

**MODELLO DI ORGANIZZAZIONE,  
GESTIONE E CONTROLLO AI SENSI DEL  
D.LGS. 8 GIUGNO 2001 N. 231**

**DELOITTE RISK ADVISORY  
S.R.L.**

Milano, 6 novembre 2020

## Indice

– <b>PARTE GENERALE I</b> – .....	4
<b>IL QUADRO NORMATIVO</b> .....	4
<b>A. Premessa</b> .....	4
<b>B. Il Decreto Legislativo 8 giugno 2001, n. 231</b> .....	4
B.1 Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società e associazioni .....	4
B.2 I reati previsti dal Decreto .....	5
B.3 Le sanzioni .....	13
B.4 L’adozione del Modello di organizzazione, gestione e controllo quale esimente della responsabilità amministrativa dell’ente .....	14
<b>C. Le “Linee Guida” di Confindustria</b> .....	15
– <b>PARTE GENERALE II</b> – .....	17
<b>IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO</b> .....	17
<b>D. Caratteristiche generali del Modello di organizzazione, gestione e controllo di Deloitte Risk Advisory S.r.l.</b> .....	17
D.1 I Destinatari .....	18
D.2 Obiettivi e finalità perseguiti con l’adozione del Modello .....	18
D.3 Elementi fondamentali del Modello .....	19
D.4 Modello e Codice Etico .....	19
D.5 Responsabilità dell’adozione e della concreta attuazione del Modello .....	20
D.6 Percorso metodologico di definizione del Modello di Deloitte Risk Advisory S.r.l. ....	20
<b>E. Aree e processi aziendali a potenziale “rischio – reato”</b> .....	21
E.1 La struttura del sistema organizzativo e di controllo .....	24
E.2 Regole Comportamentali .....	27
<b>F. Organismo di Vigilanza</b> .....	42
F.1 Durata in carica, decadenza e revoca .....	43
F.2 Funzioni e poteri dell’Organismo di Vigilanza .....	44
F.3 Reporting dell’Organismo di Vigilanza .....	46
F.4 Disciplina del <i>whistleblowing</i> : gestione delle segnalazioni .....	47
<b>G. Il Sistema Sanzionatorio</b> .....	49
G.1 Sanzioni per i lavoratori dipendenti non dirigenti .....	50
G.2 Misure nei confronti dei dirigenti .....	52

G.3	Misure nei confronti di collaboratori sottoposti a direzione e vigilanza.....	52
G.4	Misure nei confronti degli Amministratori .....	53
G.5	Misure nei confronti dei soggetti apicali.....	53
G.6	Misure nei confronti dei terzi.....	53
<b>H.</b>	<b><i>Informazione e formazione</i></b> .....	<b>53</b>
H.1.	Formazione del personale .....	54
H.2	Informativa ad altri Destinatari .....	54
<b>I.</b>	<b><i>Adozione e aggiornamento del Modello</i></b> .....	<b>54</b>

– PARTE GENERALE I –  
**IL QUADRO NORMATIVO**

## **A. Premessa**

Il presente documento è stato redatto ai sensi e per gli effetti di cui al 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, a norma dell’art. 11 della legge 29 settembre 2000, n. 300”*, allo scopo di descrivere in forma organizzata le regole, le procedure e le norme comportamentali che disciplinano l’organizzazione e la gestione di Deloitte Risk Advisory S.r.l. (di seguito alternativamente **“DRA”** o la **“Società”**).

Il Modello di organizzazione, gestione e controllo (di seguito anche solo **“Modello”**) di DRA è stato predisposto tenendo anche in considerazione i codici di comportamento redatti dalle Associazioni rappresentative degli enti e comunicati al Ministero della Giustizia.

Il Modello si compone della presente parte generale (di seguito **“Parte Generale”**) e della parte speciale ove sono stati formulati i principi di controllo, declinati nei Protocolli 231, adottati dalla Società per prevenire il rischio di commissione dei reati nella gestione delle attività sensibili e dei processi sensibili/strumentali della Società (di seguito **“Parte Speciale”**).

## **B. Il Decreto Legislativo 8 giugno 2001, n. 231**

### **B.1 Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società e associazioni**

In attuazione della delega di cui all’art. 11 della Legge 29 settembre 2000 n. 300, in data 8 giugno 2001 è stato emanato il Decreto Legislativo n. 231 (di seguito alternativamente **“D.Lgs. 231/2001”** o solo **“Decreto”**), entrato in vigore il 4 luglio 2001, con il quale il Legislatore ha adeguato la normativa interna alle convenzioni internazionali in materia di responsabilità delle persone giuridiche. In particolare, si tratta della Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, della Convenzione firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione nella quale siano coinvolti funzionari della Comunità Europea o degli Stati membri e della Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Il Decreto, recante *“Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”*, ha introdotto nell’ordinamento

giuridico italiano un regime di responsabilità amministrativa (assimilabile sostanzialmente alla responsabilità penale) a carico degli enti (da intendersi come società, associazioni, consorzi, ecc., di seguito anche gli “Enti”) per reati tassativamente elencati e commessi nel loro interesse o vantaggio: (i) da soggetti c.d. “apicali”, cioè da persone fisiche che rivestono funzioni di rappresentanza, di amministrazione o di direzione degli Enti o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitano, anche di fatto, la gestione e il controllo degli Enti medesimi, ovvero (ii) da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati. La responsabilità dell’ente si aggiunge a quella della persona fisica che ha commesso materialmente il reato.

La previsione della responsabilità amministrativa di cui al Decreto coinvolge, nella repressione degli illeciti penali ivi espressamente previsti, gli Enti che abbiano tratto interesse e/o vantaggio dalla commissione del reato. Tra le sanzioni comminabili, quelle certamente più gravose per l’ente sono rappresentate dalle misure interdittive, quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la Pubblica Amministrazione, l’interdizione dall’esercizio dell’attività, l’esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi. La suddetta responsabilità si configura anche in relazione a reati commessi all’estero, purché nei confronti dell’ente non proceda lo Stato del luogo in cui gli stessi siano stati commessi.

Quanto ai reati cui si applica la disciplina in esame, si tratta attualmente delle seguenti tipologie: (a) reati contro la Pubblica Amministrazione, (b) delitti informatici e trattamento illecito di dati (c) delitti di criminalità organizzata, (d) delitti di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, (e) delitti contro l’industria e il commercio, (f) reati societari, (g) delitti con finalità di terrorismo o di eversione dell’ordine democratico, (h) pratiche di mutilazione degli organi genitali femminili, (i) delitti contro la personalità individuale, (j) abusi di mercato, (k) reati transnazionali, (l) reati colposi commessi in violazione della normativa antinfortunistica e sulla tutela dell’igiene e della salute sul lavoro, (m) reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, (n) delitti in materia di violazione del diritto d’autore, (o) induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria, (p) reati ambientali, (q) reati inerenti stranieri irregolari, (r) razzismo e xenofobia, (s) frodi in competizioni sportive, esercizio abusivo di gioco o di scommesse e giochi d’azzardo esercitati a mezzo di apparecchi vietati, (t) reati tributari.

## B.2 I reati previsti dal Decreto

Si elencano di seguito i reati che, allo stato, sono inclusi nel perimetro di applicazione del Decreto, precisando tuttavia che si tratta di un elenco destinato ad ampliarsi nel prossimo futuro:

- *Reati contro la Pubblica Amministrazione, come integrati dalla Legge 190/2012 e dalla Legge 3/2019 (artt. 24 e 25):*

- Malversazione a danno dello Stato o di altro ente pubblico (art. 316 bis c.p.);
- Indebita percezione di erogazioni a danno dello Stato o di altro ente pubblico (art. 316 ter c.p.);
- Concussione (art. 317 c.p.);
- Corruzione (artt. 318, 319, 319 bis, 320, 321 c.p. 322 bis c.p.);

- Corruzione in atti giudiziari (art. 319 ter c.p.);
- Induzione indebita a dare o promettere utilità (art. 319 quater c.p.);
- Istigazione alla corruzione (art. 322 c.p.);
- Truffa in danno dello Stato o di un ente pubblico o delle Comunità europee (art. 640, comma 2, n. 1, c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.);
- Frode informatica a danno dello Stato o di altro ente pubblico (art. 640 ter c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

- *Delitti informatici e trattamento illecito di dati introdotti dalla Legge 48/2008 e modificati dal D.Lgs. n. 7 e 8/2016 e dal D.L. n. 105/2019 (art. 24 bis):*

- Documenti informatici (art. 491 bis c.p.);
- Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente Pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- Danneggiamento di sistemi informatici e telematici (art. 635 quater c.p.);
- Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635 quinquies c.p.);
- Frode informatica del certificatore di firma elettronica (art. 640 quinquies c.p.);
- Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11-bis, della Legge 18 novembre 2019, n. 133).

- *Delitti di criminalità organizzata introdotti dalla Legge 94/2009 e modificati dalla Legge 69/2015, nonché dalla Legge n. 43/2019 (art. 24 ter)*

- Associazione per delinquere, anche diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602, nonché all'articolo 12, comma 3-bis, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286 (art. 416 c.p.);
- Associazioni di tipo mafioso anche straniere (art. 416 bis c.p.);

- Scambio elettorale politico-mafioso (art. 416 ter c.p.);
- Sequestro di persona a scopo di estorsione (art. 630 c.p.);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9 ottobre 1990 n. 309);
- 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 o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, escluse quelle previste dall'articolo 2 comma 3, della legge 18 aprile 1975, n. 110 (art. 407 comma 2, lett. a), numero 5) c.p.p.).

- *Delitti di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, introdotti dalla Legge 409/2001 e modificati con Legge 99/2009 e con D.Lgs. 125/2016 (art. 25 bis):*

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- Alterazione di monete (art. 454 c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo, o di carta filigranata (art. 461 c.p.);
- Uso di valori bollati contraffatti o alterati (art. 464, commi 1 e 2, c.p.);
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (474 c.p.).

- *Delitti contro l'industria e il commercio, introdotti dalla Legge 99/2009 (art. 25-bis.1):*

- 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.).

- *Reati societari, introdotti dal D. Lgs. 61/2002 e parzialmente modificati dalla Legge 262/2005 nonché integrati dalla Legge 190/2012, dalla Legge 69/2015 e dal D.Lgs. 38/2017 (art. 25-ter):*

- False comunicazioni sociali (art. 2621 c.c.);
- Fatti di lieve entità (art. 2621 bis c.c.);
- False comunicazioni sociali delle società quotate (art. 2622 c.c.);
- Impedito controllo (art. 2625, comma 2, c.c.);
- Indebita restituzione dei conferimenti (art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Omessa comunicazione del conflitto di interessi (art. 2629 bis c.c.);
- Formazione fittizia del capitale (art. 2632 c.c.);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis, comma 1, c.c.);
- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Aggiotaggio (art. 2637 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.).

- *Delitti con finalità di terrorismo o di eversione dell'ordine democratico, introdotti dalla Legge 7/2003 (art. 25 quater):*

- Associazioni sovversive (art. 270 c.p.);
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270 bis c.p.);
- Assistenza agli associati (art. 270 ter c.p.);
- Arruolamento con finalità di terrorismo anche internazionale (art. 270 quater c.p.);
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270 quinquies c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270 quinquies 1, c.p.);
- Sottrazione di beni o denaro sottoposto a sequestro (art. 270 quinquies 2, c.p.);
- Condotte con finalità di terrorismo (art. 270 sexies c.p.);



- Attentato per finalità terroristiche o di eversione (art. 280 c.p.);
- Atto di terrorismo con ordigni micidiali o esplosivi (art. 280 bis c.p.);
- Atto di terrorismo nucleare (art. 280 ter c.p.);
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289 bis c.p.);
- Sequestro a scopo di coazione (art. 289 ter c.p.);
- Istigazione a commettere alcuno dei delitti previsti dai Capi primo e secondo (art. 302 c.p.);
- Cospirazione politica mediante accordo (art. 304 c.p.);
- Cospirazione politica mediante associazione (art. 305 c.p.);
- Banda armata: formazione e partecipazione (art. 306 c.p.);
- Assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.);
- Impossessamento, dirottamento o distruzione di un aereo (L. n. 342/1976, art. 1);
- Danneggiamento delle installazioni a terra (L. n. 342/1976, art. 2);
- Sanzioni (L. n. 422/1989, art. 3);
- Pentimento operoso (D.Lgs. n. 625/1979, art. 5);
- Convenzione internazionale per la repressione del finanziamento del terrorismo New York 9 dicembre 1999 (art. 2).

- *Pratiche di mutilazione degli organi genitali femminili, introdotte dalla Legge 7/2006 (art. 25 quater. 1):*

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

- *Delitti contro la personalità individuale, introdotti dalla Legge 228/2003 e parzialmente modificati con la Legge 38/2006, il D.Lgs 39/2014 e con la Legge 199/2016 (art. 25-quinquies):*

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
- Prostituzione minorile (art. 600 bis, commi 1 e 2, c.p.);
- Pornografia minorile (art. 600 ter c.p.);
- Detenzione di materiale pornografico (art. 600 quater c.p.);
- Pornografia virtuale (art. 600 quater.1 c.p.);
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 quinquies c.p.);
- Tratta di persone (art. 601 c.p.);
- Acquisto e alienazione di schiavi (art. 602 c.p.);
- Intermediazione illecita e sfruttamento del lavoro (art. 603 bis c.p.);
- Adescamento di minorenni (609 undecies c.p.).

- *Abusi di mercato, introdotti dalla Legge 62/2005 e modificati dal D.Lgs. 107/2018 (art. 25-sexies):*

- Abuso di informazioni privilegiate (art. 184 D. Lgs. 58/1998);
- Manipolazione del mercato (art. 185 D. Lgs. 58/1998).

- *Reati transnazionali, introdotti dalla Legge 16 marzo 2006, n. 146, art. 10:*

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

- *Reati colposi commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro, introdotti dalla Legge 123/2007 (art. 25-septies):*

- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose, gravi o gravissime (art. 590 c.p.).

- *Reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita introdotti dal D.Lgs. 231/2007, nonché integrati dalla Legge 186/2014 (art. 25-octies):*

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

- *Delitti in materia di violazione del diritto d'autore, introdotti dalla Legge 99/2009 (art. 25-novies):*

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni

di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa (art. 171 comma 1, lett. a-bis), Legge 633/1941);

- Reati di cui al punto precedente commessi in riferimento ad un'opera altrui non destinata alla pubblicazione qualora ne risulti offesa all'onore o alla reputazione dell'autore (art. 171, comma 3, Legge 633/1941);
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171 bis, comma 1, Legge 633/1941);
- Riproduzione, trasferimenti su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita e concessione in locazione della banca di dati (art. 171-bis, comma 2, Legge 633/1941);
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, di dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; abusiva riproduzione, trasmissione o diffusione in pubblico, con qualsiasi procedimento, di opere, o parti di opere, letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171 ter, Legge 633/1941);
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171 septies, Legge 633/1941);
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzazione per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171 octies, Legge 633/1941).

