifiuti prodotti nell'ambito delle attività aziendali in conformità a quanto stabilito dalle disposizioni normative vigenti. Con particolare riferimento ai rifiuti elettronici e informatici, la Società:
    - istituisce e tiene costantemente aggiornato il registro dei materiali elettronici e informatici in disuso;
    - conserva e archivia i certificati relativi al corretto smaltimento dei rifiuti elettronici e informatici ricevuti dai fornitori dei servizi di gestione degli stessi.
- informa adeguatamente il personale dipendente in merito alla differenziazione e raccolta di rifiuti, soprattutto in relazione alla separazione e al deposito dei rifiuti speciali in appositi contenitori e/o in luoghi specificamente dedicati;
- affida le attività di trasporto, recupero e smaltimento dei rifiuti esclusivamente a imprese autorizzate e nel rispetto delle procedure aziendali relative alla selezione dei fornitori di servizi in *outsourcing*;
- nei contratti con i fornitori dei servizi di trasporto, recupero e smaltimento di rifiuti speciali prevede l'inserimento della Clausola 231 che consente, in particolare, alla Società stessa di risolvere, con effetto immediato, il contratto medesimo nel caso in cui dovessero essere riscontrate irregolarità, da parte dei fornitori e dei propri subfornitori, nella gestione dei rifiuti prodotti dalla Società medesima;
- garantisce il pieno e libero svolgimento delle attività di vigilanza, controllo e ispezione in materia ambientale, assicurando l'accesso ai luoghi, la disponibilità delle informazioni e la collaborazione necessaria agli organi competenti, e vietando qualsiasi

comportamento volto a negare l'accesso, predisporre ostacoli, alterare artificiosamente lo stato dei luoghi o, comunque, impedire, intralciare, eludere o compromettere l'esito delle predette attività di controllo;

- garantisce che alle ispezioni o verifiche condotte da pubbliche autorità in materia ambientale siano presenti almeno due soggetti a ciò espressamente delegati;
- provvede alla conservazione di tutti i documenti dell'ispezione o verifica in ambito ambientale, nonché del verbale predisposto dall'Autorità all'esito dell'attività ispettiva

## CAPITOLO N.5

### I controlli dell'OdV e i flussi informativi

In relazione ai reati ambientali, l'Organismo di Vigilanza riceve periodicamente informazioni in merito ad eventuali aspetti ambientali rilevanti e in relazione ad eventuali anomalie e/o criticità relative alle attività di gestione dei rifiuti speciali (toner, rifiuti elettronici e informatici) dalla funzione competente. Sulla base dei flussi informativi o di eventuali segnalazioni, l'OdV valuta l'opportunità di svolgere specifiche verifiche, con il supporto di soggetti interni o esterni alla Società.

Per i flussi informativi si rimanda, in particolare, alla compilazione da parte delle funzioni competenti delle "schede di flusso" (appositi moduli predisposti al fine di dare evidenza, tramite domande aperte/chiuse, riguardo a specifici aspetti della rispettiva attività ovvero a specifici eventi di rilievo – in ottica 231 – occorsi nel periodo di riferimento) che costituiscono un allegato al Modello.