

**GOIRC**

**Gruppo Oncologico Italiano di Ricerca Clinica**

**Modello Organizzativo ai sensi del D.lgs.231/01**

**MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO IN  
MATERIA DI RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI**

**GOIRC**

**Modello Organizzativo D.lgs 231/01**

**PARTE GENERALE**

**MODELLO 231**

**GOIRC**

**Gruppo Oncologico Italiano di Ricerca Clinica**

## **1. IL CONTESTO ORGANIZZATIVO**

### **1.1 GOIRC: cenni storici, natura giuridica e oggetto sociale.**

L'Associazione denominata "Gruppo Oncologico Italiano di Ricerca Clinica" di seguito anche "GOIRC" o "Gruppo" è stata costituita, in data 18 dicembre 1982.

La sede dell'Associazione è in Parma, alla via Gramsci 14.

In data 26/09/2023 il GOIRC è stato iscritto al n. 11 del Registro delle Persone giuridiche istituito presso l'UTG di Parma.

### **1.2 Assetto associativo e contesto organizzativo.**

#### **Finalità**

Il GOIRC non ha finalità di lucro e si propone di promuovere e svolgere attività scientifica di ricerca in campo oncologico: epidemiologico, traslazionale, clinico, e psicosociale.

A tal fine l'Associazione opera con le seguenti modalità:

1. promozione e conduzione di studi clinici in campo oncologico;
2. partecipazione a studi in collaborazione con altri gruppi o Enti pubblici o privati;
3. promozione di iniziative scientifiche (congressi, riunioni, conferenze, pubblicazioni, linee guida, etc.) didattiche (seminari, corsi, master, etc.) nell'ambito dell'oncologia, nonché approfondimento e perfezionamento della metodologia della ricerca clinica;
4. promozione e conduzione di ricerche sulla caratterizzazione biologica e su aspetti epidemiologici delle neoplasie;
5. istituzione di premi, borse di studio, *grant* di ricerca, e quant'altro utile ad implementare la ricerca clinica;
6. ogni altra attività utile alla promozione ed allo svolgimento dell'attività scientifica di ricerca in campo oncologico.

#### **Unità aderenti e soci**

L'Associazione è organizzata sulla base di unità aderenti e di soci.

Le unità aderenti ("Unità GOIRC") sono costituite da Unità di Oncologia Medica o da altre Unità che svolgano attività clinica e/o di ricerca in ambito oncologico, che partecipino alle attività del GOIRC e ne abbiano richiesto la qualifica tramite il loro direttore o responsabile della struttura.

I soci sono tutti i medici o le altre figure professionali che partecipino alle attività scientifica e associativa del GOIRC, ne abbiano fatta richiesta, e siano stati ammessi con delibera del Consiglio Direttivo.

#### **Struttura operativa**

In considerazione della tipologia degli studi condotti, che non richiede particolari strutture – ma essenzialmente l'idea originaria, una certa autorevolezza per poter favorire l'adesione dei Centri allo studio, e un'attività di coordinamento scientifico (la gestione di molti degli aspetti operativi è di solito demandata a C.R.O.) –, **la struttura operativa di GOIRC è limitata, i**

collaboratori e gli eventuali dipendenti usualmente operano presso i Centri diretti dai medici che aderiscono al Gruppo, molte attività sono esternalizzate presso lo studio professionale **che presta consulenza fiscale e gestisce la contabilità.**

Dal punto di vista fiscale GOIRC è un ente commerciale (l'attività fiscalmente commerciale non è prevalente e le maggiori entrate hanno forma di contributi).

### **Studi e ricerche condotte dal GOIRC**

L'attività tipica di GOIRC è quella di **progettare e realizzare studi clinici**, sovente **studi no-profit**.

La caratteristica di tali studi è l'assenza di ogni obiettivo di commercializzazione di farmaci o di risultati, in quanto l'unico scopo è quello di migliorare le strategie assistenziali.

Oltre all'Ente interessato a ideare e condurre la ricerca, vi sono:

- a) il **Promotore della sperimentazione** che è l'ente che ha ideato e conduce la ricerca;
- b) lo **Sperimentatore**, che è di solito il medico che ha l'idea della ricerca e ne disegna il protocollo; mantiene questo ruolo in forma ufficiale, venendo designato Sperimentatore principale (Principal Investigator);
- c) l'**azienda finanziatrice** che di solito, oltre ad una erogazione monetaria, mette gratuitamente a disposizione il proprio farmaco ai fini della ricerca;
- d) i **Centri partecipanti allo studio** che sono i reparti / dipartimenti di oncologia – per la maggior parte pubblici, ma talvolta anche afferenti ad enti privati – che hanno in cura i pazienti inseriti nello studio, e conseguentemente trattati dai Centri secondo il protocollo dello studio;
- e) i **fornitori di servizi esterni** che nel settore sono sovente le **C.R.O.** (*Organizzazioni di Ricerca a Contratto*), società di servizi o qualsiasi altro organismo con cui il promotore della sperimentazione ha stipulato un contratto o ha stipulato altra forma di accordo, per affidare alla stessa una parte o tutte le proprie competenze in tema di sperimentazione clinica (stesura del protocollo, selezione dei centri e degli sperimentatori, selezione e utilizzazione del monitor, elaborazione dei report, analisi statistica, preparazione della documentazione da sottoporre all'autorità regolatoria ecc.), come previsto dalle Norme di Buona Pratica Clinica (GCP), ferme restando le responsabilità del promotore della sperimentazione medesima connesse con la sperimentazione stessa.

Le modalità di proposta, discussione, accettazione, apertura e chiusura degli studi clinici promossi dal GOIRC, sono contenute in apposito Regolamento. L'adesione del GOIRC a studi promossi da terzi deve essere approvata dal Consiglio Direttivo.

### **Organi dell'associazione**

In virtù del suo Statuto, gli organi del GOIRC sono:

- a) l'Assemblea dei soci;
- b) il Comitato Scientifico;
- c) il Consiglio Direttivo;

- d) il Presidente;
- f) il Tesoriere;
- g) il Segretario.

## **L'assemblea**

L'Assemblea dei soci può essere ordinaria o straordinaria.

L'Assemblea ordinaria, che viene convocata almeno una volta all'anno, ha il compito di:

- nominare i componenti del Consiglio Direttivo, dopo averne stabilito il numero,
- approvare il bilancio consuntivo,
- ratificare i Regolamenti sottopostigli dal Consiglio Direttivo,
- deliberare sull'esclusione dei soci e delle Unità aderenti per gravi motivi,
- deliberare sulla responsabilità dei componenti degli organi sociali e promuovere azioni di responsabilità nei loro confronti,
- deliberare su altro argomento sottopostole nell'ordine del giorno, su iniziativa del Consiglio Direttivo o su domanda di almeno un quarto dei soci, o comunque attribuiti alla sua competenza dalla legge, dall'atto costitutivo o dallo statuto.

L'Assemblea straordinaria ha il compito di:

- deliberare sulle modifiche dell'atto costitutivo e dello statuto,
- deliberare sullo scioglimento dell'Associazione
- deliberare sulla devoluzione del patrimonio sociale.

L'Assemblea è presieduta dal Presidente dell'Associazione o in sua assenza dalla persona al momento designata dagli intervenuti.

## **Il comitato scientifico**

Il Consiglio Direttivo può istituire un Comitato Scientifico, con finalità consultive, costituito da tutti gli sperimentatori responsabili scientifici degli studi aperti aventi GOIRC quale promotore, nonché da medici e ricercatori di riconosciuto valore scientifico e dai rappresentanti di associazioni di pazienti individuati dal Consiglio Direttivo. Il Comitato Scientifico potrà identificare, di volta in volta o fino a revoca, uno dei suoi membri, che avrà diritto a partecipare, senza diritto di voto, alle riunioni del Consiglio Direttivo.