- *Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, introdotto dalla Legge 116/2009 (art. 25-decies):*

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

- *Reati ambientali, introdotti dal D.Lgs. 121/2011 e integrati dalla Legge 68/2015 e dal D.Lgs. 21/2018 (art. 25 undecies):*

- Inquinamento ambientale (art. 452 bis c.p.);
- Disastro ambientale (art. 452 quater c.p.);

- Delitti colposi contro l'ambiente (art. 452 quinquies c.p.);
- Traffico e abbandono di materiale ad alta radioattività (art. 452 sexies c.p.);
- Circostanze aggravanti (art. 452 octies c.p.);
- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727 bis c.p.);
- Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733 bis c.p.);
- Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi o aeromobili (art. 137 D.Lgs. 152/2006);
- Attività di gestione di rifiuti non autorizzata (art. 256 D.Lgs. 152/2006);
- Omessa bonifica dei siti (art. 257 D.Lgs. 152/2006);
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 comma 4 secondo periodo D.Lgs. 152/2006);
- Traffico illecito di rifiuti (art. 259 comma 1 D.Lgs. 152/2006);
- Attività organizzate per il traffico illecito di rifiuti (art. 452 quaterdecies c.p.);
- Superamento di valori limite di emissione che determinano il superamento dei valori limite di qualità dell'aria (art. 279 comma 5 D.Lgs. 152/2006);
- Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. n.150/1992, art. 1, art. 2, art. 3-bis e art. 6);
- Cessazione e riduzione dell'impiego di sostanze lesive (art. 3 Legge n. 549/1993);
- Inquinamento doloso di nave battente qualsiasi bandiera (art. 8 D.Lgs. n. 202/2007);
- Inquinamento colposo di nave battente qualsiasi bandiera (art. 9 D.Lgs. n. 202/2007).

- *Reati inerenti stranieri irregolari, introdotto dal D.Lgs. 109/2012 e modificato dalla Legge 161/2017 (art. 25-duodecies):*

- Trasporto di stranieri irregolari nel territorio dello Stato (art. 12 comma 3, 3-bis e 3-ter D.Lgs. 286/1998);
- Favoreggiamento della permanenza di stranieri irregolari nel territorio dello Stato (art. 12 comma 5 D.Lgs. 286/1998);
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22 comma 12-bis D.Lgs. n. 286/1998).

- *Reati di razzismo e xenofobia, introdotto dalla Legge 167/2017 e modificati dal D.Lgs. 21/2018 (art. 25-terdecies):*

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

- *Reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati, introdotti dalla legge 39/2019 (art. 25-quaterdecies):*

- Frodi in competizioni sportive (art. 1 L. n. 401/1989);
- Esercizio abusivo di attività di giuoco o di scommesse (art. 4 L. n. 401/1989).

- *Reati tributari, introdotti dalla Legge 157/2019 (art. 25-quinquiesdecies):*

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. 74/2000);
- Dichiarazione fraudolenta mediante altri artifici; (art. 3 D.Lgs. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. 74/2000);
- Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. 74/2000);
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. 74/2000).

## **B.3 Le sanzioni**

Le sanzioni previste per gli illeciti amministrativi dipendenti da reato sono:

- sanzioni pecuniarie;
- sanzioni interdittive;
- confisca;
- pubblicazione della sentenza.

Le sanzioni interdittive, che possono essere comminate solo laddove espressamente previste e anche in via cautelare, sono le seguenti:

- interdizione dall'esercizio dell'attività;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- divieto di contrattare con la Pubblica Amministrazione;
- esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o revoca di quelli eventualmente già concessi;
- divieto di pubblicizzare beni o servizi.

Il Decreto prevede, inoltre, che qualora vi siano i presupposti per l'applicazione di una sanzione interdittiva che determina l'interruzione dell'attività della società, il giudice, in luogo dell'applicazione della sanzione, possa disporre la prosecuzione dell'attività da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando ricorre almeno una delle seguenti condizioni:

- la società svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;
- l'interruzione dell'attività può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

## **B.4. L'adozione del Modello di organizzazione, gestione e controllo quale esimente della responsabilità amministrativa dell'ente**

Il Legislatore ha individuato la possibilità per l'ente di andare esente da responsabilità amministrativa laddove sia in grado di dimostrare l'esistenza e l'efficacia di mezzi di prevenzione e controllo atti a evitare comportamenti illeciti. L'art. 6 del D.Lgs. 231/2001 stabilisce, infatti, che l'ente non risponde a titolo di responsabilità amministrativa qualora dimostri di aver predisposto ed efficacemente attuato un modello di organizzazione, di gestione e di controllo mirato alla prevenzione dei reati previsti dal D.Lgs. 231/2001, il quale preveda protocolli di comportamento diretti a programmare la formazione e l'attuazione delle decisioni dell'ente nell'ambito delle aree/attività aziendali maggiormente a rischio di commissione dei reati presupposto.

Il Legislatore prevede, inoltre, l'istituzione di un organo di controllo interno all'ente con il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del predetto modello di organizzazione, di gestione e di controllo, nonché di curarne l'aggiornamento.

Il modello di organizzazione, gestione e controllo previsto dall'art. 6 commi 2 e 3 del D. Lgs. 231/2001 deve rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito possano essere commessi i reati previsti dal Decreto;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente al fine di prevenire la commissione dei reati presupposto;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello di organizzazione, di gestione e di controllo;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello di organizzazione, di gestione e di controllo.

Ove il reato sia commesso da soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da soggetti che esercitano, anche di fatto, la gestione e il controllo dello stesso, l'ente non risponde se prova che: *(i)* l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione, di gestione e di controllo idoneo a prevenire reati della specie di quello verificatosi; *(ii)* il compito di vigilare sul funzionamento e l'osservanza del modello di organizzazione, di gestione e di controllo e di verificarne l'aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo; *(iii)* i soggetti hanno commesso il reato eludendo fraudolentemente il modello di organizzazione, di gestione e di controllo; *(iv)* non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di controllo.

Nel caso in cui, invece, il reato venga commesso da soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Detta inosservanza è, in ogni caso, esclusa qualora l'ente, prima della commissione del reato, abbia adottato ed efficacemente attuato un modello di organizzazione, di gestione e di controllo idoneo a prevenire reati della specie di quello verificatosi.

## C. Le “Linee Guida” di Confindustria

L'art. 6 del D.Lgs. 231/2001 dispone espressamente che i modelli di organizzazione, di gestione e di controllo possano essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti.

Ai fini della predisposizione del modello di organizzazione, di gestione e di controllo, vengono quindi prese in considerazione le “Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001” (di seguito solo “**Linee Guida**”) redatte da Confindustria e approvate dal Ministero della Giustizia con il D.M. 4 dicembre 2003. Le Linee Guida sono state da ultimo aggiornate da Confindustria alla data del 31 marzo 2014 e approvate il 21 luglio 2014 dal Ministero della Giustizia.

Nella definizione del modello di organizzazione, gestione e controllo, le Linee Guida prevedono le seguenti fasi progettuali:

- l'identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare in quali aree di attività e secondo quali modalità si possano verificare nel contesto aziendale i reati previsti dal D.Lgs. 231/2001;
- la predisposizione di un sistema di controllo idoneo a prevenire i rischi di reato identificati nella fase precedente, da effettuarsi attraverso la valutazione del sistema di controllo esistente e il relativo grado di adeguamento alle esigenze di prevenzione espresse dal D.Lgs. 231/2001.

Le componenti più rilevanti del sistema di controllo delineato nelle Linee Guida per garantire l'efficacia del modello di organizzazione, gestione e controllo sono di seguito riassunte:

- la previsione di principi etici e di regole comportamentali in un Codice Etico;
- un modello organizzativo sufficientemente formalizzato e chiaro, in particolare con riguardo all'attribuzione di responsabilità, alle linee di dipendenza gerarchica e alla descrizione dei compiti;
- procedure manuali e/o informatiche che regolino lo svolgimento delle attività, prevedendo gli opportuni e adeguati controlli;
- poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali attribuite dall'ente, prevedendo, laddove opportuno, limiti di spesa;

- sistemi di controllo di gestione, capaci di segnalare tempestivamente possibili criticità;
- informazione e formazione del personale.

Le Linee Guida precisano, inoltre, che le componenti del sistema di controllo sopra descritte devono conformarsi ad una serie di principi di controllo, tra cui:

- verificabilità, tracciabilità, coerenza e congruità di ogni operazione, transazione e azione;
- applicazione del principio di separazione delle funzioni e segregazione dei compiti (nessuno può gestire in autonomia un intero processo);
- istituzione, esecuzione e documentazione dell'attività di controllo sui processi e sulle attività a rischio di reato.



– PARTE GENERALE II –

**IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO**

**D. Caratteristiche generali del Modello di organizzazione, gestione e controllo di Deloitte Risk Advisory S.r.l.**

Deloitte Risk Advisory S.r.l. ha per oggetto la prestazione di servizi di consulenza e di gestione di servizi di supporto alle imprese per la mitigazione dei rischi strategici e reputazionali, regolamentari, finanziari, operativi, fra i quali rientrano quelli a supporto delle funzioni e delle attività di Internal Audit e di Cyber Security. A titolo esemplificativo e non esaustivo, la Società svolge l'attività di revisione contabile, di revisione informatica, la gestione di attività di controllo interno, consulenza in materia di sistemi per la sicurezza delle informazioni e delle infrastrutture elettroniche, consulenza in materia di organizzazione e sistemi per la protezione della riservatezza dei dati, consulenza in materia di regulatory compliance, consulenza in materia di corporate compliance e di internal audit, consulenza in materia di bilanci sociali e di sostenibilità, rischi ambientali e sicurezza sul lavoro, assistenza nei processi di quotazione in relazione agli international financial reporting standards.

Deloitte Risk Advisory S.r.l., facente parte del DTTL Network<sup>1</sup>, consapevole dell'importanza di adottare ed efficacemente attuare un modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001 idoneo a prevenire la commissione di comportamenti illeciti nel contesto aziendale, ha approvato, con delibera del Consiglio di Amministrazione in data **29 aprile 2010**, una prima versione del proprio Modello di organizzazione gestione e controllo, successivamente rivisitata in data **13 novembre 2014** a seguito dell'introduzione nel Decreto di ulteriori reati presupposto della responsabilità amministrativa degli enti quali ad esempio i reati ambientali e del reato di corruzione tra privati, e in data **8 luglio 2016**, a seguito dell'introduzione nel Decreto della fattispecie di autoriciclaggio ex Legge 186/2014 e delle modifiche intervenute con la Legge 69/2015 in tema di reati societari.

A seguito di successivi aggiornamenti normativi che hanno portato all'inserimento nel Decreto di ulteriori nuove fattispecie di reato, la Società ha conseguentemente adottato, con delibera del Consiglio di Amministrazione in data [...] **settembre 2020**, la versione aggiornata del Modello di organizzazione, gestione e controllo (il "**Modello**").

<sup>1</sup> "DTTL": indica Deloitte Touche Tohmatsu Limited, una società a responsabilità limitata di diritto inglese.

"DTTL Network": indica DTTL, il suo network di member firm e di entità alle stesse affiliate.

## **D.1 I Destinatari**

I principi e le disposizioni del Modello trovano applicazione, come ulteriormente dettagliato nella Parte Speciale del presente Modello, nei confronti degli Amministratori, dei Soci e di tutti coloro che rivestono, all'interno della Società, funzioni di rappresentanza, amministrazione e direzione ovvero gestione e controllo (anche di fatto), nonché dei dipendenti (per tali intendendosi tutti coloro che sono legati alla Società da un rapporto di lavoro subordinato, ivi compresi i dirigenti) e dei collaboratori sottoposti alla direzione o vigilanza dei soggetti apicali della Società e dei dipendenti/collaboratori di Deloitte Italy S.p.A. o di altre società italiane del DCM Network<sup>2</sup> limitatamente alle attività svolte in favore della Fondazione in regime di outsourcing (tutti insieme i “Destinatari”).

Resta inteso che il riferimento ai “Destinatari” deve considerarsi circoscritto ai Destinatari coinvolti nelle specifiche attività e processi di volta in volta considerati.

## **D.2 Obiettivi e finalità perseguiti con l’adozione del Modello**

La Società è sensibile all’esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione e immagine, delle aspettative dei Soci e del lavoro dei propri collaboratori e dipendenti ed è, altresì, consapevole dell’importanza di un sistema di controllo interno quale strumento idoneo a prevenire la commissione di comportamenti illeciti.

DRA ritiene, dunque, che l’adozione del Modello, unitamente al Codice Etico (documento pubblicato sulla Intranet della Società) - al di là delle prescrizioni del Decreto, che indicano il Modello stesso come elemento facoltativo e non obbligatorio - possa costituire un valido strumento di ulteriore sensibilizzazione nei confronti di tutti i dipendenti della Società e di tutti gli altri Destinatari, affinché seguano, nell’espletamento delle proprie attività, comportamenti corretti e trasparenti, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.

In particolare, attraverso un continuo adeguamento della propria struttura organizzativa DRA si propone di perseguire le seguenti principali finalità:

- determinare, in tutti i Destinatari che operano nelle aree di attività a rischio, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni del Modello, nella commissione di illeciti passibili di sanzioni penali comminabili nei loro stessi confronti e di sanzioni amministrative irrogabili alla Società;
- ribadire che tali forme di comportamento illecito sono fortemente condannate da DRA, in quanto tali condotte (anche nel caso in cui la Società fosse apparentemente in condizione di trarre vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etici ai quali la Società intende attenersi nell’esercizio della propria attività aziendale;
- consentire alla Società, grazie ad un’azione di stretto controllo e monitoraggio sulle aree

---

<sup>2</sup> “DCM Network” indica Deloitte Central Mediterranean S.r.l. e le entità ad essa affiliate nel territorio della Repubblica Italiana (nonché della Città del Vaticano e della Repubblica di San Marino), della Repubblica Greca e della Repubblica di Malta;

di attività a rischio e all'implementazione di idonei strumenti e procedure, di intervenire tempestivamente per prevenire o contrastare la commissione dei reati contemplati nel Decreto.

### D.3 Elementi fondamentali del Modello

Con riferimento alle esigenze individuate nel Decreto, gli elementi fondamentali del Modello di Deloitte Risk Advisory S.r.l. possono essere così brevemente riassunti:

- i principi etici e le regole di comportamento volte alla prevenzione di condotte che possano integrare le fattispecie di reato previste dal Decreto, contenute sia nel Codice Etico adottato dalla Società, sia, più in dettaglio, nel presente Modello;
- la mappatura delle attività sensibili e dei processi aziendali “strumentali/funzionali” rispetto alla commissione dei reati di cui al Decreto, da sottoporre, pertanto, ad analisi e monitoraggio periodico (c.d. Mappatura delle aree di attività a rischio reato);
- i principi di controllo generali e specifici relativi ai c.d. processi “strumentali/funzionali” alla commissione dei reati, che forniscono indicazioni sul sistema di controlli preventivi da adottare in relazione ai reati specifici da prevenire (di seguito “**Protocolli 231**”);
- l’Organismo di Vigilanza (di seguito anche “**OdV**”) e l’attribuzione allo stesso di specifici compiti di vigilanza sull’efficace e corretto funzionamento del Modello;
- i flussi informativi nei confronti dell’OdV;
- un sistema sanzionatorio idoneo a garantire l’efficace attuazione del Modello, contenente le disposizioni disciplinari applicabili ai Destinatari in caso di mancato rispetto delle misure indicate nel Modello medesimo;
- le attività di informazione, sensibilizzazione, divulgazione e formazione ai Destinatari previste nel presente Modello;
- le regole e le responsabilità per l’adozione, l’implementazione e le successive modifiche e/o integrazioni del Modello (c.d. aggiornamento del Modello).

### D.4 Modello e Codice Etico

DRA intende improntare la conduzione del proprio business al rispetto delle leggi e dei regolamenti vigenti.

DRA ispira la propria attività ai valori comuni del DTTL Network, nonché ai relativi principi etici ai quali la Società conforma le proprie attività, comportamenti e rapporti, sia all’interno sia all’esterno dell’organizzazione aziendale.

La Società ha, in particolare, adottato un codice etico (di seguito, alternativamente il “**Codice**” o il “**Codice Etico**”), che sancisce una serie di regole di deontologia aziendale che la Società riconosce come proprie e delle quali richiede l’osservanza da parte sia dei propri Soci, organi sociali e dipendenti sia dei terzi che, a qualunque titolo, intrattengano rapporti di natura contrattuale con DRA.

Il Codice Etico afferma, pertanto, principi di corretta conduzione degli affari sociali idonei anche a prevenire i comportamenti illeciti di cui al Decreto, acquisendo rilevanza preventiva ai fini del

Modello e costituendone, dunque, un elemento integrativo fondamentale.

Il Modello, le cui previsioni sono in ogni caso coerenti e conformi ai principi del Codice Etico, risponde più specificamente alle esigenze espresse dal Decreto ed è, pertanto, finalizzato a prevenire la commissione delle fattispecie di reato ricomprese nell'ambito del D.Lgs. 231/2001.

## **D.5 Responsabilità dell'adozione e della concreta attuazione del Modello**

L'art. 6, comma 1, lettera a) del Decreto richiede che il Modello sia un "atto di emanazione dell'organo dirigente". L'adozione dello stesso è dunque di competenza del Consiglio di Amministrazione della Società, come meglio specificato nel successivo paragrafo I.

L'efficace e concreta attuazione del Modello è garantita dalle funzioni/direzioni aziendali, vale a dire dai responsabili delle varie strutture organizzative della Società, in relazione alle attività a rischio potenziale dalle stesse svolte.

L'Organismo di Vigilanza verifica, nell'esercizio dei poteri di iniziativa e di controllo allo stesso conferiti, le attività svolte dalle singole unità organizzative nelle aree a rischio.

In particolare, è responsabilità delle funzioni/direzioni aziendali trasferire ai propri collaboratori la consapevolezza delle situazioni a "rischio-reato", nonché impartire direttive circa le modalità operative di svolgimento dei compiti assegnati, in coerenza con i principi e le prescrizioni contenuti nel presente Modello e tenendo conto delle peculiarità del proprio ambito di attività.

Le verifiche sul Modello competono all'Organismo di Vigilanza con il supporto della funzione internal audit, i.e. la funzione di internal audit composta da personale di altre società facenti parte del DCM Network mediante contratti di servizio nei quali vengono disciplinate le condizioni e i livelli di servizio che concorrono a costituire adeguato presidio di controllo con riferimento alle attività gestite per conto della Società (di seguito la "**Funzione Internal Audit**"), che potrà svolgere per conto dello stesso OdV, attività di monitoraggio e verifica in attuazione dei periodici piani di attività elaborati dall'Organismo di Vigilanza.

## **D.6 Percorso metodologico di definizione del Modello di Deloitte Risk Advisory S.r.l.**

Il D.Lgs. 231/2001 prevede espressamente, al relativo art. 6, comma 2, lett. a), che il modello di organizzazione, gestione e controllo dell'ente individui le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Di conseguenza, la Società ha proceduto ad un'analisi approfondita delle stesse.

Nell'ambito di tale attività, la Società ha, in primo luogo, analizzato la propria struttura organizzativa rappresentata nell'organigramma aziendale che individua le funzioni aziendali, evidenziandone ruoli e linee di riporto gerarchico-funzionali. Detto documento è custodito presso la sede della Società disponibile per relativa consultazione.

Come anticipato, i risultati di detta attività sono stati raccolti e formalizzati in una scheda descrittiva che forma parte del Modello, denominata "**Mappatura delle attività a rischio-reato**" e che illustra in dettaglio i profili di rischio di Deloitte Risk Advisory S.r.l. relativi alla

commissione dei reati ricompresi nel D.Lgs. 231/2001.

In particolare, nella Mappatura delle attività a rischio-reato sono dettagliate le aree aziendali (declinate a loro volta in una serie di esempi di attività “sensibili”) a rischio di possibile commissione dei reati previsti dal D.Lgs. 231/2001 (c.d. “aree di attività a rischio”), i reati associabili, gli esempi di possibili modalità e finalità di realizzazione degli stessi, nonché i processi nel cui svolgimento, sempre in linea di principio, potrebbero crearsi le condizioni e/o i mezzi per la commissione dei reati (c.d. “processi strumentali/funzionali”).

La Mappatura delle attività a rischio-reato è custodita presso la sede della Società e viene archiviata e resa disponibile - per eventuale consultazione - al Consiglio di Amministrazione, all’Organismo di Vigilanza e a chiunque sia autorizzato dalla Società a prenderne visione.

## **E. Aree e processi aziendali a potenziale “rischio – reato”**

### ▪ Aree a “rischio - reato”

È stato riscontrato il rischio di potenziale commissione dei reati previsti dal D.Lgs. 231/2001 nelle aree di attività aziendale di seguito riportate, come individuate nella Mappatura delle attività a rischio-reato:

- A. Gestione dei rapporti di alto profilo con soggetti appartenenti alla Pubblica Amministrazione o ad altri Enti Pubblici;
- B. Acquisizione di incarichi professionali con enti pubblici mediante procedura ad evidenza pubblica;
- C. Acquisizione di incarichi professionali con clienti privati;
- D. Gestione degli incarichi professionali con clienti pubblici, privati e con entità del DTTL Network;
- E. Gestione delle attività professionali nell'ambito di incarichi a favore di clienti pubblici o privati e dei rapporti con Autorità pubbliche in nome e per conto dei clienti;
- F. Gestione delle attività promozionali;
- G. Gestione delle informazioni *price sensitive* (economiche, patrimoniali, finanziarie e strategiche), trattate nello svolgimento delle attività;
- H. Gestione dei rapporti con i fornitori nell'ambito della gestione dell'attività caratteristica;
- I. Gestione dei rapporti con funzionari pubblici per adempimenti normativi anche in occasione di verifiche e ispezioni sul rispetto della normativa applicabile;
- J. Gestione del rapporto di lavoro relativo a dipendenti e collaboratori;
- K. Gestione degli adempimenti previsti dal D. Lgs. 81/2008 (Testo Unico Sicurezza);

- L. Adempimenti connessi alla gestione dei rifiuti;
- M. Contenzioso in capo alla Società;
- N. Gestione dei sistemi informativi aziendali;
- O. Gestione della contabilità generale e predisposizione del progetto di bilancio civilistico e di eventuali situazioni patrimoniali, anche in occasione di operazioni straordinarie, ed altri adempimenti in materia societaria;
- P. Richiesta, percezione e gestione di contributi e finanziamenti agevolati erogati da enti pubblici nazionali e sovranazionali;
- Q. Presentazione delle dichiarazioni fiscali.

In considerazione delle aree di attività aziendale sopra richiamate, sono risultati ad esse potenzialmente associabili i seguenti reati presupposto:

- **Art. 24:** *Truffa in danno dello Stato o di altro ente pubblico (art. 640, comma 2, n. 1, c.p.); Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.); Indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.); Malversazione a danno dello Stato (art. 316-bis c.p.);*
- **Art. 24-bis:** *Accesso abusivo a sistema informatico e telematico (art. 615-ter c.p.); Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.); Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);*
- **Art. 24-ter:** *Associazione per delinquere (art. 416 c.p.), reato associato in via prudenziale;*
- **Art. 25:** *Corruzione e Istigazione alla Corruzione (artt. 318, 319, 320, 322, 322-bis c.p.), Corruzione in atti giudiziari (art. 319-ter c.p.), Induzione indebita a dare o promettere utilità (art. 319-quater c.p.), Traffico di influenze illecite (art. 346-bis c.p.);*
- **Art. 25-ter:** *False comunicazioni sociali (art. 2621 c.c.); Fatti di lieve entità (art. 2621-bis c.c.); Impedito controllo (art. 2625, comma II); Indebita restituzione dei conferimenti (art. 2626 c.c.); Illegale ripartizione di utili e riserve (art. 2627 c.c.); Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.); Operazioni in pregiudizio dei creditori (art. 2629 c.c.); Formazione fittizia del capitale (art. 2632 c.c.), Corruzione tra privati (art. 2635 c.c.), Istigazione alla corruzione tra privati (art. 2635-bis c.c.); Illecita influenza sull'assemblea (art. 2636 c.c.); Aggiotaggio (art. 2637 c.c.); Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.);*
- **Art. 25-sexies:** *Manipolazione del mercato (art. 185 D.Lgs. n. 58/1998 come successivamente modificato); Abuso di informazioni privilegiate (art. 184 D.Lgs. n. 58/1998 come successivamente modificato);*

- **Art. 25-septies:** *Omicidio colposo, Lesioni personali colpose (artt. 589-590 c.p.);*
- **Art. 25-octies:** *Ricettazione, Riciclaggio, Impiego di denaro, beni o utilità di provenienza illecita, nonché Autoriciclaggio (artt. 648, 648-bis, 648-ter, 648-ter.1 c.p.);*
- **Art. 25-novies:** *Violazione dell'art. 171bis della Legge 22 aprile 1941 n. 633 (“Protezione del diritto d'autore e di altri diritti connessi al suo esercizio – Duplicazione abusiva di software”);*
- **Art. 25-decies:** *Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.);*
- **Art. 25-undecies:** *Attività di gestione di rifiuti non autorizzata (art. 256 D.Lgs. 152/2006), reato associato in via prudenziale;*
- **Art. 25-duodecies:** *Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12-bis, D.Lgs. n. 286/1998); Disposizioni contro le immigrazioni clandestine (art. 12, comma 3, 3-bis, 3-ter e comma 5, D.Lgs. n. 286/1998);*
- **Art. 25-quinquiesdecies:** *Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 1, del D.Lgs. 74/2000); Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 2-bis, del D.Lgs. 74/2000); Dichiarazione fraudolenta mediante altri artifici (art. 3 del D.Lgs. 74/2000); Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, comma 1, del D.Lgs. 74/2000); Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, comma 2-bis, del D.Lgs. 74/2000); Occultamento o distruzione di documenti contabili (art. 10 del D.Lgs. 74/2000); Sottrazione fraudolenta al pagamento di imposte (art. 11 del D.Lgs. 74/2000).*

Il rischio di commissione dei reati di cui agli artt. 25 bis, 25 bis.1, 25 quater, 25 quater.1, 25 quinquies, 25 terdecies e 25 quaterdecies del Decreto, nonché dei reati transnazionali di cui all'art. 10 della Legge 146/2006, per quanto non si possa escludere *tout court*, è stato ritenuto remoto e ragionevolmente coperto dal rispetto dei principi enunciati nel Codice Etico della Società, che vincola tutti i suoi destinatari alla più rigorosa osservanza delle leggi e delle normative applicabili.

#### ▪ **Processi aziendali “strumentali/funzionali”**

Nell'ambito dell'attività sopra rappresentata, sono stati anche individuati dalla Società i processi aziendali c.d. strumentali/funzionali alla commissione del reato, ovvero sia quei processi aziendali nel cui ambito, in linea di principio, potrebbero verificarsi le condizioni e/o essere rinvenuti i mezzi per la commissione delle fattispecie di reato rilevanti ai fini del Decreto.

Si precisa che lo svolgimento delle attività nell'ambito di taluni processi aziendali viene svolto

con il supporto di altre società italiane facenti parte del DCM Network mediante contratti di servizio nei quali vengono disciplinate le condizioni e i livelli di servizio che concorrono a costituire adeguato presidio di controllo con riferimento alle attività gestite per conto della Società.

Vengono di seguito riportati i processi aziendali c.d. strumentali/funzionali:

1. Gestione dei flussi monetari e finanziari;
2. Gestione degli acquisti;
3. Gestione di consulenze e incarichi professionali a terzi;
4. Gestione delle donazioni, sponsorizzazioni e altre liberalità;
5. Selezione, assunzione e gestione del personale dipendente e dei collaboratori, assegnazione dei benefit aziendali;
6. Gestione dei rimborsi spese, anticipi e spese di rappresentanza;
7. Gestione della contabilità generale, della formazione del bilancio e degli adempimenti societari e dei rapporti con il Collegio Sindacale e i Soci;
8. Gestione delle gare e dei rapporti con la Pubblica Amministrazione;
9. Gestione dei rapporti con il Mercato;
10. Gestione delle erogazioni pubbliche (fasi di richiesta, utilizzo e rendicontazione);
11. Gestione del sistema salute, sicurezza e ambiente;
12. Gestione dei dati, utilizzo e intervento sui sistemi informativi, anche di soggetti terzi;
13. Gestione degli adempimenti fiscali;
14. Valutazione e accettazione del cliente e dell'incarico professionale.

A ciascun processo strumentale, rilevante nella realtà aziendale, ritenuto a rischio di commissione dei reati previsti dal Decreto, è stata dedicata una specifica Sezione della Parte Speciale del presente Modello ove sono stati formulati i principi di controllo, declinati nei Protocolli 231, adottati dalla Società per prevenire il rischio di commissione dei reati nella gestione delle attività sensibili e dei processi sensibili/strumentali della Società.

## **E.1 La struttura del sistema organizzativo e di controllo**

Nella predisposizione del Modello e sulla base dei processi aziendali risultati rilevanti in chiave 231, la Società ha riesaminato il proprio sistema organizzativo e di controllo, al fine di verificare se esso fosse idoneo a prevenire gli specifici reati previsti dal Decreto nelle aree di attività aziendale identificate a rischio.

In particolare, il sistema organizzativo e di controllo di DRA si basa, oltre che sulle regole comportamentali riportate nel paragrafo E.2 e sui principi di controllo declinati nella Parte Speciale del presente Modello, sui seguenti elementi:

- il Codice Etico di cui al par. D.4;



- il sistema di deleghe e procure esistente;
- la struttura gerarchico-funzionale rappresentata nell'organigramma aziendale;
- sistemi informativi orientati alla segregazione delle funzioni e alla protezione delle informazioni in essi contenute, con particolare riferimento ai sistemi gestionali e contabili;
- un sistema di procedure che disciplina ulteriormente in dettaglio lo svolgimento delle attività aziendali, nonché delle modalità operative richieste per l'espletamento dei compiti assegnati a ciascuno;
- certificazioni in conformità ad esempio agli standard ISO/IEC 27001 - Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e ISO 9001 - Sistema di gestione della Qualità (SGQ);
- i contratti di servizio con altre società italiane del DCM Network nei quali vengono disciplinate le condizioni e i livelli di servizio che concorrono a costituire adeguato presidio di controllo con riferimento alle attività gestite per conto della Società.