## **Il consiglio direttivo**

L'Associazione è retta da un Consiglio Direttivo (di seguito, anche: Organo Amministrativo”) i cui componenti sono eletti dall'Assemblea fra i candidati.

Tutti membri del Consiglio Direttivo sottoscrivono all'inizio di ogni mandato una dichiarazione per potenziali Conflitti di Interesse, che tenga conto dei tre anni precedenti alla data di sottoscrizione.

L'amministrazione dell'Associazione per tutti gli atti di ordinaria e straordinaria amministrazione intesi a conseguire le sue finalità è affidata al Consiglio Direttivo, cui spettano tutti i poteri e le funzioni che non siano espressamente riservate dalla legge, dall'atto costitutivo e/o dallo statuto ad altri organi.

Al Consiglio Direttivo spettano, fra gli altri, i compiti di:

- a) deliberare sulle questioni riguardanti l'attività dell'Associazione per l'attuazione delle sue finalità, assumendo tutte le iniziative del caso;
- b) predisporre il bilancio consuntivo;
- c) predisporre e approvare tutti Regolamenti sulla funzionalità del GOIRC, da sottoporre all'Assemblea per ratifica;
- d) attivare eventuali gruppi o comitati di lavoro nominando i relativi responsabili, scelti fra i soci, anche al di fuori dei membri del Consiglio Direttivo;
- e) nominare, fra i membri eletti, il Presidente, il Tesoriere, il Segretario;
- f) deliberare sulle domande di nuove adesioni presentate dalle richiedenti Unità o soci;
- g) deliberare sulla revoca di Unità aderenti o soci, nei casi ove non già previsto che debba provvedervi l'assemblea;
- h) stabilire l'importo dell'eventuale quota annuale dei soci.

Il Consiglio Direttivo si riunisce almeno tre volte all'anno in forma ordinaria e possono essere indette ulteriori riunioni convocate dal Presidente ogniqualvolta lo ritenga necessario o ne faccia richiesta la maggioranza dei suoi membri.

Su invito del Presidente possono partecipare alle riunioni anche altre persone esterne al Consiglio, senza diritto di voto, oltre all'eventuale rappresentante del Comitato Scientifico.

La riunione è presieduta dal Presidente dell'Associazione, o, in caso di sua assenza, dal consigliere al momento designato dagli intervenuti.

#### **Presidente, tesoriere, segretario**

Il Presidente è nominato dal Consiglio Direttivo fra i suoi membri, dura in carica sino alla scadenza del mandato del Consiglio che lo ha nominato, e non è rieleggibile per più di due mandati consecutivi.

Il Presidente rappresenta legalmente il GOIRC di fronte a terzi o in giudizio.

Il Tesoriere è scelto dal Consiglio Direttivo tra suoi membri, dura in carica sino alla scadenza del mandato del Consiglio che lo ha nominato, è responsabile della conduzione degli aspetti amministrativi e finanziari del Gruppo, e può avvalersi della cooperazione di un esperto esterno.

Il Segretario è scelto dal Consiglio Direttivo fra i suoi membri, dura in carica sino alla scadenza del mandato del Consiglio che lo ha nominato, e può avvalersi della cooperazione di un esperto esterno.

In caso di temporanea indisponibilità del Presidente il Segretario ne assume le funzioni.

E' prevista l'assoluta gratuità delle cariche associative e pertanto ai membri del Consiglio Direttivo e del Comitato Scientifico, così come al Presidente, al Tesoriere ed al Segretario, non spetta alcun compenso per l'opera prestata, salvo il rimborso per le spese effettivamente sostenute per l'attività prestata. Eventuali compensi professionali possono essere erogati

allorché persone esterne all'Associazione siano chiamate a svolgere attività di collaborazione nell'ambito della segreteria e/o della conduzione degli aspetti amministrativi e fiscali.

### **Risorse economiche**

Il GOIRC trae le risorse economiche per il funzionamento e per lo svolgimento delle proprie attività da:

- a) contributi privati;
- b) contributi dello Stato, di Enti e di istituzioni pubbliche;
- c) donazioni e lasciti testamentari;
- d) rimborsi derivanti da convenzioni;
- e) eventuali entrate o acquisizioni a qualsiasi altro titolo conseguite, nonché dagli ulteriori redditi derivanti dal patrimonio e dalle proprie attività.

L'accettazione e l'utilizzazione dei contributi sono proposte dal Presidente ed approvate dal Consiglio Direttivo. I finanziamenti possono essere anche finalizzati dal donatore a singole unità del GOIRC o a specifici progetti e verranno in tal caso utilizzati su proposta del direttore o responsabile della struttura dell'unità aderente o del responsabile del progetto.

I finanziamenti per la ricerca, assegnati a specifici studi GOIRC, sono gestiti secondo le abituali metodologie amministrative, ma sotto la responsabilità di finalizzazione, di distribuzione e di utilizzazione da parte del responsabile scientifico dello studio.

Il patrimonio dell'Associazione, costituito con tutte le risorse di cui sopra, non può essere ripartito tra i soci né durante la vita dell'Associazione, né all'atto del suo scioglimento.

E' possibile devolvere fondi per il finanziamento o la costituzione di Enti aventi analoghe finalità a condizione che il patrimonio dell'Associazione rimanga sufficiente per il conseguimento dei suoi scopi.

E' vietata la distribuzione, anche in modo indiretto, di utili e avanzi di gestione nonché fondi, riserve o capitale durante la vita dell'organizzazione, a meno che la destinazione o la distribuzione non siano imposte per legge.

### **Esercizio sociale**

L'esercizio sociale coincide con l'anno solare.

Al termine di ogni esercizio il Consiglio Direttivo redige il bilancio consuntivo, che deve essere approvato dall'Assemblea ordinaria dei soci entro l'anno successivo a quello cui fa riferimento il bilancio.

### **Scioglimento**

Lo scioglimento del GOIRC può avvenire su proposta di almeno 4/5 dei componenti del Consiglio Direttivo, motivata dal sopravvenuto venire meno degli scopi sociali, o dal mancato funzionamento degli organi sociali.

### **Regolamenti**

I Regolamenti redatti dal Consiglio Direttivo, e ratificati dall'Assemblea, integrano e completano le disposizioni dello Statuto

### **Il Consiglio Direttivo di GOIRC, in data 23 marzo 2021, ha approvato il Regolamento sulla Funzionalità**

#### **Detto Regolamento contiene:**

- specificazioni in merito ad unità aderenti, soci e assemblea;
- specificazioni in merito alle modalità operative per gli studi GOIRC (per la modalità di proposta, discussione, accettazione, apertura, gestione e chiusura degli studi clinici promossi dal GOIRC, il Regolamento rinvia agli allegati documenti);
- indicazioni in merito ai gruppi di studio per patologia (i Gruppi di Studio per Patologia “Gruppi di Patologia” che partecipano al Comitato Scientifico sono individuati di volta in volta dal Consiglio Direttivo e riguardano singole patologie: patologie mammarie; polmonari; gastrointestinali; genitourinarie; l'attività dei Gruppi di Patologia, nell'ambito della patologia di riferimento, consiste nel: valutare e promuovere nuovi studi che vengono proposti all'interno del GOIRC o da altri promotori; promuovere interventi di formazione e aggiornamento rivolti ai giovani sperimentatori.
- specificazioni in merito al comitato scientifico (l'attività del Comitato Scientifico consiste nel: valutare nuovi studi che vengono proposti dai Gruppi di Patologia; identificare iniziative di formazione e di informazione anche in collaborazione con le associazioni dei pazienti da proporre al Consiglio Direttivo)
- specificazioni in merito alle norme elettorali per la nomina del Consiglio Direttivo;
- specificazioni in merito alla cessazione di componente del Consiglio Direttivo;
- specificazioni in merito alla quota associativa annuale;
- specificazioni in merito ai rimborsi spese;
- specificazioni in merito alle risorse economiche.

#### **In proposito, si evince dal Regolamento quanto segue:**

- fermo il diritto prioritario di GOIRC e del suo Consiglio Direttivo sull'amministrazione delle risorse, la gestione dei finanziamenti per la ricerca è assegnata all'unità aderente GOIRC di cui faccia parte la persona indicata come *principal investigator* dello studio o, nel caso il *principal investigator* non appartenga ad alcuna unità aderente, all'unità dallo stesso indicata in fase di predisposizione del protocollo;
- l'unità aderente potrà disporre, in persona del suo direttore o responsabile della struttura e nell'ambito del perseguimento delle finalità statutarie di GOIRC, sull'utilizzo di tali risorse;
- ogni spesa superiore all'importo di € 1.000 non previamente individuata nei budget degli studi dovrà comunque essere approvata dal Consiglio Direttivo, preferibilmente con voto segreto;
- nella stessa maniera sono trattate eventuali somme pervenute a diverso titolo finalizzate a specifiche unità operative;
- ogni 6 mesi il Consiglio Direttivo dedica una riunione all'esame dei budget aggiornati degli

studi in corso;

- salvo diversa decisione del Consiglio Direttivo per specifiche fattispecie, una quota pari al 15% di ogni somma ricevuta dal GOIRC e finalizzata a specifiche unità operative, viene destinata alla copertura delle spese per la gestione generale.

### **1.3 Sistemi gestionali, standard e certificazioni.**

GOIRC ha adottato un MOP (Modello Organizzativo Privacy) volto alla completa gestione dei dati personali inerenti all'attività associativa nonché un Sistema di gestione del Whistleblowing, in attuazione della recente normativa di settore (D.Lgs. n. 24/2023).

### **1.4 Sedi legali ed operative.**

**GOIRC ha sede legale in Parma** alla via Gramsci 14.

### **1.5 MOG 231 di GOIRC**

Il presente Modello Organizzativo, di seguito anche: "MOG 231" o "Modello 231" è stato redatto, in base ai requisiti del D.Lgs. 231/2001, in collaborazione con un gruppo di lavoro opportunamente formatosi nell'Ente.

**La redazione è avvenuta in ragione dei seguenti requisiti:**

- Contesto aziendale
- Normative applicabili
- Direzione, politica e responsabilità
- Processi per pianificare e considerare rischi ed opportunità
- Processi relativi a utenti, prodotti e servizi
- Processi per il miglioramento.

## **2. GOIRC e il decreto legislativo n. 231/2001: i reati presupposto e le attività sensibili.**

### **2.1 La normativa e i reati-presupposto**

Il D.Lgs. 8 giugno 2001 n. 231, 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 collettivi** (società, persone giuridiche, enti collettivi non riconosciuti, associazioni, consorzi) **per alcuni reati**, tassativamente elencati, **ove commessi nel loro interesse o vantaggio**:

- da persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli enti stessi 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 (c.d. soggetti apicali);
- da persone fisiche sottoposte alla direzione o alla vigilanza dei soggetti apicali, se la commissione del reato sia stata resa possibile dall’omissione di vigilanza di questi ultimi.

La responsabilità dell’ente collettivo – che si aggiunge a quella della persona fisica che ha commesso il reato - si configura anche in relazione a reati commessi all’estero, nell’interesse o a vantaggio di un ente che abbia in Italia la sua sede principale, purché, tra l’altro, per la loro repressione non proceda lo Stato del luogo in cui siano stati commessi.

**2.2** Alla data di adozione del presente Modello organizzativo, **le tipologie di reato** dalla cui commissione può derivare la responsabilità amministrativa degli enti collettivi (c.d. **reati-presupposto**) sono le seguenti:

#### **Articolo 24 del (D.lgs 231/2001)**

**Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell’Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture**  
(artt.316 bis, 316 ter, 640 comma 2, 640 bis e 640 ter del codice Penale)

#### **Articolo 24 bis del (D.lgs 231/2001)**

##### **Delitti informatici e trattamento illecito di dati**

(artt. 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies, 629, terzo comma, articoli 615-quater, 635 quater 1, 491 bis e 640 quinquies del Codice Penale)

#### **Articolo 24 ter del (D.lgs 231/2001)**

##### **Delitti di criminalità organizzata**

(artt. 416 sesto comma, 416 bis, 416 ter e 630 del Codice Penale,  
art.407, comma 2, lettera a numero 5 del codice di procedura penale)  
art.74 D.P.R 309/1990

**Articolo 25 del (D.lgs 231/2001)**

Peculato , indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione [e abuso d'ufficio]  
(artt.318,321,322, 346 bis, 314 bis, 316, 319, 319 ter, 317, 321, 320 e 322 bis del codice penale)

**Articolo 25 bis del (D.lgs 231/2001)**

**Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento**  
(artt. 453,454,460,461,455,457,464,459,464,473 e 474 del Codice penale)

**Articolo 25 bis 1 del (D.lgs 231/2001)**

**Delitti contro l'industria e il commercio**

(artt. 513 , 513 bis , 514, 515, 516, 517, 517 ter e 517 quater del Codice penale)

**Articolo 25 ter 3 del (D.lgs 231/2001)**

**Reati societari**

(artt.2621, 2621 bis, 2622, 2622 terzo comma, 2623 primo comma, 2623 secondo comma, 2624 primo comma, 2624 secondo comma, 2625 secondo comma, 2632, 2626,2627, 2628 del codice civile)

**Articolo 25 quater**

**Delitti con finalità di terrorismo o di eversione dell'ordine democratico**

**Articolo 25 quater - 1**

**Pratiche di mutilazione degli organi genitali femminili:**

(art.583 bis Codice Penale)

**Articolo 25 quinquies**

**Delitti contro la personalità individuale**

(artt. 600,600 bis, 600 bis secondo comma, 600 ter- terzo e quarto comma, 600 quater, 600 quater 1, 600 quinquies, 601,602,603 bis, 609 undecies Codice Penale)

**Articolo 25 sexies**

**Abusi di mercato**

( D.lgs 24 febbraio 1998 n.58 Parte V, titolo I bis, capo II)

**Articolo 25 septies**

**Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro**

(artt.589 e 590 terzo comma)

**Articolo 25 octies**

**Ricettazione riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché di auto riciclaggio**

(artt.648,648 bis,648 ter, Codice Penale)

**Articolo 25 nonies**

**Delitti in materia di violazione del diritto di autore**

(Legge 22 Aprile 1941 n.633 artt.171 primo e terzo comma, 171 bis, 171 ter,171 septies, 171 octies, 174 quinquies)

#### **Articolo 25 decies**

#### **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria**

(art 377 bis Codice Penale)

#### **Articolo 25 undecies**

#### **Reati Ambientali**

(artt.452 bis, 452 quater, 452 quinquies, 452 sexies, 452 septies, 452 octies, 452 terdecies, 452 quaterdecies, 727 bis, 733 bis,137 commi 2-3-5, 255 bis, 255 ter, 256 commi 1-1bis, 3- 3 bis-5 e 6, 256 bis commi 1 e 3 bis, 257 comma 1 e 2, 258 comma 4, 259 comma 1, 260, 260 bis, 279 comma 5 del Codice Penale)

#### **Articolo 25 duodecies**

#### **Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare**

(Articolo 22 comma 12 bis, articolo 12 commi 3,3 bis e 3 ter, articolo 12 comma 5 del Decreto legislativo 25 Luglio 1998)

#### **Articolo 25 terdecies**

#### **Razzismo e xenofobia**

(Articolo 3 commi 1 e 3 bis della Legge 13 Ottobre 1975 n.654)

#### **Articolo 25 quinquiesdecies**

#### **Reati tributari**

### **2.3 L'APPLICABILITÀ A GOIRC DEL D.Lgs. 231/2001**

GOIRC (di seguito anche solo "Ente" o "Associazione") è un'associazione con personalità giuridica, senza finalità di lucro.