L'attuale sistema organizzativo e di controllo di Deloitte Risk Advisory S.r.l., volto a gestire e monitorare i principali rischi aziendali, assicura il raggiungimento dei seguenti obiettivi:

- efficacia ed efficienza nell'impiegare le risorse aziendali, nel proteggersi dalle perdite e nel salvaguardare il patrimonio della Società;
- rispetto delle leggi e dei regolamenti applicabili in tutte le operazioni ed azioni della Società;
- affidabilità delle informazioni, da intendersi come comunicazioni tempestive e veritiere a garanzia del corretto svolgimento di ogni processo decisionale.
- verificabilità di ogni operazione, transazione e azione, che deve essere inoltre documentata, coerente e congrua.

- **Sistema organizzativo, separazione dei ruoli e attribuzione delle responsabilità**

Il sistema organizzativo deve rispettare requisiti di: (i) chiarezza, formalizzazione e pubblicità, con particolare riferimento all'attribuzione di responsabilità, alla definizione delle linee gerarchiche e all'assegnazione delle attività operative; (ii) corretta distribuzione delle responsabilità e previsione di adeguati livelli autorizzativi (i.e. principio di separazione dei ruoli), in modo da evitare sovrapposizioni funzionali e la concentrazione su di una sola persona di attività che presentino profili di criticità o rischio.

Al fine di garantire tali requisiti, DRA è dotata di:

1. strumenti organizzativi (es. organigramma, comunicazioni organizzative, ecc.) improntati a principi generali di: (i) conoscibilità all'interno della Società; (ii) chiara descrizione delle

linee di riporto; *(iii)* chiara e formale delimitazione dei ruoli, con descrizione dei compiti e delle responsabilità attribuite a ciascuna funzione;

2. un sistema di deleghe e procure, riguardante sia i poteri autorizzativi interni, dai quali dipendono i processi decisionali della Società in merito alle operazioni da porre in essere, sia i poteri di rappresentanza per la firma di atti o documenti destinati all'esterno e idonei a vincolare la Società (cosiddette "procure" speciali o generali). Le deleghe di poteri rispettano i seguenti requisiti: *(i)* sono definite e formalmente assegnate; *(ii)* sono coerenti con le responsabilità ed i compiti delegati e con le posizioni ricoperte nell'ambito della struttura organizzativa; *(iii)* prevedono limiti di esercizio in coerenza con i ruoli attribuiti, con particolare attenzione ai poteri di spesa e ai poteri autorizzativi e/o di firma delle operazioni e degli atti considerati a rischio in ambito aziendale; *(iv)* sono aggiornate in conseguenza dei mutamenti organizzativi.

## • **Protocolli 231**

All'esito dell'identificazione delle attività a rischio-reato e dei relativi processi strumentali, Deloitte Risk Advisory S.r.l. ha deciso di dotarsi, altresì, di principi di controllo posti a presidio dei processi strumentali più critici, come declinati nel paragrafo E.

I Protocolli 231, che sono inseriti nella Parte Speciale del Modello, contengono in sostanza la disciplina ritenuta più idonea a governare i profili di rischio individuati, declinando un insieme di principi per lo svolgimento di ciascun processo aziendale, che richiedono costante aggiornamento al fine di rappresentare efficacemente la realtà organizzativa di DRA.

Si tratta, in particolare, dei seguenti Protocolli 231:

- 1) Protocollo ex D.Lgs. 231/2001 – Gestione dei flussi monetari e finanziari;
- 2) Protocollo ex D.Lgs. 231/2001 – Gestione degli acquisti;
- 3) Protocollo ex D.Lgs. 231/2001 – Gestione di consulenze o incarichi professionali a terzi;
- 4) Protocollo ex D.Lgs. 231/2001 – Gestione delle donazioni, sponsorizzazioni e altre liberalità;
- 5) Protocollo ex D.Lgs. 231/2001 – Selezione, assunzione e gestione del personale dipendente e dei collaboratori, assegnazione dei benefit aziendali;
- 6) Protocollo ex D.Lgs. 231/2001 – Gestione dei rimborsi spese, anticipi e spese di rappresentanza;
- 7) Protocollo ex D.Lgs. 231/2001 – Gestione della contabilità generale, della formazione del Bilancio e degli adempimenti societari e dei rapporti con il Collegio Sindacale e i Soci;
- 8) Protocollo ex D.Lgs. 231/2001 – Gestione delle gare e dei rapporti con la Pubblica Amministrazione;
- 9) Protocollo ex D.Lgs. 231/2001 – Gestione dei rapporti con il mercato;
- 10) Protocollo ex D.Lgs. 231/2001 – Gestione delle erogazioni pubbliche (fasi di richiesta, utilizzo e rendicontazione);

- 11) Protocollo ex D.Lgs. 231/2001 — Gestione del sistema salute, sicurezza e ambiente;
- 12) Protocollo ex D.Lgs. 231/2001 – Gestione dei dati, utilizzo e intervento sui sistemi informativi, anche di soggetti terzi;
- 13) Protocollo ex D.Lgs. 231/2001 – Gestione degli adempimenti fiscali;
- 14) Protocollo ex D.Lgs. 231/2001 - Valutazione e accettazione del cliente e dell'incarico professionale.

- **Attività di controllo e monitoraggio**

DRA ha posto in essere attività di controllo e monitoraggio che coinvolgono, con ruoli diversi, vari organismi di controllo dotati, oltre che di autonomia ed indipendenza, anche di un elevato grado di competenza e professionalità.

I compiti di controllo di tali organi sono definiti nel rispetto delle seguenti tipologie di controllo: (i) *controlli di linea*, finalizzati ad assicurare il corretto svolgimento delle attività, effettuati dagli stessi partecipanti alle attività; (ii) *attività di monitoraggio esterna*, finalizzata alla rilevazione delle anomalie e delle violazioni delle procedure aziendali ed alla valutazione della funzionalità del complessivo sistema dei controlli interni, esercitata dalla Funzione Internal Audit; (iii) *attività di vigilanza* sulla corretta amministrazione della Società, sull'adeguatezza delle strutture organizzative e sull'osservanza della legge e dell'atto costitutivo.

## **E.2 Regole Comportamentali**

Di seguito si riportano le regole comportamentali di carattere generale adottate dalla Società nel rispetto dei dettami del Decreto.

### *E.2.1. Comportamenti da tenere nei rapporti con la Pubblica Amministrazione, con le Autorità Amministrative Indipendenti e con le Autorità di Vigilanza*

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, intrattengano rapporti con la Pubblica Amministrazione, le Autorità Amministrative Indipendenti o con le Autorità di Vigilanza, italiane o straniere, per conto o nell'interesse della Società.

In via generale, ai Destinatari è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste dagli artt. 24 e 25 del Decreto.

In particolare, coerentemente con i principi espressi nel Codice Etico adottato dalla Società, è fatto divieto di:

- promettere o effettuare erogazioni in denaro a favore di rappresentanti della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti o delle Autorità di Vigilanza;
- promettere o concedere vantaggi di qualsiasi natura in favore di rappresentanti della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti e Autorità di

Vigilanza, al fine di influenzarne l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio alla Società;

- effettuare prestazioni o pagamenti in favore di collaboratori, fornitori, consulenti, o altri soggetti terzi che operino per conto della Società, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi ovvero in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- favorire, nei processi di acquisto, collaboratori, fornitori, consulenti o altri soggetti terzi in quanto indicati da rappresentanti della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti o delle Autorità di Vigilanza;
- prendere in considerazione o proporre un'opportunità di impiego che possa avvantaggiare un rappresentante della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti o dell'Autorità di Vigilanza ovvero un soggetto da questi segnalato, al fine di assicurare un qualsiasi vantaggio alla Società;
- distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale come illustrato nel Protocollo 4 della Parte Speciale. In particolare, è vietata qualsiasi forma di regalo o altra utilità a rappresentanti della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti o delle Autorità di Vigilanza o a loro familiari, che possa influenzarne l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore. I regali offerti - salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire le verifiche da parte dell'Organismo di Vigilanza;
- tenere una condotta ingannevole che possa indurre la Pubblica Amministrazione, le Autorità Amministrative Indipendenti o l'Autorità di Vigilanza in errore di valutazione tecnico-economica sulla documentazione presentata;
- esibire al Funzionario della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti o dell'Autorità di Vigilanza, documenti o dati falsi o alterati ovvero rendere informazioni non corrispondenti al vero;
- omettere informazioni dovute al fine di orientare a proprio favore le decisioni della Pubblica Amministrazione, delle Autorità Amministrative Indipendenti o delle Autorità di Vigilanza;
- presentare dichiarazioni non veritiere a organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui sono destinati;
- sfruttare relazioni esistenti o asserite con un pubblico ufficiale o con un incaricato di un pubblico servizio, facendo dare o promettere indebitamente, a sé o ad altri, denaro o altra utilità come corrispettivo della mediazione illecita verso il pubblico ufficiale, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri;
- dare o promettere denaro o altra utilità ad altri affinché intercedano presso un pubblico ufficiale ovvero per remunerare quest'ultimo in relazione all'esercizio delle sue funzioni o dei suoi poteri.

È fatto obbligo di applicare le medesime regole comportamentali ai Destinatari che, per conto di DRA, intrattengano rapporti con l’Autorità giudiziaria (nell’ambito di procedimenti di qualsiasi natura). In particolare, è richiesto di:

- evadere con tempestività, correttezza e buona fede tutte le richieste provenienti dagli organi di polizia giudiziaria e dall’Autorità giudiziaria inquirente e giudicante, fornendo tutte le informazioni, i dati e le notizie richieste;
- mantenere, nei confronti degli organi di polizia giudiziaria e dell’Autorità giudiziaria un comportamento disponibile, collaborativo e trasparente.

Ai fini dell’attuazione dei comportamenti di cui sopra:

- i rapporti nei confronti dell’Autorità giudiziaria, della Pubblica Amministrazione e delle Autorità di Vigilanza devono essere gestiti in modo unitario, attraverso l’individuazione di uno o più responsabili aziendali di riferimento per ciascuna attività svolta;
- gli incarichi conferiti a soggetti terzi (es. fornitori, consulenti) devono essere redatti per iscritto, con indicazione dell’oggetto dell’incarico, del compenso pattuito ed essere sottoscritti conformemente alle deleghe ricevute;
- sono vietate forme di pagamento “cash” o in natura.

Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all’espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull’attuazione degli adempimenti stessi e riferire immediatamente all’Organismo di Vigilanza presunte situazioni di irregolarità o di non conformità eventualmente riscontrate.

E’ fatto obbligo ai Destinatari di attenersi alle seguenti prescrizioni: in caso di presunta tentata concussione da parte di un pubblico funzionario (da intendersi quale abuso della qualità o potere da parte di un funzionario pubblico al fine di costringere o indurre taluno a dare o promettere, allo stesso o a un terzo, denaro o altre utilità non dovute per lo svolgimento dei relativi doveri d’ufficio), il soggetto interessato deve: (i) rifiutare la richiesta; (ii) fornire tempestivamente informativa al *Business Risk Leader* e attivare formale informativa nei confronti dell’Organismo di Vigilanza.

La Società applica inoltre i principi di comportamento della Policy Anti-Corruzione, nonché delle *policy* e linee guida, sia nazionali sia straniere applicabili alle entità del DCM Network<sup>3</sup>.

*E.2.2. Comportamenti da tenere nell’ambito delle attività “sensibili” rispetto ai delitti informatici e trattamento illecito di dati (cybercrime).*

–  
<sup>3</sup> La Convenzione dell’Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) del 17 dicembre 1997, sulla lotta alla corruzione dei Pubblici Ufficiali stranieri nelle operazioni economiche internazionali; La Convenzione delle Nazioni Unite contro la corruzione, adottata dall’Assemblea generale il 31 ottobre 2003, entrata in vigore a livello internazionale il 14 dicembre 2005 e ratificata in Italia dalla Legge 116/2009; Il Foreign Corrupt Practice Act (FCPA) emanato negli Stati Uniti nel 1977; Il 2010 United Kingdom Bribery Act (UKBA) emanato nel Regno Unito; Le “Disposizioni per la prevenzione e la repressione della corruzione e dell’illegalità nella pubblica amministrazione” emanate in Italia con la Legge 6 novembre 2012 n. 190; Le “Disposizioni in materia di delitti contro la pubblica amministrazione, di associazioni di tipo mafioso e di falso in bilancio” emanate in Italia con la Legge 27 maggio 2015, n. 69; La norma UNI ISO 37001:2016. Disciplinary Policy; DPM 1550 (Anti-Corruption); DPM 1551 (The United States Foreign Corrupt Practices Act); DPM 1552 (The UK Bribery Act 2010); Detailed Guidelines and Minimum Expectations for Conducting Third Party Due Diligence; DCM Policy.

Le seguenti regole comportamentali obbligano i Destinatari che, nello svolgimento della propria attività lavorativa, utilizzano i sistemi informativi della Società o accedono, autorizzati, ai sistemi dei clienti.

In via generale è fatto loro obbligo di rispettare la normativa e le procedure aziendali poste a tutela del sistema informativo aziendale e del trattamento di dati personali, astenendosi dal commettere, o anche solo agevolare, la realizzazione dei delitti informatici di cui all'art. 24-bis del Decreto.

In particolare, i Destinatari sono tenuti a:

- promuovere un adeguato livello di salvaguardia del patrimonio informatico e telematico aziendale, dei terzi e dei clienti, siano essi privati o pubblici, e astenersi, pertanto, da qualsiasi condotta che possa compromettere la sicurezza, riservatezza e integrità delle informazioni e dei dati aziendali e altrui;
- non diffondere le informazioni ricevute dalla Società per l'uso dei mezzi informatici aziendali e l'accesso a dati, sistemi e applicazioni aziendali;
- astenersi da qualsiasi condotta diretta a superare o ad aggirare le protezioni del sistema informativo aziendale o dei clienti o di terzi, siano essi privati o pubblici;
- astenersi da qualsiasi condotta diretta a comunicare chiavi di accesso ai sistemi informativi di clienti o di terzi conosciute nello svolgimento dell'attività di consulenza;
- attuare i comportamenti necessari per proteggere il sistema informativo aziendale, diretti ad evitare che terzi possano accedervi in caso di allontanamento dalla postazione di lavoro;
- accedere al sistema informativo aziendale unicamente attraverso i codici di identificazione assegnati, provvedendo alla modifica periodica tutte le volte in cui il sistema lo richieda;
- astenersi dall'alterare, distruggere, sopprimere, cancellare dati, informazioni o programmi del sistema informativo della Società o dei clienti, siano essi privati o pubblici, nonché dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità;
- conservare i codici identificativi assegnati, astenendosi dal comunicarli a terzi che in tal modo potrebbero accedere abusivamente a dati aziendali riservati;
- astenersi dall'accedere ai sistemi informativi dei clienti in assenza della relativa autorizzazione e, in caso di autorizzazione, nei limiti dell'attività professionale svolta e comunque secondo le modalità e direttive impartite dal cliente;
- astenersi, in caso di autorizzazione da parte del cliente all'accesso al proprio sistema informativo, dall'alterarne in qualsiasi modo il funzionamento, anche al solo fine di acquisire senza diritto dati, informazioni o programmi informatici.