#### **2.3.1 GOIRC: organizzazione e attività svolte**

La più recente dottrina ha confermato che:

- il D.lgs 231/01 trova applicazione con riferimento alle associazioni e le fondazioni riconosciute, disciplinate nell'art.14 c.c in quanto dotate di personalità giuridica <sup>1</sup>.
- il Legislatore, utilizzando l'espressione "società e associazioni senza personalità giuridica" ha voluto estendere l'applicazione del D.lgs 231/01 a tutte quelle organizzazioni nelle quali è possibile individuare un autonomo centro di interessi (le società di persone, le associazioni non riconosciute, le fondazioni, i comitati).

#### **Per completezza, si evidenzia che:**

- la Relazione Ministeriale specifica che quanto agli enti "a soggettività privata" non dotati di personalità giuridica "la scelta ben si comprende da un punto di vista di politica

---

<sup>1</sup> FABRIZIO D'ARCANGELO, Fondazioni e associazioni nel disegno sistematico del D.lgs 231/01 , in Rivista 231.

legislativa, dal momento che si tratta dei soggetti che, potendo più agevolmente sottrarsi ai controlli statali, sono a “maggior rischio” di attività illecite ed “attorno ai quali appare dunque ingiustificato creare vere e proprie zone di immunità”;

- allo scopo di contenere tale rischio, il D.lgs 231/01 ha preferito utilizzare una formula elastica, limitandosi a citare **“le società e le associazioni anche prive di personalità giuridica, in modo da indirizzare l'interprete verso la considerazione di enti che, seppur sprovvisti di personalità giuridica, possano comunque ottenerla”**. In proposito, si è rilevato che sebbene l'art.38 c.c preveda che gli amministratori di enti non riconosciuti rispondano illimitatamente delle obbligazioni contratte dalla società, tale disposizione non trova applicazione rispetto alla responsabilità ex D.lgs 231/01, la cui eventuale sanzione pecuniaria viene soddisfatta solo con il patrimonio o il fondo comune della società <sup>2</sup>.

### **2.3.2 GOIRC, quale Associazione senza finalità di lucro.**

Parte della dottrina ritiene che il sistema normativo rappresentato dal D.Lgs. n. 231 riguarderebbe esclusivamente gli **enti caratterizzati da scopo di lucro**: attraverso il citato decreto, il legislatore avrebbe voluto ispirarsi ad una realtà esclusivamente imprenditoriale, mossa in via principale da un fine di profitto in senso economico.

Questa interpretazione non trova alcun addentellato testuale nell'ambito dello stesso Decreto, in quanto l'esercizio dell'attività economica o lo scopo di lucro sono requisiti di fattispecie che, pur essendo latenti nel sistema, non sono gli unici che la legge intende disciplinare.

**L'esplicita menzione delle associazioni anche prive di personalità giuridica e il generico richiamo agli enti collettivi comprovano che, nel disegno del legislatore delegato, il fine di lucro dell'ente non rappresenta affatto un presupposto necessario per l'operatività della disciplina in materia di responsabilità amministrativa degli enti.**

In altri termini, ai sensi del D.Lgs. 231/01, il sistema di responsabilità amministrativa degli enti, benché concepito per contrastare la criminalità d'impresa, non è un carattere esclusivo della società o degli enti esercenti l'attività di impresa commerciale.

Il D.Lgs. n. 231 vuole contrastare non il perseguimento di un profitto mediante la commissione di un reato ma evitare che la struttura predisposta all'organizzazione di qualsivoglia attività sia causa o elemento facilitante la commissione di crimini <sup>3</sup>.

### **2.3.4 GOIRC quale Ente di piccole dimensioni**

L'art. 6, comma 4, del D.Lgs. n. 231 prevede che, negli “enti di piccole dimensioni”, i compiti attribuiti all'organismo di vigilanza possano essere svolti, direttamente, dall'organo dirigente.

Il legislatore delegato, tuttavia, non fornisce la definizione di ente di piccole dimensioni, lasciando pertanto all'interprete il compito di individuarne le caratteristiche.

---

<sup>2</sup> D'ARCANGELO, Fondazioni ed associazioni nel disegno del decreto legislativo 231/01, in Rivista 231.

<sup>3</sup> Il giudice dell'udienza preliminare del Tribunale di Milano ha comminato una sanzione, in sede di patteggiamento, ad una associazione volontaria di pubblica assistenza (ONLUS) in relazione al delitto di truffa in danno di ente pubblico (30 marzo 2011). La Onlus in questione è stata condannata per le condotte fraudolente attraverso le quali simulava nei confronti dei terzi la propria natura solidaristica e volontaristica (senza fini di lucro) per ottenere sussidi e contributi a titolo gratuito, nonché per assicurarsi contratti e convenzioni con enti e istituzioni pubbliche, anche in mancanza dei requisiti necessari. Il Giudice ha applicato la sanzione pecuniaria di 26.000 euro all'ente, disponendo altresì la confisca delle giacenze bancarie e di tutti gli automezzi già oggetto di precedente sequestro preventivo.

La struttura organizzativa delle piccole imprese (per “struttura organizzativa” si intendono le modalità attraverso le quali si ripartiscono compiti, poteri e responsabilità all’interno dell’organizzazione) si contraddistingue per la sua “essenzialità”, in quanto dotata dei soli elementi indispensabili per il suo funzionamento.

Al fine di comprendere se la struttura di un’impresa sia essenziale, occorre svolgere un’analisi degli elementi che la compongono, per verificare se essi possano considerarsi necessari perché l’ente possa esistere ed operare.

Altro elemento che contraddistingue gli enti di piccole dimensioni è il grado di concentrazione delle funzioni in capo a poche persone; in altri termini, la maggior parte delle operazioni che si riferiscono alla gestione aziendale fanno capo a pochi determinati soggetti.

Sotto un profilo operativo, può essere utile il raffronto del numero delle funzioni esistenti nella specifica realtà aziendale, con i soggetti a cui le stesse sono affidate.

Tra i principi di revisione delle imprese ed enti minori è opportuno verificare la concentrazione della proprietà e della direzione, la limitatezza delle fonti di ricavi e la semplicità dei sistemi contabili e di controllo interno.

Il modello da adottare in un ente di piccole dimensioni ha una complessità sicuramente inferiore rispetto al modello adottato in un’impresa medio-grande; infatti, le questioni concernenti l’organizzazione, le deleghe di funzioni e le procedure decisionali ed operative sono destinate ad assumere un minor rilievo in una piccola impresa, nella quale (come già rilevato) la maggior parte delle funzioni è concentrata in capo a poche persone.