La Società, allo scopo di proteggere il proprio sistema informativo e di evitare il

coinvolgimento in delitti informatici e di trattamento illecito di dati, si è dotata, tra le altre, delle seguenti misure di protezione:

- accesso ai sistemi informativi aziendali esclusivamente previa identificazione dell'utente, a mezzo username e password assegnati;
- comunicazione al personale delle modalità di modifica dei codici identificativi originariamente assegnati;
- verifica della coincidenza tra i poteri assegnati al profilo utente e le rispettive mansioni all'interno dell'azienda, anche in caso di cessazione del rapporto di lavoro;
- controllo, con frequenza periodica, di tutti gli accessi e le attività svolte sulla rete aziendale nel rispetto dei limiti imposti dalla legge in materia di protezione dei dati personali e dai provvedimenti emessi dalla competente Autorità Garante della privacy;
- informazione adeguata in merito ai comportamenti richiesti a tutela della sicurezza informatica aziendale.

La Società si è inoltre dotata di un sistema di gestione della sicurezza delle informazioni conforme allo standard internazionale ISO/IEC 27001.

### *E.2.3. Comportamenti da tenere nell'ambito delle attività "sensibili" rispetto ai reati di associazione per delinquere.*

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del Modello che, a qualunque titolo, siano coinvolti nelle attività "sensibili" rispetto al reato di associazione per delinquere (associato in via prudenziale).

Il reato di associazione per delinquere trova adeguato presidio nei principi del Codice Etico, nel sistema di deleghe nonché nel Modello nel suo complesso. Tali principi sono volti a prevenire il rischio di costituzione di un'associazione per delinquere sia all'interno della Società, sia nei rapporti con i terzi (ad esempio clienti, fornitori).

In via generale, la Società richiede di conformarsi alle seguenti regole comportamentali:

- conformità alle leggi vigenti, nonché ai principi di correttezza, trasparenza, buona fede e tracciabilità della documentazione;
- rispetto del principio di separazione di ruoli e responsabilità.

È inoltre vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare la fattispecie di associazione per delinquere, nonché, in ogni caso, incoraggiare, sostenere o partecipare ad associazioni per delinquere.

### *E.2.4. Comportamenti da tenere nell'ambito delle attività "sensibili" rispetto ai reati societari*

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari che, a qualunque titolo, siano coinvolti nelle attività “sensibili” rispetto ai reati societari di cui agli artt. 2621 e ss. c.c..

In via generale, ai Destinatari è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, possano integrare o concorrere a integrare, direttamente o indirettamente, le fattispecie di reato previste dall’art. 25 ter del Decreto.

In via generale, a tali soggetti è richiesto di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai Soci ed ai terzi un’informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, ponendo la massima attenzione ed accuratezza nell’acquisizione, elaborazione ed illustrazione dei dati e delle informazioni relative a società clienti (quotate e non quotate), necessarie per consentire agli investitori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della Società, sull’evoluzione della sua attività, nella gestione di tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire al mercato un’informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria delle società clienti;
- garantire la massima collaborazione, assicurando la completezza, chiarezza e tempestività delle informazioni fornite, nonché l’accuratezza dei dati e delle elaborazioni contabili;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell’integrità ed effettività del capitale sociale;
- assicurare il regolare funzionamento della Società e degli organi societari, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale, nonché la libera e corretta formazione della volontà assembleare;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge nei confronti delle Autorità di Vigilanza, con cui la Società intrattiene rapporti, non frapponendo alcun ostacolo all’esercizio delle funzioni di vigilanza da queste esercitate, anche con riferimento alle attività gestite per conto del cliente, non frapponendo alcun ostacolo all’esercizio delle funzioni di vigilanza da queste esercitate, anche in sede di visita ispettiva, garantendo la massima collaborazione e completezza delle informazioni fornite.

È inoltre previsto l’espreso divieto a carico dei Destinatari, qualora se ne configuri l’applicabilità, di:

- porre in essere operazioni simulate o diffondere notizie false sulla Società e sulla sua attività;
- rappresentare o trasmettere per l’elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società;



- omettere dati e informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- restituire conferimenti ai Soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- acquistare o sottoscrivere quote della Società fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- procedere a formazione o aumenti fittizi del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;
- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo da parte dei Soci e del Collegio Sindacale;
- determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di Vigilanza cui è soggetta l'attività aziendale, nonché la trasmissione di dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette Autorità;
- esporre, nelle predette comunicazioni e trasmissioni, fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza, anche in sede di ispezione, da parte delle Autorità di Vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

In relazione al reato di "Corruzione tra privati" (art. 2635 c.c.) e di "Istigazione alla corruzione tra privati" (art. 2635-bis c.c.), è imputabile a titolo di responsabilità amministrativa la società che ponga in essere, anche attraverso la condotta di propri dipendenti, atti di corruzione nei confronti dei soggetti apicali di una controparte privata o di loro sottoposti, al fine di influenzarne il comportamento per ottenere un vantaggio per la società stessa (es. società cliente, fornitore, *partner* commerciale).

Per soggetti apicali di una controparte privata si intendono, in particolare, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori; per soggetti sottoposti si intendono coloro che soggiacciono alla direzione o alla vigilanza dei predetti apicali.

Il referente della controparte privata agisce in conflitto di interessi con l'ente di appartenenza, avvantaggiando la società corruttrice in conseguenza del denaro o delle altre utilità ricevute a

titolo personale o elargite a favore di terzi allo stesso legati.

Al fine di prevenire il rischio di commissione degli anzidetti reati, lo svolgimento delle attività di negoziazione, stipulazione ed esecuzione dei contratti con i clienti privati, i fornitori di beni e servizi, i *partner* commerciali e i consulenti terzi deve ispirarsi ai principi di correttezza, trasparenza e indipendenza nonché ai valori sanciti nel Codice Etico di Deloitte Risk Advisory S.r.l..

Più in particolare, è fatto divieto ai Destinatari di influenzare le decisioni dei soggetti che operano presso la controparte privata in maniera impropria e/o illecita, anche per interposta persona.

È fatto inoltre divieto, direttamente o per interposta persona di:

- offrire, promettere o effettuare erogazioni in denaro, sollecitare, autorizzare qualcuno a promettere denaro o pagare a favore di soggetti che operano presso la controparte privata al fine di accedere in anteprima a informazioni utili per la realizzazione degli obiettivi sociali o comunque di favorire le politiche economiche e commerciali della Società;
- promettere e/o offrire e/o corrispondere (e/o sollecitare qualcuno a farlo) a soggetti che operano presso la controparte privata, direttamente o tramite terzi, somme di denaro o altre utilità al fine di pervenire alla stipulazione di contratti e all'affidamento di incarichi di consulenza vantaggiosi per la Società, o di ottenere, più in generale, favori o vantaggi impropri;
- offrire e/o corrispondere omaggi o forme di ospitalità diversi di quanto previsto dalla prassi aziendale come illustrata nel Protocollo 4 della Parte Speciale del presente Modello e/o, in ogni caso, tali da compromettere l'imparzialità e l'indipendenza di giudizio della controparte, salvo nel caso in cui l'omaggio o il beneficio sia di valore modico e riconducibile a normali relazioni di cortesia;
- sfruttare relazioni esistenti o asserite con un pubblico ufficiale o con un incaricato di un pubblico servizio, facendo dare o promettere indebitamente, a sé o ad altri, denaro o altra utilità come corrispettivo della mediazione illecita verso il pubblico ufficiale o l'incaricato di pubblico servizio, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri;
- effettuare pagamenti o riconoscere altre utilità a clienti, fornitori, consulenti, che non trovino adeguata giustificazione nel rapporto contrattuale ovvero nella prassi vigenti;
- favorire, nei processi di assunzione o di acquisto, soggetti segnalati da clienti, fornitori o consulenti, in cambio di favori, compensi o altri vantaggi.

Inoltre, i principi di comportamento anti-corruzione, così come specificati al paragrafo E.2.1. *“Comportamenti da tenere nei rapporti con la Pubblica Amministrazione e con le Autorità di Vigilanza”*, costituiscono un utile presidio anche ai fini del reato di corruzione tra privati.

#### *E.2.5. Comportamenti da tenere nell'ambito delle attività “sensibili” rispetto ai reati di “Abuso di informazioni privilegiate” e di “Manipolazione del mercato”*

Le seguenti regole comportamentali si applicano ai Destinatari che nello svolgimento delle proprie attività si trovino, a qualunque titolo, a gestire informazioni riservate o privilegiate concernenti i propri clienti.

In via generale, ai Destinatari è richiesto di:

- assicurare diligenza e professionalità nello svolgimento dell'attività lavorativa;
- gestire la documentazione e le informazioni relative ai clienti, acquisite nello svolgimento delle attività professionali, assicurandosi che l'accesso alle stesse sia limitato ai soli componenti del team di progetto ovvero a soggetti autorizzati, nel rispetto delle disposizioni normative vigenti;
- tenere, in ogni caso, un comportamento corretto e trasparente, nel rispetto delle norme di legge, ponendo la massima attenzione nell'acquisizione ed elaborazione dei dati e delle informazioni relative a società clienti, necessarie per consentire agli investitori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria delle società stesse;
- valutare periodicamente l'assenza di situazioni di conflitto d'interessi in relazione agli incarichi professionali ed ai clienti acquisiti.

È fatto inoltre divieto ai Destinatari di:

- con riferimento al reato di “abuso di informazioni privilegiate”, qualora gli stessi siano venuti in possesso di tali informazioni nell'esercizio della loro attività lavorativa, professione o ufficio:
  - i. acquistare, vendere o compiere altre operazioni, direttamente o indirettamente, per conto proprio o di terzi sugli strumenti finanziari utilizzando le medesime informazioni;
  - ii. comunicare tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione o ufficio o di un sondaggio di mercato effettuato ai sensi dell'art. 11 del Regolamento UE n. 596/2014);
  - iii. raccomandare o indurre altri, sulla base di tali informazioni, al compimento di una delle operazioni di cui alla precedente lettera i);
- con riferimento al reato di “manipolazione del mercato” e aggioaggio:
  - i. diffondere notizie false o porre in essere operazioni simulate o altri artifici, concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari delle società clienti;
  - ii. diffondere notizie false o porre in essere operazioni simulate o altri artifici, idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato relativi a società clienti;
  - iii. divulgare qualsiasi notizia o informazione sull'attività di DRA e sull'attività professionale svolta presso le società clienti.

La Società ha istituito e mantiene, il “Registro delle persone che hanno accesso alle informazioni privilegiate” (c.d. *Registro Insiders*) del Regolamento UE 2014/596 (c.d. MAR), in ragione dell'attività professionale resa in favore di emittenti quotati (per tali intendendosi anche coloro

che hanno richiesto l'ammissione alla quotazione ed è in corso la relativa procedura) ovvero di soggetti in rapporto di controllo con questi ultimi (sia controllanti sia controllati).

## *E.2.6. Comportamenti da tenere nell'ambito delle attività "sensibili" rispetto ai reati colposi commessi in violazione della normativa antinfortunistica*

In via generale è fatto obbligo a tutti i Destinatari, a vario titolo coinvolti nella gestione del sistema sicurezza della Società adottato ai sensi del D.Lgs. 81/2008 e successive modifiche e integrazioni (di seguito anche "**Testo Unico Sicurezza**") per la tutela della salute e della sicurezza dei propri dipendenti, di dare attuazione, ciascuno per la parte di propria competenza e nel rispetto delle deleghe e procure attribuite, alle procedure aziendali che regolano il sistema sicurezza della Società, alle misure di prevenzione poste a presidio dei rischi connessi alla sicurezza identificati nel Documento di Valutazione dei Rischi (di seguito "**DVR**") redatto secondo le prescrizioni del Testo Unico Sicurezza.

Per un'effettiva prevenzione dei rischi e in coerenza con le previsioni del D.Lgs. 81/2008, nonché con la ripartizione di ruoli, compiti e responsabilità all'interno della Società, è fatta espressa richiesta:

- al Datore di Lavoro e alle altre funzioni aziendali - a vario titolo - coinvolte nella gestione del sistema sicurezza aziendale (Delegato in materia di sicurezza ex art. 16 del D.Lgs. 81/2008 e Dirigenti), di svolgere i compiti loro attribuiti dalla Società in tale ambito, nel rispetto delle procure e/o deleghe ricevute, delle misure di prevenzione adottate e delle procedure aziendali esistenti, avendo cura di formare e informare il personale che, nello svolgimento delle proprie attività, si trovi esposto ai rischi;
- ai soggetti incaricati ai sensi del D.Lgs. 81/2008 (es. Responsabile del Servizio di Prevenzione e Protezione; Addetti al Servizio di Prevenzione e Protezione; Incaricati dell'attuazione delle misure di prevenzione incendi, evacuazione in caso di pericolo grave e immediato, salvataggio, primo soccorso; Medico Competente; Rappresentanti per la Sicurezza dei Lavoratori) di svolgere, ciascuno nell'ambito delle proprie attribuzioni, i compiti di sicurezza specificamente affidati dalla normativa vigente e previsti nel sistema sicurezza della Società;
- ai Preposti di vigilare sulla corretta osservanza, da parte di tutti i lavoratori, delle misure e delle procedure di sicurezza adottate dalla Società, segnalando eventuali carenze o disallineamenti del sistema sicurezza, nonché comportamenti ad esso contrari;
- a tutto il personale di osservare le misure e le procedure di sicurezza adottate dalla Società, collaborando in tal modo ad un'effettiva prevenzione dei rischi.

Ogni comportamento contrario al sistema di gestione della sicurezza della Società dovrà essere adeguatamente sanzionato, da parte della stessa, a seguito di un regolare procedimento disciplinare.

## *E.2.7. Comportamenti da tenere nell'ambito delle attività "sensibili" rispetto ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio*

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività "sensibili" rispetto ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché di autoriciclaggio di cui all'art. 25-octies del D.Lgs. 231/2001.

In via generale, la Società richiede ai Destinatari il rispetto delle seguenti regole comportamentali:

- utilizzo nelle transazioni del sistema bancario;
- accertamento, attraverso le informazioni disponibili, della rispettabilità dei fornitori e di eventuali ulteriori terze parti prima di avviare con esse relazioni d'affari.

Occorre, inoltre, tenere conto del fatto che la Società ha ritenuto di sottoporsi agli obblighi in materia di antiriciclaggio previsti dal D.Lgs. 231/2007 (*"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"*), modificato dal D.Lgs 90/2017 (*Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006*), nonché, da ultimo, dal D.Lgs 125/2019 (*Modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della direttiva (UE) 2015/849, nonché attuazione della direttiva (UE) 2018/843 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE*). A tal fine sono imposti alla Società i seguenti ulteriori obblighi:

- adeguata verifica della clientela che consiste nei seguenti adempimenti:
  - o identificare il cliente e verificarne l'identità;
  - o identificare l'eventuale titolare effettivo e verificarne l'identità;
  - o svolgere un controllo costante nel corso della prestazione professionale;
- registrazione nell'Archivio Unico Informatico (A.U.I.) di una serie determinata di informazioni;
- conservazione per un periodo di 10 anni dalla cessazione della prestazione professionale delle informazioni registrate nell'A.U.I. e di copia dei documenti utilizzati per assolvere gli obblighi di adeguata verifica della clientela;
- segnalazione alla Unità di Informazione Finanziaria (U.I.F.) di un'operazione sospetta;
- comunicazione al Ministero dell'Economia e delle Finanze delle infrazioni, di cui si abbia notizia, alle disposizioni antiriciclaggio riguardanti le limitazioni all'uso del contante e dei titoli al portatore.