**Le piccole imprese sono caratterizzate da minori risorse da poter dedicare alla predisposizione di un modello organizzativo ed ai relativi controlli. Proprio per la dimensione e la semplicità della struttura organizzativa esse, infatti, non dispongono di una funzione (o persona) con compiti di monitoraggio del sistema di controllo interno, e l’onere derivante dall’istituzione di un organismo ad hoc potrebbe non essere economicamente sostenibile.**

Considerate le osservazioni sopra svolte, la normativa in esame è stata ritenuta applicabile agli Enti di piccole dimensioni dotati di personalità giuridica privata.

A GOIRC, in quanto enti dotati di personalità giuridica privata, con un patrimonio finalizzato a un preciso scopo, lecito e di utilità sociale, si applica il D.lgs. 231/01 in ragione “della posizione talvolta di indubbio spessore che detti enti assumono nella sfera giuridica ed economica ” e in virtù dell' art.27 del D.lgs 231/01 che nello stabilire che dell'obbligazione per il pagamento della sanzione pecuniaria risponde soltanto l'ente con il patrimonio o con il fondo comune, sembra fare riferimento proprio anche alle Associazioni non riconosciute e alle fondazioni (il richiamo al “patrimonio” nella sistematica del codice civile fa riferimento, oltre che alle strutture societarie, alle associazioni non riconosciute e alle fondazioni <sup>4</sup>.

In conclusione, al GOIRC, quale Ente no profit di piccole dimensioni, è applicabile, in ragione: della sua struttura organizzativa e delle attività svolte, il D.Lgs. 231/01.

---

<sup>4</sup> Tribunale di Milano, Sez. Riesame, ordinanza 26 Giugno 2008.

Pertanto, il GOIRC è interessato all'adozione di un proprio Modello organizzativo ex artt. 6 e 7 D.Lgs. 231/01, al fine di prevenire il rischio reato.

Nell'ambito dell'Associazione sono da ritenere soggetti apicali i componenti del Consiglio Direttivo.

## **2.4 CRITERI UTILIZZATI PER L'ELABORAZIONE DEL MODELLO**

**Per l'elaborazione di un adeguato Modello organizzativo di GOIRC occorre esaminare:**

- 1) il tipo di attività svolta:** per comprendere quali siano gli illeciti, tra quelli previsti dal decreto, che nell'ambito delle attività svolte dall'ente potrebbero verificarsi;
- 2) la complessità organizzativa:** al crescere della "consistenza occupazionale" dell'ente, dei livelli gerarchici, del numero degli associati e delle sedi operative, della complessità dei processi da governare, aumenta la possibilità dell'esistenza di falle all'interno del sistema di prevenzione in vigore e diventa più difficile garantire la trasparenza, la separazione delle funzioni e delle responsabilità, nonché la tracciabilità delle operazioni;
- 3) la consistenza patrimoniale e i flussi economico-finanziari:** soggetti che gestiscono ingenti patrimoni, siano essi immobili o valori mobiliari e sono caratterizzati da elevati volumi di affari corrono certamente rischi maggiori rispetto ad operatori che gestiscono attività di dimensioni più ridotte;
- 4) la natura giuridica e i rapporti con la P.A.:** molti dei soggetti appartenenti al terzo settore interagiscono con la Pubblica Amministrazione per una serie di ragioni; appare evidente come tali soggetti siano certamente molto esposti al rischio di commissione di reati di corruzione.
- 5) la tipologia di controlli** a cui il soggetto è sottoposto: per la valutazione dei rischi connessi alla commissione di alcuni dei reati-presupposto, la mancanza di obblighi stringenti in relazione al controllo e alla rendicontazione contabile o al rispetto dei vincoli gestionali e di scopo, è un fattore che incrementa la probabilità che un illecito possa effettivamente verificarsi.

### **2.4.1 L'individuazione dei reati-presupposto e delle attività sensibili.**

Il D.lgs. 231 è stato applicato quasi esclusivamente ad imprese di tipo commerciale sicchè adattare alle realtà del non profit i dettami normativi richiede uno sforzo di rielaborazione.

In mancanza di schemi ed approcci specifici per il non profit, per l'elaborazione di un adeguato Modello organizzativo di GOIRC è opportuno traslare *framework* e principi prettamente aziendalistici, fatte salve le dovute distinzioni connesse alle peculiari caratteristiche degli enti in questione.

Gli operatori del terzo settore non devono analizzare solo componenti *hard* del rischio-reato, quali l'intensità e la tipologia delle sanzioni, ma altresì elementi *soft* quali l'influenza sull'opinione pubblica e su altri *stakeholders* rilevanti per l'attività dell'ente.

Anche gli illeciti che non generano la comminazione di sanzioni estremamente incisive (come, ad esempio, le false comunicazioni sociali per le quali non sono previste sanzioni interdittive), possono diventare critici se impattano in maniera rilevante sull'opinione

pubblica e sulla percezione che gli interlocutori hanno dell'ente in questione <sup>5</sup>.

#### 2.4.2 I reati ipotizzabili nell'attività di GOIRC

In relazione all'attività caratteristica di GOIRC e alla sua organizzazione associativa appaiono **astrattamente ipotizzabili, in prima analisi** (nella presente Parte Generale del MOG 231 di GOIRC) le seguenti fattispecie di reato:

• Corruzione per l'esercizio della funzione (art 318 c.p.)
• Corruzione per un atto contrario ai doveri d'ufficio (art 319 c.p.)
• Istigazione alla corruzione (art 322 c.p.)
• Induzione indebita a dare o promettere utilità (art 319- <i>quater</i> c.p.)
• Traffico di influenze illecite (art 346-bis c.p.)
• False comunicazioni sociali (art 2621 c.c.)
• Impedito controllo (art 2625 c.c.)
• Corruzione tra privati (art 2635 c.c.); istigazione alla corruzione tra privati (art 2635-bis c.c.)
• Riciclaggio, reimpiego di utilità illecite e autoriciclaggio (artt. 648- <i>bis</i> , 648- <i>ter</i> e 648- <i>ter.1</i> c.p.)
• Associazione per delinquere (art 416 c.p.)

Nella **Parte Speciale del presente MOG 231** verranno esaminate le singole fattispecie di reato correlate alle funzioni e ruoli assegnati dall'Ente ai suoi dipendenti e apicali; inoltre, verranno descritte le Procedure specificamente dedicate alla prevenzione dei reati-presupposto correlati alle attività sensibili ex D.Lgs. 231/01.

---

<sup>5</sup> Secondo il documento *"Il modello 231/2001 per gli enti non profit: una soluzione per la gestione dei rischi"* (Consiglio nazionale Ordine dottori commercialisti ed esperti contabili, 2012) – d'ora in avanti: **Linee-guida 231 commercialisti**.