DRA ha, altresì, deciso di definire e formalmente adottare le proprie *"Politiche per la gestione del rischio di riciclaggio e finanziamento del terrorismo"*, attraverso le quali la Società si è dotata di

un assetto organizzativo e di controllo in grado di garantire l'applicazione delle norme di legge e dei regolamenti in materia di prevenzione e contrasto del riciclaggio e del terrorismo.

In particolare, la Società ha provveduto a nominare il **Responsabile della Funzione Antiriciclaggio**, al quale competono funzioni da esercitarsi trasversalmente su tutta l'operatività svolta dalla Società, qualificabili sia in termini di verifica della funzionalità di procedure, strutture e sistemi, sia di supporto e consulenza sulle scelte gestionali.

È, dunque, fatto obbligo ai Destinatari, che intervengono nella gestione degli adempimenti sopra descritti, di rispettare e attuare la normativa in materia di antiriciclaggio applicata dalla Società, svolgendo con diligenza i compiti loro assegnati in tale ambito e avendo cura di applicare, correttamente e nei limiti delle proprie attribuzioni, tutte le procedure aziendali all'uopo predisposte.

Inoltre, ai Destinatari, nello svolgimento dei propri compiti aziendali, è fatto espresso divieto di:

- trasferire a qualsiasi titolo tra soggetti diversi, se non per il tramite di banche o istituti di moneta elettronica o Poste Italiane S.p.A., denaro contante o libretti di deposito bancari o postali al portatore o titoli al portatore in euro o in valuta estera, quando il valore dell'operazione, anche frazionata, sia complessivamente pari o superiore al valore previsto dalla vigente normativa;
- emettere assegni bancari e postali senza clausola di non trasferibilità *(i)* per importi superiori a quelli previsti dalla normativa vigente e *(ii)* che non rechino l'indicazione del nome o della ragione sociale del beneficiario;
- girare per l'incasso assegni bancari e postali emessi all'ordine del traente a soggetti diversi da banche o Poste Italiane S.p.A.;
- effettuare versamenti su conti correnti cifrati o presso Istituti di credito privi di insediamenti fisici;
- effettuare pagamenti su conti correnti di banche operanti in Paesi ricompresi nelle liste "tax heaven" e in favore di società "off-shore";
- occultare i proventi derivanti da eventuali reati commessi nel presunto interesse o vantaggio della Società. Sono, pertanto, da intendersi vietate tutte le condotte atte a impiegare, sostituire, trasferire o, comunque, occultare somme di denaro di cui si conosca o si sospetti la provenienza illecita.

Inoltre, al fine di prevenire il reato di autoriciclaggio, ai Destinatari è richiesto di:

- custodire in modo corretto ed ordinato le scritture contabili e gli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali, approntando difese fisiche e/o informatiche che impediscano eventuali atti di distruzione e/o occultamento;
- in tutte le dichiarazioni di natura contabile/fiscale, garantire la veridicità e la completezza dei dati esposti;
- rispettare le disposizioni normative in materia contabile e fiscale, compresi i termini previsti dalla normativa applicabile per la presentazione delle dichiarazioni contabili/fiscali e il successivo versamento delle imposte da esse risultanti;

- coordinarsi con gli outsourcer coinvolti nella redazione delle suddette scritture e per i sistemi di archiviazione ottica.

## *E.2.8. Comportamenti da tenere nell'ambito delle attività "sensibili" rispetto ai delitti in materia di violazione del diritto d'autore*

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nell'uso del sistema informativo aziendale e nell'utilizzo di *software* e di banche dati tutelati dal diritto d'autore.

In via generale, ai Destinatari è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste dall'art. 25 novies del Decreto.

In particolare, coerentemente con i principi di cui al presente Modello e al Codice Etico adottato dalla Società, a tali soggetti è richiesto di:

- assicurare il rispetto delle norme interne, comunitarie e internazionali applicabili, poste a tutela della proprietà intellettuale e promuovere il corretto uso di tutte le opere dell'ingegno, compresi i programmi per elaboratore e le banche di dati.

È fatto espresso divieto ai Destinatari, di:

- realizzare condotte finalizzate, in generale, alla duplicazione di programmi per elaboratore protetti dal diritto d'autore o di banche di dati sulla memoria fissa del computer;
- installare programmi per elaboratore senza aver preventivamente informato il servizio IT preposto alla gestione della sicurezza informatica.

## *E.2.9. Comportamenti da tenere nell'ambito delle attività "sensibili" rispetto al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti in rapporti con soggetti che, nell'ambito del processo penale, possono avvalersi della facoltà di non rispondere.

In via generale, ai Destinatari è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste dall'art. 25-decies del Decreto.

In particolare, coerentemente con i principi di cui al presente Modello e al Codice Etico adottato dalla Società, a tali soggetti è richiesto di:

- evadere con tempestività, correttezza e buona fede tutte le richieste provenienti dagli organi di polizia giudiziaria e dall'autorità giudiziaria inquirente e giudicante, fornendo tutte le informazioni, i dati e le notizie eventualmente utili;
- mantenere, nei confronti degli organi di polizia giudiziaria e dell'autorità giudiziaria un comportamento disponibile e collaborativo in qualsiasi situazione.

È fatto espresso divieto ai Destinatari, di ricorrere alla forza fisica, a minacce o all'intimidazione

oppure promettere, offrire o concedere un'indebita utilità per indurre colui il quale può avvalersi della facoltà di non rispondere nel procedimento penale, a non rendere dichiarazioni o a rendere false dichiarazioni all'Autorità giudiziaria, con l'intento di ottenere una pronuncia favorevole alla Società o determinare il conseguimento di altro genere di vantaggio.

È, in particolare, vietato:

- intrattenere rapporti con persone sottoposte alle indagini preliminari e imputati nel processo penale al fine di turbare la loro libertà di autodeterminazione;
- riconoscere forme di liberalità o altre utilità a dipendenti o terzi che siano persone sottoposte alle indagini preliminari e imputati nel processo penale per indurli a omettere dichiarazioni o a falsare le stesse, in favore di DRA;
- riconoscere progressioni in carriera, scatti retributivi o incentivi premianti a dipendenti o collaboratori che non trovino adeguata corrispondenza nei piani di sviluppo delle risorse umane aziendali, nelle politiche remunerative e di incentivazioni aziendali o che comunque non rispondano a ragioni obiettive che giustifichino l'assunzione di dette iniziative.

#### *E.2.10. Comportamenti da tenere nell'ambito delle attività "sensibili" rispetto ai reati ambientali.*

A seguito dell'analisi condotta, non sono emerse attività di *core-business* sensibili alla potenziale commissione dei reati ambientali di cui all'art. 25-*undecies* del Decreto (associato in via prudenziale).

Occorre, tuttavia, considerare che Deloitte Risk Advisory S.r.l., anche attraverso la devoluzione tramite accordi di outsourcing stipulati con altre società del DCM Network, cura l'attuazione e il controllo degli adempimenti connessi alla verifica delle autorizzazioni dei fornitori di servizi in materia ambientale.

Limitatamente a tale attività, è pertanto richiesto ai Destinatari di:

- verificare, anche attraverso la predisposizione di apposite clausole contrattuali, che i fornitori di servizi connessi alla gestione dei rifiuti, ove richiesto dal D.Lgs. 152/2006 e dalle ulteriori fonti normative e regolamentari, diano evidenza, in base alla natura del servizio prestato, del rispetto della disciplina in materia di gestione dei rifiuti e di tutela dell'ambiente;
- accertare, prima dell'instaurazione del rapporto, la rispettabilità e l'affidabilità dei fornitori di servizi connessi alla gestione dei rifiuti;
- gestire i rapporti con i funzionari degli Enti della Pubblica Amministrazione preposti al controllo della normativa ambientale (es. ARPA, Polizia Municipale), secondo il sistema di deleghe e procure.

#### *E.2.11. Comportamenti da tenere nell'ambito delle attività "sensibili" rispetto ai reati inerenti stranieri irregolari*



Le seguenti regole si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività “sensibili” rispetto ai reati inerenti stranieri irregolari di cui all’art. 25-*duodecies* del D.Lgs. 231/2001.

In particolare, è fatto espresso divieto ai Destinatari di impiegare personale extracomunitario che non sia in regola con i requisiti richiesti dalla legge per soggiornare e svolgere attività lavorativa all'interno del territorio nazionale.

Qualora si debba procedere all’instaurazione di un rapporto di lavoro subordinato con un cittadino extracomunitario già soggiornante in Italia, è necessario che:

- il lavoratore sia munito del permesso di soggiorno europeo per soggiornanti di lungo periodo o del permesso di soggiorno che abiliti al lavoro;
- il contratto di lavoro sia comunicato agli enti pubblici competenti (Centro unico per l’impiego, INAIL e INPS).

La cessazione del rapporto di lavoro o altre variazioni dello stesso (i.e. instaurazione di nuovi rapporti di lavoro, trasferimento di sede) deve essere comunicata agli enti pubblici competenti (e.g. Sportello Unico per l’Immigrazione e Centro per l’impiego).

#### *E.2.12. Comportamenti da tenere nell’ambito delle attività “sensibili” rispetto ai reati tributari introdotti dalla legge 157/2019*

Le seguenti regole comportamentali si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività “sensibili” rispetto ai reati tributari di cui all’art. 25-*quinquiesdecies* del D.Lgs. 231/2001.

In particolare, ai Destinatari è richiesto di:

- rispettare e applicare tutte le norme tributarie vigenti, eseguendo gli adempimenti fiscali nei termini e con le modalità prescritti dalla normativa applicabile o dall’Autorità fiscale, al fine di garantire la piena *compliance* alla disciplina di settore, anche avvalendosi di consulenti esterni di comprovata competenza e professionalità;
- rappresentare gli atti, i fatti e i negozi intrapresi in modo da rendere applicabili forme di imposizione fiscale conformi alla reale sostanza economica delle operazioni;
- in tutte le dichiarazioni di natura contabile/fiscale, garantire la veridicità e la completezza dei dati esposti;
- rispettare le disposizioni normative in materia contabile e fiscale, compresi i termini previsti dalla legislazione applicabile per la presentazione delle dichiarazioni contabili/fiscali e il successivo versamento delle imposte da esse risultanti;
- rispettare i termini previsti dalla normativa applicabile per il versamento delle ritenute dovute sulla base della dichiarazione annuale di sostituto d’imposta;
- garantire trasparenza nei rapporti con fornitori e consulenti nonché un periodico controllo sull’effettività delle prestazioni rispetto alle fatture emesse;
- garantire la corretta archiviazione delle scritture contabili obbligatorie e dei documenti di cui è necessaria la conservazione;

- collaborare in modo trasparente con le Autorità fiscali, fornendo ad esse, ove necessario per lo svolgimento di verifiche o l'attività di riscossione, tutte le informazioni richieste, in modo veritiero e completo.

Inoltre, è fatto divieto di:

- indicare nelle dichiarazioni fiscali elementi passivi fittizi avvalendosi di fatture o altri documenti per operazioni inesistenti, quando tali fatture o documenti siano registrati nelle scritture contabili obbligatorie o siano detenuti a fine di prova nei confronti dell'Amministrazione finanziaria;
- indicare nelle dichiarazioni fiscali elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi (e.g., costi fittiziamente sostenuti e/o ricavi indicati in misura inferiore a quella reale), facendo leva su una falsa rappresentazione nelle scritture contabili obbligatorie e avvalendosi di mezzi idonei ad ostacolarne l'accertamento;
- porre in essere attività e/o operazioni volte a creare disponibilità extracontabili (e.g., ricorrendo a fatture per operazioni inesistenti o alla sovra fatturazione), ovvero volte a creare fondi extracontabili o "contabilità parallele".

## F. Organismo di Vigilanza

L'art. 6 comma 1 del D.Lgs. 231/2001 richiede, quale condizione per beneficiare dell'esimente dalla responsabilità amministrativa, che il compito di vigilare sull'osservanza e funzionamento del Modello, curandone il relativo aggiornamento, sia affidato ad un Organismo di Vigilanza ("OdV") interno all'ente che, dotato di autonomi poteri di iniziativa e di controllo, eserciti in via continuativa i compiti ad esso affidati.

Il Decreto richiede che l'Organismo di Vigilanza svolga le sue funzioni al di fuori dei processi operativi della Società, riferendo periodicamente al Consiglio di Amministrazione, svincolato da ogni rapporto gerarchico con il Consiglio stesso e con i singoli responsabili delle funzioni/direzioni aziendali.

In ossequio alle prescrizioni del D.Lgs. 231/2001, la Società ha ritenuto di istituire un organo a composizione collegiale, che possa assicurare la conoscenza delle attività aziendali, ed - al tempo stesso - abbia autorevolezza e indipendenza tali da garantire la credibilità delle funzioni dallo stesso svolte.

In particolare, la composizione dell'Organismo di Vigilanza è stata definita in modo da garantire i seguenti requisiti:

- **Autonomia e indipendenza**

I requisiti di autonomia e indipendenza mirano ad assicurare che l'OdV non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo e, soprattutto, la possibilità di svolgere il proprio ruolo senza condizionamenti diretti o indiretti da parte dei soggetti controllati. Detti requisiti sono garantiti dalla composizione collegiale e dall'attività di *reporting* direttamente al Consiglio di Amministrazione, senza vincolo di subordinazione gerarchica rispetto a detto organo.

- **Professionalità**

L'OdV deve possedere competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. In particolare, la composizione prescelta garantisce idonee conoscenze giuridiche e dei principi e delle tecniche di controllo e monitoraggio.

- **Continuità d'azione**

L'Organismo di Vigilanza è tenuto a vigilare costantemente, attraverso poteri di indagine, sul rispetto del Modello da parte dei Destinatari, a curarne l'attuazione e l'aggiornamento, rappresentando un riferimento costante per tutto il personale di Deloitte Risk Advisory S.r.l..

Inoltre, al fine di assicurarne la continuità di azione, l'OdV si avvale, ove necessario, del supporto della funzione "*Internal Audit*", che potrà svolgere per conto dell'Organismo di Vigilanza, relativamente alle aree che rientrano nella competenza istituzionale di detto ufficio, attività di monitoraggio e verifica in attuazione dei periodici piani di attività elaborati dall'OdV.

All'uopo, la funzione *Internal Audit* elabora dettagliati *report* che trasmette all'Organismo di Vigilanza al fine di fornirgli le informazioni di cui lo stesso necessita per l'espletamento del suo incarico.

Ove ritenuto necessario o opportuno dall'OdV, rappresentanti della funzione *Internal Audit* possono partecipare alle riunioni dell'Organismo di Vigilanza con funzioni consultive.

Infine, oltre che dalla Funzione *Internal Audit* per l'attività di monitoraggio, per specifiche attività, l'Organismo di Vigilanza può farsi assistere da professionisti esperti nella specifica materia.

## **F.1 Durata in carica, decadenza e revoca**

I componenti dell'Organismo di Vigilanza sono scelti tra soggetti in possesso di un profilo etico e professionale di indiscutibile valore e non debbono essere in rapporti di coniugio o parentela entro il quarto grado con i componenti del Consiglio di Amministrazione.

L'Organismo di Vigilanza resta in carica per il periodo determinato dal Consiglio di Amministrazione nella delibera consiliare di nomina dell'OdV.

In ogni caso, i membri dell'Organismo di Vigilanza rimangono in carica oltre la scadenza fissata nella delibera consiliare di relativa nomina fino a quando il Consiglio di Amministrazione non abbia provveduto con specifica delibera consiliare alla nomina dell'Organismo di Vigilanza nella nuova composizione o abbia confermato quella precedente. In ogni caso il periodo di "*prorogatio*" non potrà risultare superiore ai sei mesi.

Possono essere nominati componenti dell'Organismo di Vigilanza dipendenti della Società e professionisti esterni. Detti ultimi non debbono avere con la Società rapporti tali da integrare ipotesi di conflitto di interessi e da pregiudicarne l'indipendenza.

I compensi dei componenti dell'Organismo di Vigilanza, sia interni che esterni alla Società, non costituiscono ipotesi di conflitto di interessi.

Non può essere nominato componente dell'Organismo di Vigilanza, e, se nominato decade, l'interdetto, l'inabilitato, il fallito o chi è stato condannato, ancorché con condanna non definitiva, ad una pena che importi l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità di esercitare uffici direttivi, ovvero sia stato condannato, anche con sentenza non definitiva o con

sentenza di applicazione della pena su richiesta delle parti ex art. 444 c.p.p. (c.d. sentenza di patteggiamento), per aver commesso uno dei reati previsti dal D.Lgs. 231/2001.

I componenti che abbiano un rapporto di lavoro subordinato con la Società o che siano professionisti delle società italiane del DCM Network decadono automaticamente dall'incarico, in caso di cessazione di detti rapporti e indipendentemente dalla causa di interruzione degli stessi.

Analogamente, il professionista individuato quale componente dell'Organismo di Vigilanza che si trovi ad interrompere i rapporti con la Società, indipendentemente dalla causa di interruzione occorsa, decade automaticamente dall'incarico nelle ipotesi di conflitto di interesse o incompatibilità tali da pregiudicarne l'indipendenza.

Il Consiglio di Amministrazione può revocare, con delibera consiliare, il componente dell'OdV in ogni momento ma solo per giusta causa. Costituiscono giusta causa di revoca:

- l'omessa comunicazione al Consiglio di Amministrazione di un conflitto di interessi che impedisca il mantenimento del ruolo di componente dell'Organismo di Vigilanza stesso;
- la violazione degli obblighi di riservatezza in ordine alle notizie e informazioni acquisite nell'esercizio delle funzioni proprie dell'Organismo di Vigilanza;
- per i componenti legati alla Società da un rapporto di lavoro subordinato, la conclusione di un procedimento disciplinare da cui sia derivata l'applicazione della sanzione del licenziamento.

Qualora la revoca avvenga senza giusta causa, il componente revocato potrà chiedere di essere immediatamente reintegrato in carica.

Costituisce, invece, causa di decadenza dell'intero Organismo di Vigilanza:

- l'accertamento di un grave inadempimento da parte dell'Organismo di Vigilanza nello svolgimento dei propri compiti di verifica e controllo;
- la sentenza di condanna della Società, anche non divenuta irrevocabile, ovvero una sentenza di applicazione della pena su richiesta delle parti ex art. 444 c.p.p. (c.d. sentenza di patteggiamento), ove risulti dagli atti l'omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Ciascun componente può recedere in ogni momento dall'incarico con preavviso scritto di almeno 30 giorni, da comunicarsi al Consiglio di Amministrazione a mezzo pec.

L'Organismo di Vigilanza provvede a disciplinare in autonomia le regole per il proprio funzionamento in un apposito Regolamento, in particolare definendo le modalità operative per l'espletamento delle funzioni ad esso rimesse. Il Regolamento è successivamente trasmesso al Consiglio di Amministrazione per la relativa presa d'atto.

## **F.2 Funzioni e poteri dell'Organismo di Vigilanza**

L'Organismo di Vigilanza è chiamato ad assolvere i seguenti compiti:

- vigilare sulla diffusione all'interno della Società della conoscenza, della comprensione e dell'osservanza del Modello;

- vigilare sull'osservanza del Modello da parte dei Destinatari nell'ambito delle aree di attività a rischio di reato;
- vigilare sulla validità e adeguatezza del Modello, con particolare riferimento all'effettiva capacità del Modello di prevenire la commissione dei reati previsti dal Decreto;
- segnalare alla Società l'opportunità di aggiornare il Modello, laddove si riscontrino esigenze di adeguamento in relazione a mutate condizioni aziendali e/o normative. La responsabilità ultima dell'adozione delle modifiche da apportare al Modello è in ogni caso del Consiglio di Amministrazione.

Nello svolgimento di dette attività, l'OdV provvede ai seguenti adempimenti:

- verifica l'adeguatezza delle soluzioni organizzative adottate per l'attuazione e l'implementazione del Modello, avvalendosi delle funzioni/direzioni aziendali competenti;
- verifica l'esistenza di idonee iniziative per la diffusione della conoscenza e della comprensione dei principi del Modello;
- definisce e aggiorna la lista di informazioni ("**Flussi informativi**") che devono essere periodicamente messe a sua disposizione;
- definisce le modalità di raccolta e gestione dei Flussi informativi; a tal fine, l'OdV si coordina con le funzioni/direzioni aziendali coinvolte per un efficace e costante monitoraggio delle attività a "rischio-reato";
- raccoglie, elabora e conserva le informazioni rilevanti in ordine al rispetto del Modello;
- effettua verifiche periodiche nell'ambito delle aree di attività sensibili;
- verifica l'istituzione e il funzionamento di uno specifico canale informativo "dedicato" (i.e. indirizzo di posta elettronica), nonché di un canale alternativo (i.e. un indirizzo postale per le segnalazioni cartacee), diretti a facilitare il flusso di segnalazioni e informazioni verso l'Organismo di Vigilanza (come definiti al capitolo F.4);
- conduce indagini interne per l'accertamento di presunte violazioni delle prescrizioni del Modello.

Ai fini dello svolgimento degli adempimenti sopra elencati, l'Organismo di Vigilanza è dotato dei seguenti poteri:

- emanare disposizioni e comunicazioni volte a regolare le proprie attività e predisporre e aggiornare l'elenco dei Flussi informativi;
- accedere, senza autorizzazioni preventive, a ogni documento aziendale rilevante per lo svolgimento delle funzioni allo stesso attribuite dal D.Lgs. 231/2001;
- disporre che i responsabili delle funzioni/direzioni aziendali, e in ogni caso tutti i Destinatari, forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso;
- ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo di propria competenza.

Per un miglior svolgimento delle proprie attività, l'Organismo di Vigilanza può delegare uno o più compiti specifici a singoli suoi componenti, che li svolgeranno in nome e per conto dell'OdV stesso. In merito ai compiti delegati, la responsabilità da essi derivante ricade sull'Organismo di

Vigilanza nel suo complesso.

Il Consiglio di Amministrazione della Società assegna all'Organismo di Vigilanza un *budget* di spesa annuale nell'importo proposto dall'OdV stesso e, in ogni caso, adeguato rispetto alle funzioni ad esso rimesse.

L'Organismo di Vigilanza delibera in autonomia le spese da sostenere, nel rispetto dei poteri di firma aziendali, e, in caso di spese eccedenti il *budget*, viene autorizzato direttamente dal Consiglio di Amministrazione.

### **F.3 Reporting dell'Organismo di Vigilanza**

Come sopra già anticipato, al fine di garantire la piena autonomia e indipendenza nello svolgimento delle relative funzioni, l'Organismo di Vigilanza comunica direttamente al Consiglio di Amministrazione della Società.

L'Organismo di Vigilanza può essere convocato in qualsiasi momento dal Consiglio di Amministrazione e, a sua volta, può richiedere di essere sentito qualora ravvisi l'opportunità di riferire su questioni inerenti il funzionamento e l'efficace attuazione del Modello o in relazione a situazioni specifiche.

Segnatamente, l'Organismo di Vigilanza riferisce circa lo stato di attuazione del Modello e gli esiti dell'attività di vigilanza svolta nelle seguenti modalità:

- periodicamente con l'Amministratore Delegato;
- con cadenza annuale nei confronti del Consiglio di Amministrazione, attraverso una relazione scritta, nella quale vengano illustrate le attività di monitoraggio svolte dall'Organismo stesso, le criticità emerse e gli eventuali interventi correttivi o migliorativi opportuni per l'implementazione del Modello;
- occasionalmente nei confronti del Collegio Sindacale, ove ne ravvisi la necessità, anche in relazione a presunte violazioni poste in essere dai vertici aziendali o dai componenti del Consiglio di Amministrazione, potendo ricevere dal Collegio Sindacale richieste di informazioni o di chiarimenti in merito alle suddette presunte violazioni.

Come già anticipato, il D.Lgs. 231/2001 enuncia, tra le esigenze che il Modello deve soddisfare, l'istituzione di specifici obblighi informativi nei confronti dell'Organismo di Vigilanza da parte dei Destinatari, per consentire all'Organismo di Vigilanza stesso lo svolgimento delle proprie attività di vigilanza e di verifica.

A tale proposito devono essere comunicate all'Organismo di Vigilanza le seguenti informazioni:

- su base periodica i Flussi informativi, ovvero informazioni, dati, notizie e documenti previamente identificati dall'Organismo di Vigilanza e da quest'ultimo formalmente richiesti ai singoli responsabile delle funzioni/direzioni aziendali, secondo le tempistiche definite dall'OdV medesimo;
- nell'ambito delle attività di verifica dell'Organismo di Vigilanza, ogni informazione, dato, notizia e documento ritenuto utile e/o necessario per lo svolgimento di dette verifiche, previamente identificati dall'OdV e formalmente richiesti ai singoli responsabili delle funzioni/direzioni aziendali.

Devono essere altresì obbligatoriamente trasmesse all'Organismo di Vigilanza le informative concernenti:

- i provvedimenti e/o le notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, anche amministrativa, che vedano il coinvolgimento della Società e dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto, fatti salvi gli obblighi di riservatezza e segretezza legalmente imposti;
- le richieste di assistenza legale inoltrate da Soci, dirigenti e/o dipendenti della Società in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;
- le modifiche nel sistema delle deleghe e delle procure, le modifiche statutarie o dell'organigramma aziendale;
- i rapporti preparati dai responsabili delle funzioni/direzioni aziendali nell'ambito della loro attività di controllo e dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto;
- le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello, con evidenza degli eventuali procedimenti disciplinari svolti e delle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i dipendenti), ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- l'avvenuta segnalazione di operazioni sospette ai sensi della normativa antiriciclaggio;
- la segnalazione di violazioni delle regole comportamentali relative alla limitazione all'uso del contante e dei valori al portatore;
- la segnalazione di infortuni gravi (qualsiasi infortunio con prognosi iniziale di 40 giorni e, in ogni caso, la cui durata sia superiore ai 40 giorni) occorsi a dipendenti, collaboratori della Società, e più genericamente a tutti coloro che abbiano accesso alle strutture della Società.

In relazione alle modalità di trasmissione delle informazioni di cui al presente paragrafo l'Organismo ha istituito un indirizzo di posta elettronica (odvra@deloitte.it), reso noto al personale aziendale e il cui accesso è riservato ai soli componenti dell'Organismo. Tale canale di comunicazione potrà altresì essere utilizzato in caso di dubbi sulla corretta interpretazione delle previsioni contenute nel presente Modello o qualsiasi altro chiarimento inerente l'applicazione del sistema implementato dalla Società ai sensi del D.Lgs. 231/2001.

Tutte le informazioni e la documentazione raccolta dall'Organismo di Vigilanza – e allo stesso pervenuta – nell'espletamento dei propri compiti istituzionali, deve essere custodita a cura dell'OdV in un apposito archivio e conservata in conformità con le disposizioni di legge applicabili.

L'omesso invio all'Organismo di Vigilanza delle informazioni di cui al presente paragrafo integra violazione del Modello (cfr. cap. G).

## **F.4 Disciplina del *whistleblowing*: gestione delle segnalazioni**

La legge n. 179, 30 novembre 2017, recante “*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*” ha introdotto il sistema del c.d. “*Whistleblowing*”, volto alla tutela del dipendente o collaboratore che segnali illeciti.

In particolare, il provvedimento ha modificato l'articolo 6 del D.Lgs. 231/2001 stabilendo che i Modelli adottati dagli enti debbano ora prevedere:

- a) *“uno o più canali che consentano ai soggetti di cui all'art. 5 (apicali o sottoposti alla direzione e alla vigilanza degli apicali) di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;*
- b) *almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;*
- c) *il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;*
- d) *nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.”*

Alla luce di quanto sopra, i Destinatari devono pertanto riferire all'Organismo di Vigilanza, a tutela dell'integrità della Società, ogni informazione relativa a comportamenti che possano integrare una violazione delle prescrizioni del Decreto e/o del Modello, nonché specifiche fattispecie di reato, sulla base di elementi di fatto precisi e concordanti, di cui siano venuti a conoscenza nello svolgimento delle proprie mansioni (“**Segnalazioni**”).

A tal fine la Società ha istituito canali dedicati di comunicazione consistenti, come già anticipato al precedente paragrafo, in un indirizzo di posta elettronica, (odvra@deloitte.it), nonché nell'indirizzo postale della sede sociale per segnalazioni cartacee (via Tortona, 25 – 20144 Milano), resi noti al personale aziendale, ai quali potranno essere inviate le eventuali segnalazioni e il cui accesso/ricezione è riservato ai soli componenti dell'Organismo di Vigilanza.

Tali modalità di trasmissione delle segnalazioni garantiscono la massima riservatezza dell'identità dei segnalanti nelle attività di gestione della segnalazione, anche al fine di evitare atteggiamenti ritorsivi o qualsiasi altra forma di discriminazione o penalizzazione nei loro confronti.

La Società adotta tutte le misure idonee a tutelare la riservatezza dell'identità del segnalante.

L'Organismo di Vigilanza valuterà le segnalazioni pervenutegli, anche in forma anonima, e potrà convocare, qualora lo ritenga opportuno, sia il segnalante, ove conosciuto, per ottenere maggiori informazioni, che il presunto autore della violazione, dando inoltre luogo a tutti gli accertamenti e le indagini che siano necessarie per appurare la fondatezza della segnalazione.

Accertata la fondatezza della segnalazione, l'Organismo di Vigilanza:

- per le violazioni poste in essere dal personale dipendente, ne dà immediata comunicazione per iscritto alla funzione/direzione aziendale competente per la valutazione circa l'avvio delle conseguenti azioni disciplinari;



- per violazioni del Modello, ritenute fondate, da parte di figure apicali, ne dà immediata comunicazione al Consiglio di Amministrazione;
- per violazioni del Modello, ritenute fondate, da parte degli Amministratori della Società, ne dà immediata comunicazione al Consiglio di Amministrazione e al Collegio Sindacale.