### 2.4.3 I PROCESSI SENSIBILI

Nell'ambito dell'attività di GOIRC si possono individuare i seguenti **Processi sensibili** (intesi quali insieme di attività funzionalmente interrelate, nell'ambito delle quali è astrattamente possibile la commissione dei reati ex D.Lgs 231/01 sopra indicati):

<b>1. Gestione dei rapporti con soggetti appartenenti alla Pubblica Amministrazione</b>
<b>2. Gestione ed esecuzione dei contratti con enti pubblici</b>
<b>3. Gestione dei rapporti con gli enti pubblici competenti in occasione dell'espletamento degli adempimenti amministrativi connessi all'attività dell'associazione</b>
<b>4. Gestione del ciclo passivo su beni, servizi e lavori</b>
<b>5. Gestione degli adempimenti richiesti dalla normativa vigente non connessi all'attività caratteristica, anche in occasione di verifiche, ispezioni e accertamenti da parte degli enti pubblici competenti</b>
<b>6. Gestione della contabilità generale e formazione del bilancio</b>
<b>7. Adempimenti amministrativi dell'associazione</b>
<b>8. Gestione della Tesoreria e della finanza ordinaria</b>
<b>9. Gestione dei rapporti con società ed enti privati</b>

La **descrizione analitica dei processi sensibili e delle procedure** previste per la prevenzione dei reati-presupposto e per la mitigazione dei relativi rischi sono descritte nel Sistema generale di prevenzione, nella **Parte Speciale del presente MOG 231** e, in particolare, nelle singole Procedure relative alle aree sensibili individuate.

L'individuazione e descrizione delle aree/processi sensibili verranno correlate ai ruoli e funzioni dei dipendenti ed apicali di GOIRC: assemblea dei soci; comitato scientifico; consiglio direttivo; presidente; tesoriere; segretario; gli adempimenti amministrativi e contrattuali connessi all'attività di GOIRC (contabilità, redazione di bilanci annuali e periodici, fatturazione, gestione rapporti con la banca, adempimenti tributari) sono gestiti in outsourcing da consulente esterno.

Il rapporto contrattuale con tale consulente è disciplinato da apposita regolamentazione integrativa del presente Modello.

#### **2.4.4 Le attività a rischio di reato**

In seguito all'analisi dei rischi condotta con riferimento allo svolgimento delle attività associative, sono state individuate le seguenti attività sensibili:

##### **- Attività a rischio-corrruzione (istigazione alla corruzione, induzione indebita a dare o promettere utilità e traffico di influenze illecite)**

- dazione o promessa di utilità a soggetti con poteri decisionali sullo studio no profit
- utilizzo di agenzie per mascherare ricezione di denaro (correlate alla posizione pubblicistica dei membri del Consiglio Direttivo) da parte di società farmaceutiche

##### **Attività a rischio-corrruzione tra privati**

- dazione o promessa di utilità a direttore di banca per ottenere agevolazioni nel rapporto con la banca stessa
- dazione o promessa di utilità ad esponente di società farmaceutica al fine di ottenere sponsorizzazione

##### **Attività a rischio-false comunicazioni sociali**

###### **PRO-SOC**

alterazione delle voci che confluiscono nel bilancio al fine di esporre una situazione finanziaria non rispondente alla realtà.

##### **Attività a rischio-impedito controllo**

###### **PRO-SOC**

Impedimento o ostacolo delle attività di controllo attribuite agli Organi statutari mediante occultamento di documenti o con altri artifici

##### **Attività a rischio-riciclaggio (reimpiego e autoriciclaggio)**

###### **PRO-TRI**

utilizzo nella propria attività associativa di risparmio d'imposta, illecitamente conseguito in seguito alla commissione di reato tributario

##### **Attività a rischio-associazione per delinquere**

###### **PRO-CRI**

Realizzazione delle condotte sopra menzionate da parte di più persone (almeno tre) in maniera coordinata e ripetuta nel tempo (vincolo associativo).

### **3. CODICE ETICO di GOIRC**

#### **INDICE**

##### **Premessa**

- art. 1 - finalità.
- art. 2 - destinatari ed ambito di applicazione.
- art. 3 - principi generali.
  - art. 4 - eguaglianza, legalità e correttezza.
  - art. 5 - onestà, fiducia e fedeltà.
  - art. 6 - trasparenza.
  - art. 7 - imparzialità del personale.
- art. 8 - riservatezza.
- art. 9 - protezione dei dati personali.
- art. 10 - conflitto di interessi ed attività esterne.
- art. 11 - politiche del personale.
- art. 12 - professionalità e diligenza.
- art. 13 - controllo e responsabilità.
- art. 14 - tutela del patrimonio aziendale.
- art. 15 - tutela ambientale.
- art. 16 - rapporti con i clienti.
- art. 17 - rapporti con i fornitori.
- art. 18 - rapporti con i collaboratori.
- art. 19 - rapporti con i concorrenti.
- art. 20 - rapporti con la pubblica amministrazione.
- art. 21 - rapporti con la collettività e con gli organi di informazione.
- art. 22 - rapporti con le organizzazioni politiche e sindacali.
- art. 23 - rapporti con le autorità pubbliche di vigilanza.
- art. 24 - misure disciplinari.
- art. 25 - procedure, controllo, diffusione e aggiornamento

## **PREMESSA**

Elemento fondamentale nell'implementazione di un Modello che riduca il rischio-reato è lo sviluppo, all'interno dell'Organizzazione, di un clima culturale che dissuada dalla commissione dei reati.

A tal fine, un'importante operazione consiste nella redazione del Codice etico, nel quale si racchiudono gli impegni e le responsabilità morali nella conduzione delle attività svolte dalle persone che operano nell'ente o entrano in contatto con esso al fine di:

- Conservare e diffondere il rapporto di fiducia con i principali stakeholders (organi sociali, personale, clienti, fornitori, enti pubblici, associazioni di categoria, ecc.);
- Scongiurare comportamenti non etici.

### **Pertanto:**

- Il presente Codice Etico definisce i valori che “ GOIRC” o “Ente” riconosce, accetta e condivide, descrivendo i principi e le norme di condotta ai quali tutti i destinatari devono attenersi nello svolgimento della loro attività.

- Il Codice è volto a diffondere, all'interno dell'Ente, un clima culturale che dissuada da condotte che possano configurare reati e costituisce un presidio essenziale per la prevenzione della commissione di illeciti.

- Le norme del Codice Etico devono ritenersi estese oltre l'ambito di operatività del D.Lgs. n. 231/01, costituendo un elenco di doveri del personale integranti una specificazione dei principi contenuti nei contratti di lavoro.

### **ART. 1 - FINALITÀ.**

Le regole del Codice costituiscono condizione imprescindibile per il conseguimento della missione dell'Ente, integrano i doveri fondamentali dei lavoratori e non esimono dall'osservanza della normativa civile, penale, amministrativa e contrattuale vigente in materia.

Il Codice Etico di GOIRC intende: garantire una gestione aziendale etica, trasparente e consapevole; accrescere il grado di credibilità e di reputazione dell'Associazione, diffondendone un'immagine di trasparenza, correttezza ed affidabilità; creare rapporti stabili e proficui ispirati alla fiducia reciproca di tutti i suoi destinatari.

Mediante l'osservanza del Codice Etico, GOIRC intende favorire:

- all'esterno, la fedeltà degli utenti, l'attrazione delle migliori risorse umane, la serenità dei fornitori, l'affidabilità verso i creditori;
- all'interno, l'attuazione di decisioni senza frizioni e l'organizzazione del lavoro senza controlli burocratici ed eccessivi esercizi dell'autorità.

## **ART. 2 - DESTINATARI ED AMBITO DI APPLICAZIONE.**

Le norme del Codice Etico si applicano, senza deroghe o eccezioni, a tutti coloro che, direttamente o indirettamente, in modo stabile o occasionale, operano, all'interno o all'esterno dell'Ente, per perseguirne/o condividerne gli obiettivi.

Il Codice Etico vincola gli amministratori, i dipendenti, i collaboratori, i consorziati e, in via generale, i *partners* di GOIRC e si propone, in via generale, come modello comportamentale per tutti gli *stakeholders*, considerati, nel complesso, "destinatari".