Tutte le segnalazioni raccolte dall'Organismo di Vigilanza – e allo stesso pervenute – nell'espletamento dei propri compiti istituzionali, devono essere custodite a cura dell'Organismo in un apposito archivio e conservate in conformità con le disposizioni di legge applicabili.

La Società dispone inoltre di un ulteriore canale di segnalazione, denominato “*Deloitte SpeakUp*”<sup>4</sup>, trattasi di un sistema attraverso cui è possibile segnalare una condotta scorretta e fare domande su temi di etica. Il servizio è accessibile da tutti ed è disponibile sia via telefono (800-797076), sia mediante uno specifico portale online (disponibile sulla intranet aziendale) in cui inoltrare la segnalazione via mail.

## G. Il Sistema Sanzionatorio

Ai sensi del D. Lgs. 231/2001, il Modello, la cui adozione e attuazione costituisce condizione *sine qua non* per l'esenzione di responsabilità della Società in caso di commissione dei reati di cui al Decreto, può ritenersi efficacemente attuato solo se prevede un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure in esso indicate.

L'applicazione delle sanzioni disciplinari prescinde dall'avvio o dall'esito di un eventuale procedimento penale, in quanto le previsioni del Modello costituiscono regole vincolanti per i Destinatari, la violazione delle quali deve pertanto, al fine di ottemperare ai dettami del Decreto, essere sanzionata indipendentemente dall'effettiva realizzazione di un reato o dalla punibilità dello stesso.

Le sanzioni comminabili sono diversificate in ragione della natura del rapporto tra l'autore della violazione e la Società, nonché del rilievo e gravità della violazione commessa e del ruolo e responsabilità dell'autore.

In generale, le violazioni possono essere ricondotte ai seguenti comportamenti e classificate come segue:

- comportamenti che integrano una mancata attuazione colposa delle prescrizioni del Modello;
- comportamenti che integrano una trasgressione dolosa delle prescrizioni del Modello, tale da compromettere il rapporto di fiducia tra l'autore e la Società in quanto preordinata in modo univoco a commettere un reato.

Il procedimento sanzionatorio è in ogni caso rimesso agli organi societari competenti.

---

<sup>4</sup> Deloitte SpeakUp: il canale attraverso cui è possibile segnalare o formulare eventuali domande relative a condotte scorrette o richieste di chiarimento riguardanti l'applicazione di Policy, Linee Guida e Protocolli (selezionando la specifica sezione "Frode o Corruzione"). Il servizio risulta accessibile a tutti 24/24, 365 giorni l'anno, via telefono o via email. Tale canale è amministrato da una terza parte a garanzia di confidenzialità e anonimato del segnalante.

## **G.1 Sanzioni per i lavoratori dipendenti non dirigenti**

I comportamenti tenuti dai lavoratori dipendenti in violazione di regole comportamentali contenute nel presente Modello e nel Codice Etico sono definiti come illeciti disciplinari.

Le sanzioni eventualmente comminate a lavoratori dipendenti sono applicate nel rispetto delle procedure e delle garanzie previste dalla legge, con particolare riferimento alle previsioni contenute nell'art. 7 della Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori), ove applicabile, e dalle norme pattizie contenute nei contratti collettivi applicabili.

In particolare, il Modello fa riferimento alle categorie di fatti sanzionabili previste dalle norme pattizie di cui al contratto collettivo dei “*dipendenti da aziende del terziario, della distribuzione e dei servizi*”. Tali categorie descrivono i comportamenti sanzionabili a seconda del rilievo che assumono le singole fattispecie considerate, nonché le sanzioni in concreto previste per la commissione dei fatti stessi, a seconda della loro gravità.

Sono pertanto previste diverse sanzioni commisurate alla gravità della violazione commessa e ai soggetti che la pongono in essere, ovvero:

- biasimo inflitto verbalmente;
- biasimo inflitto per iscritto;
- multa in misura non eccedente l'importo di 4 ore della normale retribuzione;
- sospensione dalla retribuzione e dal servizio per un massimo di giorni 10;
- licenziamento disciplinare senza preavviso.

Al fine di evidenziare i criteri di correlazione tra le violazioni e i provvedimenti disciplinari si precisa che:

- i) incorre nel provvedimento disciplinare del biasimo inflitto verbalmente il dipendente che:
  - violi, per mera negligenza le prescrizioni del Codice Etico o adottati, nello svolgimento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni contenute nel Modello, qualora la violazione non abbia rilevanza esterna;
- ii) incorre nel provvedimento disciplinare del biasimo inflitto per iscritto il dipendente che:
  - risulti recidivo, durante il biennio, nella commissione di infrazioni per le quali è applicabile il biasimo inflitto verbalmente;
  - violi, per mera negligenza le prescrizioni del Codice Etico o adottati, nello svolgimento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni contenute nel Modello, qualora la violazione abbia rilevanza esterna;
- iii) incorre nel provvedimento disciplinare della multa in misura non eccedente l'importo di 4 ore della normale retribuzione il dipendente che:
  - risulti recidivo, durante il biennio, nella commissione di infrazioni per le quali è applicabile il biasimo inflitto per iscritto;
  - per il livello di responsabilità gerarchico o tecnico, o in presenza di circostanze

aggravanti, leda l'efficacia del Modello con comportamenti quali:

- l'inosservanza dell'obbligo di informativa all'Organismo di Vigilanza;
- la reiterata inosservanza degli adempimenti previsti dalle prescrizioni indicate nel Modello, nell'ipotesi in cui riguardano un procedimento o rapporto in cui è parte la Pubblica Amministrazione;
- l'effettuazione con colpa grave di false o infondate segnalazioni inerenti violazioni del Modello o del Codice Etico;
- la violazione delle misure adottate dalla Società volte a garantire la tutela della riservatezza dell'identità del segnalante.

iv) incorre nel provvedimento disciplinare della sospensione dalla retribuzione e dal servizio per un massimo di giorni 10 il dipendente che:

- risulti recidivo, durante il biennio, nella commissione di infrazioni per le quali è applicabile la multa in misura non eccedente l'importo di 4 ore della normale retribuzione;
- violi le disposizioni concernenti i poteri di firma e il sistema delle deleghe attribuite con riguardo ad atti e documenti rivolti alla Pubblica Amministrazione e alle Autorità di Vigilanza;
- effettui con dolo false o infondate segnalazioni inerenti violazioni del Modello o del Codice Etico;
- violi le misure adottate dalla Società volte a garantire la tutela della riservatezza dell'identità del segnalante in modo da generare atteggiamenti ritorsivi o qualsiasi altra forma di discriminazione o penalizzazione nei confronti del segnalante.

v) incorre nel provvedimento disciplinare del licenziamento senza preavviso il dipendente che:

- eluda fraudolentemente le prescrizioni del Modello attraverso un comportamento inequivocabilmente diretto alla commissione di uno dei reati ricompreso fra quelli previsti nel D.Lgs. 231/2001;
- violi il sistema di controllo interno attraverso la sottrazione, la distruzione o l'alterazione di documentazione ovvero impedendo il controllo o l'accesso alle informazioni e alla documentazione ai soggetti preposti, incluso l'Organismo di Vigilanza, in modo da impedire la trasparenza e verificabilità delle stesse;
- in ipotesi di recidiva, si renda responsabile con dolo o colpa grave delle infrazioni relative a false o infondate segnalazioni inerenti violazioni del Modello o del Codice Etico nonché a violazioni delle misure adottate dalla Società volte a garantire la tutela della riservatezza dell'identità del segnalante.

Il tipo e l'entità di ciascuna delle sanzioni sopra richiamate, sono altresì applicate, in relazione:

- all'intenzionalità del comportamento o al grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;

- al comportamento complessivo del lavoratore, con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- alle mansioni, ruolo, responsabilità e autonomia del lavoratore;
- alla posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- alle altre particolari circostanze che accompagnano la violazione disciplinare.

L'accertamento delle suddette infrazioni, l'instaurazione dei procedimenti disciplinari e l'irrogazione delle sanzioni competono alla funzione/direzione aziendale competente, secondo le modalità stabilite dal Consiglio di Amministrazione, con comunicazione all'Organismo di Vigilanza.

## **G.2 Misure nei confronti dei dirigenti**

In caso di violazione, da parte dei dirigenti, delle previsioni del presente Modello o del Codice Etico, o di tenuta, nell'espletamento di attività inerenti le aree a rischio, di comportamenti non conformi alle prescrizioni del Modello o del Codice Etico, si applicano nei confronti dei responsabili le sanzioni di cui alla contrattazione collettiva per le altre categorie di dipendenti, nel rispetto degli artt. 2106, 2118 e 2119 cod. civ., nonché dell'art. 7 della Legge 300/1970.

In via generale, al personale dirigente possono essere comminate le seguenti sanzioni:

- sospensione dal lavoro;
- risoluzione anticipata del rapporto di lavoro.

Nei casi di gravi violazioni, la Società potrà procedere alla risoluzione anticipata del contratto di lavoro senza preavviso ai sensi e per gli effetti dell'art. 2119 cod. civ.

La competenza ad assumere le misure più idonee sopra menzionate è rimessa all'Amministratore Delegato, ovvero, in caso di conflitto d'interessi o per i casi più gravi, al Consiglio di Amministrazione.

## **G.3 Misure nei confronti di collaboratori sottoposti a direzione e vigilanza**

I contratti stipulati con tali soggetti contengono una dichiarazione di conoscenza del Modello e del Codice Etico e l'impegno ad osservarne le relative prescrizioni; contengono, altresì, una specifica clausola di recesso e/o di risoluzione connessa all'inadempimento di tali obbligazioni, fermo restando il diritto della Società di rivalersi per gli eventuali danni subiti in conseguenza di dette condotte, ivi inclusi i danni causati dall'applicazione in capo a DRA delle sanzioni amministrative previste dal Decreto.

## **G.4 Misure nei confronti degli Amministratori**

In caso di violazione del Modello e del Codice Etico da parte di Amministratori della Società, l'Organismo di Vigilanza informa senza indugio il Collegio Sindacale e, laddove possibile, l'intero Consiglio di Amministrazione, che provvederanno ad assumere o promuovere l'applicazione delle misure sanzionatorie ritenute più opportune in relazione alla natura e gravità della violazione commessa (es. richiami scritti, sospensione o revoca delle procure, sospensione temporanea dalla carica, revoca dalla carica).

## **G.5 Misure nei confronti dei soggetti apicali**

La violazione dello specifico obbligo di vigilanza sui sottoposti gravante sugli apicali comporterà, da parte della Società, l'assunzione delle misure sanzionatorie ritenute più opportune in relazione sia alla natura e gravità della violazione commessa sia alla qualifica o ruolo ricoperto dall'apicale autore della violazione.

## **G.6 Misure nei confronti dei terzi**

La Società si riserva inoltre di valutare l'inserimento, negli accordi contrattuali sottoscritti con terze parti, di una clausola che impegni la controparte alla condivisione dei principi del Codice Etico e che preveda, in caso di eventuale violazione degli stessi, la facoltà per la Società di valutare l'eventuale inadempimento contrattuale, con ogni conseguenza di legge.

## **H. Informazione e formazione**

Le attività di informazione e formazione sui contenuti del Modello e del Codice Etico coinvolgono il Consiglio di Amministrazione e tutto il personale di DRA, risultando articolate come di seguito indicato:

- personale dipendente (professionale e non professionale) e con funzioni di rappresentanza della Società: informativa nella lettera di assunzione e formazione iniziale per i neoassunti; *e-learning* dedicato all'argomento con *test* di verifica; accesso agli spazi della *intranet* aziendale dedicati all'argomento; specifiche comunicazioni di aggiornamento;
- altri Destinatari: nota informativa sui principi di comportamento previsti dal Modello e dal Codice Etico.

## **H.1. Formazione del personale**

È obiettivo di DRA garantire una corretta divulgazione e conoscenza delle regole di condotta contenute nel Modello e nel Codice Etico nei confronti delle risorse già presenti in azienda e di quelle di nuova assunzione.

Il funzionamento del sistema di informazione e formazione è verificato dall'Organismo di Vigilanza, in collaborazione con il responsabile della funzione/direzione coinvolta.

- **La comunicazione iniziale**

Il Modello e le relative modifiche sono comunicate a tutte le risorse presenti in azienda al momento della loro adozione; a tal fine, la *intranet* aziendale contiene uno spazio dedicato all'argomento nel quale risiedono i documenti descrittivi del Modello.

Ai nuovi assunti viene data adeguata informativa circa il fatto che DRA ha adottato un proprio Modello e un proprio Codice Etico, il cui esame e la cui consultazione attraverso la *intranet* aziendale assicurano a ciascun dipendente la conoscibilità delle norme comportamentali considerate di primaria rilevanza.

- **La formazione**

L'attività di formazione, finalizzata a diffondere la conoscenza della normativa di cui al Decreto, nonché i contenuti del Modello e del Codice Etico di DRA, è differenziata nei contenuti e nelle modalità di erogazione in funzione della qualifica dei destinatari e del livello di rischio dell'area in cui operano, nonché del fatto che essi abbiano o meno funzioni di rappresentanza della Società.

## **H.2 Informativa ad altri Destinatari**

I collaboratori sottoposti alla direzione o vigilanza degli apicali della Società che sono coinvolti nello svolgimento di attività sensibili ai sensi del Decreto sono informati, per le parti di rispettivo interesse, del contenuto del Modello e del Codice Etico e dell'esigenza di DRA che il loro comportamento sia sempre ad esso conforme.

## **I. Adozione e aggiornamento del Modello**

L'art. 6, comma 1, lett. a) del Decreto richiede che il Modello sia un "atto di emanazione dell'organo dirigente". L'adozione dello stesso, così come la nomina dell'OdV, è dunque rimessa alla competenza del Consiglio di Amministrazione della Società, che provvede mediante delibera consiliare. Con l'adozione formale del Modello questo diviene regola imperativa per la Società e i Destinatari.

Le successive modifiche o integrazioni di carattere sostanziale, anche proposte dall'OdV (intendendosi per tali le modifiche delle regole e dei principi generali contenuti nel presente Modello), sono rimesse alla competenza del Consiglio di Amministrazione della Società. Per

l'adozione di modifiche non sostanziali, il Consiglio di Amministrazione delega l'Amministratore Delegato alla gestione della Società, che periodicamente riferisce al Consiglio di Amministrazione sulla natura delle modifiche apportate.

L'efficace e concreta attuazione del Modello adottato è garantita:

- dai soggetti apicali della Società;
- dall'OdV, nell'esercizio dei poteri di iniziativa e di controllo allo stesso conferiti sulle attività svolte dalla Società nelle aree a rischio.

In particolare, è responsabilità degli apicali della Società, in collaborazione con l'OdV, contribuire alla conoscenza e trasferire ai propri collaboratori la consapevolezza delle situazioni a rischio-reato, nonché impartire direttive circa le modalità operative di svolgimento dei compiti assegnati, in coerenza con i principi e le prescrizioni contenute nel Modello e nel Codice Etico e tenendo conto delle peculiarità del proprio ambito di attività.