Tutti coloro che rappresentano, dirigono o lavorano a qualsiasi titolo in GOIRC devono osservare, nell'esercizio delle proprie funzioni e responsabilità, i principi, le norme di comportamento ed i divieti del Codice Etico.

Il Codice deve essere osservato da ogni soggetto titolare di contratto di lavoro a tempo indeterminato o determinato o di altro rapporto che comporti prestazioni di opera anche temporanea, lo svolgimento di attività in nome e per conto del GOIRC ovvero una relazione fiduciaria con GOIRC, ivi compresa l'attività di consulenza.

Il Codice dev'essere osservato, inoltre, dai soggetti che rivestono funzioni di rappresentanza, di amministrazione o direzione di GOIRC o di una sua eventuale unità organizzativa dotata di autonomia finanziaria e funzionale.

I responsabili di ciascuna Direzione/Funzione vigilano sull'osservanza del Codice, danno indicazioni ai dipendenti che richiedono chiarimenti in caso di dubbi e, nell'ipotesi di accertata violazione, riferiscono ai diretti superiori (intesi quali soggetti formalmente sovraordinati in via gerarchica e legittimati alla vigilanza e/o al controllo sull'attività dei dipendenti).

I dirigenti predispongono, altresì, i controlli necessari a garantire l'osservanza del Codice e, qualora vengano a conoscenza di violazioni alle regole stabilite dal presente Codice, ne riferiscono tempestivamente all'Organo Amministrativo al fine di adottare ogni iniziativa.

## **ART. 3 - PRINCIPI GENERALI**

I principi etici devono ispirare tutti i comportamenti di GOIRC e, in particolare, dei suoi dirigenti, dipendenti e collaboratori.

L'inosservanza dei principi e delle disposizioni del Codice Etico è incompatibile con l'attività svolta da GOIRC e con gli obiettivi di una gestione associativa etica, trasparente ed efficace.

Il personale si impegna ad evitare situazioni e comportamenti che possano nuocere agli interessi o all'immagine di GOIRC.

Le comunicazioni di GOIRC effettuate dai dipendenti e dirette a soggetti esterni devono essere preventivamente concertate con il diretto superiore.

I destinatari del presente Codice non possono utilizzare per fini privati e

nel proprio interesse o a vantaggio di altri, informazioni o documenti, anche non riservati, di cui dispongono per ragioni di ufficio.

Le diverse pratiche vanno trattate con i soggetti titolari o loro rappresentanti, evitando di discutere argomenti d'ufficio o di mettere documenti a disposizione di persone o di ex dipendenti di GOIRC non autorizzati.

Il personale partecipa a riunioni od incontri con terzi che attengono alle attività di GOIRC solo se espressamente autorizzato dal Consiglio Direttivo.

Il personale che, per fatti relativi all'esercizio della propria funzione di dipendente di GOIRC, viene ad essere parte in un procedimento penale, ivi compresa la fase delle indagini preliminari, è obbligato a darne tempestiva comunicazione scritta, in via riservata, all'Organo Amministrativo.

I soggetti che, per ragioni d'ufficio, vengano a conoscenza dell'esistenza di irregolarità amministrative e procedurali devono riferirlo immediatamente al Consiglio direttivo e agli Organi dell'associazione e nel caso in cui tale irregolarità coinvolga lo stesso titolare dell'ufficio, a soggetti ad esso sovraordinati.

#### **ART. 4 - EGUAGLIANZA, LEGALITA' E CORRETTEZZA.**

GOIRC gestisce i rapporti con i vari destinatari nell'ottica di diffondere la cultura dell'eguaglianza e dell'imparzialità. Il Codice Etico promuove e favorisce la pari dignità e l'eguaglianza dei destinatari senza distinzioni di razza, ceto, lingua, convincimenti o orientamenti, filosofici, religiosi o sessuali, opinioni politiche o appartenenze sindacali, condizioni personali, anagrafiche o sociali.

La condotta di GOIRC e di tutti i destinatari del Codice Etico è improntata all'osservanza del principio di legalità e, dunque, al diligente rispetto della disciplina normativa, generale e di settore, oltre che dei provvedimenti emanati da Autorità o Istituzioni afferenti all'organizzazione ed alle attività aziendali.

Tutti i destinatari del Codice Etico devono conformare il proprio comportamento quotidiano al rispetto dei principi di lealtà e correttezza, quale parte essenziale delle obbligazioni assunte nei confronti di GOIRC.

#### **ART. 5 - ONESTA', FIDUCIA E FEDELTA'.**

Tutte le attività di GOIRC devono essere svolte con onestà, buona fede ed integrità morale, assicurando il rispetto dei diritti e degli interessi legittimi dei clienti, dipendenti, azionisti, *partner* commerciali e della collettività nella quale GOIRC è presente ed opera.

GOIRC instaura con i propri dipendenti rapporti fondati sulla reciproca fiducia e lealtà. La condivisione della missione dell'Azienda e la fiducia nella capacità di perseguire e conseguire gli obiettivi associativi trovano solido fondamento nel rispetto, da parte di ciascuno, dei valori espressi nel presente

Codice Etico. La fiducia e la coesione del gruppo di lavoro, fondata sull'osservanza dei valori e dei principi del Codice Etico, garantisce, nell'ambito di una strategia di lungo termine, il benessere dei dipendenti e della collettività.

L'obbligo di fedeltà gravante su ciascuno dei dipendenti comporta il divieto di: trattare affari, per conto proprio o di terzi, in concorrenza con l'Ente; svolgere attività contrarie agli interessi dell'Ente o incompatibili con i doveri d'ufficio; divulgare notizie attinenti all'organizzazione ed ai metodi di produzione dell'Associazione o farne uso in modo da cagionare ad essa un pregiudizio.

#### **ART. 6 - TRASPARENZA.**

Il personale deve conformare le proprie azioni, operazioni e/o negoziazioni al principio di massima trasparenza, intesa come chiarezza e veridicità delle condotte. GOIRC assicura una gestione aziendale che applichi i principi di tracciabilità, controllo e verificadei comportamenti.

GOIRC osserva i principi di corretta e trasparente tenuta contabile, rispettando i valori di verità, accuratezza e completezza dell'informazione.

Ogni operazione e transazione effettuata in GOIRC dev'essere correttamente registrata e ciascuna operazione dev'essere supportata da adeguata documentazione, al fine di consentire la puntuale ricostruzione dell'operazione svolta, effettuare gli opportuni controlli, distinguere tra i diversi livelli di responsabilità ed individuare chi ha autorizzato, effettuato, registrato e verificato l'operazione stessa.

I bilanci, le relazioni e le comunicazioni sociali previsti dalla legge devono essere redatti, in osservanza delle norme codicistiche e dei principi contabili, con chiarezza e trasparenza e rappresentare, in modo corretto e veritiero, la situazione patrimoniale e finanziaria dell'Ente.

Tutto il personale di GOIRC coinvolto nel processo deve: fornire informazioni chiare e complete; assicurare l'accuratezza dei dati e delle elaborazioni; segnalare la presenza di conflitti di interesse; non interferire, con qualsiasi modalità, sul contenuto delle relazioni o comunicazioni dei responsabili della revisione o, comunque, influenzare la loro indipendenza; non impedire od ostacolare il regolare svolgimento delle attività degli organi sociali, dei revisori, della società di revisione e del socio, collaborando, ove richiesto, all'espletamento di ogni forma di controllo e revisione della gestione sociale, previste dalla legge.

E' fatto divieto di tenere comportamenti (occultamento di documenti o uso di altri mezzi fraudolenti) che impediscano o che comunque ostacolino lo svolgimento dell'attività di controllo o revisione legalmente attribuite al socio, al collegio sindacale o alla società di revisione.

#### **ART. 7 - IMPARZIALITA' DEL PERSONALE.**

GOIRC adotta scelte imparziali in tutte le relazioni intercorrenti con i plurimi portatori di interesse.

I destinatari del Codice operano, nell'adempimento della prestazione lavorativa, con imparzialità e neutralità in tutti i procedimenti ed assumono decisioni con rigore e trasparenza e nel rispetto della legge.

Il personale non rifiuta né accorda ad alcuno prestazioni che siano normalmente accordate o rifiutate ad altri, garantendo la parità di trattamento tra tutti coloro che vengono in contatto con il GOIRC.

Il personale svolge correttamente l'attività amministrativa e respinge pressioni illegittime, ancorché provenienti dai suoi diretti superiori.

Qualora subisca pressioni, lusinghe o richieste di favori che riguardino la propria o altrui attività aziendale ovvero riceva proposte che ledano il dovere di imparzialità, il personale ne informa, senza indugio, il suo diretto superiore.

Il personale, qualora aspiri ad una promozione, ad un trasferimento o ad altro provvedimento, non tenta di influenzare coloro che devono o possono adottare la relativa decisione o influire sulla sua adozione, né chiede che altri lo facciano.

Il personale rispetta, nella trattazione delle pratiche e nello svolgimento delle singole attività, le procedure dell'Ente e, in particolare, l'ordine cronologico delle richieste ovvero le priorità stabilite dalle procedure interne.

Il personale non prende impegni né fa promesse in ordine a decisioni o azioni proprie o altrui inerenti all'ufficio, se ciò può generare sfiducia nell'Ente o nella sua indipendenza ed imparzialità o comunque pregiudicare l'immagine aziendale.

#### **ART. 8 - RISERVATEZZA.**

Il personale deve garantire la massima riservatezza in ordine ai dati, informazioni e notizie acquisiti in ragione dell'attività lavorativa e/o professionale. Il personale, ferma restando l'osservanza delle norme a tutela della *privacy*, rispetta il segreto d'ufficio e mantiene riservate le notizie e le informazioni apprese nell'esercizio delle proprie funzioni ed osserva il dovere di riservatezza anche dopo la cessazione dal servizio.

E' vietata la comunicazione o diffusione di notizie afferenti all'organizzazione ed ai metodi di lavoro nonché l'utilizzazione delle stesse che possa cagionare danno all'Ente; nessun dipendente, collaboratore o *partner* può trarre vantaggi, diretti o indiretti, personali o patrimoniali, dall'uso di informazioni riservate.

Fermi restando i divieti e gli obblighi previsti dalla legge, il personale non rilascia informazioni in merito ad atti o provvedimenti relativi a procedimenti amministrativi, civili e penali in corso, nonché all'iter della pratica, prima che siano stati ufficialmente approvati da GOIRC e comunicati formalmente alle

parti; in ogni caso, per il rilascio di qualsiasi informazione è necessaria la preventiva autorizzazione da parte del diretto superiore.

Il personale consulta i soli atti e fascicoli ai quali è autorizzato ad accedere e ne fa un uso conforme ai doveri d'ufficio, consentendone l'accesso a terzi solo nei casi previsti dalla legge, ed ai colleghi per motivi di servizio, in conformità alle prescrizioni impartite dall'ufficio.

I dati e le informazioni aziendali dovranno essere: conservati con adeguate misure tecniche ed organizzative, impedendo che soggetti non autorizzati ne prendano conoscenza; comunicati seguendo rigorosamente procedure prefissate in osservanza della normativa vigente; organizzati ed associati in modo da garantire ai soggetti autorizzati ad accedervi la conoscibilità degli stessi.

#### **ART. 9 - PROTEZIONE DEI DATI PERSONALI.**

GOIRC tutela i dati personali relativi ai propri dipendenti ed ai terzi, adottando tutte le misure, tecniche ed organizzative, idonee a prevenire danni alla persona e/o al *know how* aziendale e conforma la propria organizzazione e la propria attività ai principi di tutela dei dati personali sanciti nella normativa nazionale e comunitaria.

La politica di protezione dei dati personali dell'Associazione è improntata ai principi di liceità, correttezza e trasparenza nei confronti degli interessati nonché ai principi di "limitazione delle finalità" (i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo conforme a tali finalità), "minimizzazione dei dati" (i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati), "limitazione della conservazione" (i dati personali sono conservati in una forma che consente l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati trattati), "integrità e riservatezza" (i dati personali sono trattati in modo da garantire un'adeguata sicurezza dei dati), "responsabilizzazione" (il titolare del trattamento deve osservare la disciplina normativa in tema di protezione dei dati personali ed essere in grado di comprovare tale osservanza).

GOIRC, quale titolare del trattamento, mette in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento.

GOIRC mette in atto misure adeguate a tutelare i dati personali fin dalla progettazione e tramite impostazioni predefinite.

A tal fine, GOIRC tiene conto: a) della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento; b) dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche; c) dello stato dell'arte e dei costi di attuazione.

#### **ART. 10 - CONFLITTO DI INTERESSI ED ATTIVITA' ESTERNE.**

I destinatari del presente Codice devono astenersi dal partecipare a qualsiasi attività che possa generare conflitto d'interessi.

Il personale di GOIRC deve astenersi dall'intrattenere rapporti professionali esterni con soggetti nei confronti dei quali abbia un obbligo di imparzialità. Ove ricorrano queste ipotesi e, in ogni caso, qualora sussistano ragioni di opportunità e di convenienza, il personale si astiene da attività o rapporti implicanti conflitto di interessi, informandone, senza indugio, il suo diretto superiore.

Il personale, fermo restando quanto dettato dalle norme contrattuali sul tema, non deve assumere incarichi esterni in società o imprese commerciali i cui interessi siano direttamente, o anche solo potenzialmente, contrastanti o interferenti con quelli di GOIRC.

Il personale non accetta incarichi di collaborazione con persone od organizzazioni che abbiano, o abbiano avuto nel biennio precedente, un interesse economico in decisioni o attività inerenti l'ufficio.

A tal fine, il personale di GOIRC, onde consentire la valutazione di eventuali incompatibilità, informa il diretto superiore di attività ed incarichi a lui affidati o comunque attribuiti.

Il personale non accetta da soggetti diversi da GOIRC retribuzioni o altre utilità per prestazioni alle quali è comunque tenuto nello svolgimento dei propri compiti d'ufficio.

Il personale non sollecita ai propri diretti superiori il conferimento di incarichi remunerati.

## **ART. 11 - POLITICHE DEL PERSONALE.**

La selezione del personale da assumere è effettuata in base alla corrispondenza dei profili dei candidati rispetto alle esigenze aziendali e nel pieno rispetto del principio di pari opportunità fra tutti i soggetti interessati, escludendo ogni forma di favoritismo.

All'atto della costituzione del rapporto di lavoro ogni collaboratore riceve accurate informazioni relative a: caratteristiche della funzione e delle mansioni da svolgere; elementi normativi e retributivi, come regolati dal contratto collettivo nazionale di lavoro; norme e procedure da adottare per la propria attività lavorativa. Nella gestione del personale, GOIRC evita qualsiasi forma di discriminazione e offre a tutti i lavoratori le medesime opportunità, in modo che ciascuno possa godere di un trattamento equo basato su criteri di merito. GOIRC adotta criteri basati sulla corrispondenza fra profilo atteso e profilo posseduto (ad esempio per le promozioni) e/o su valutazioni di merito e di competenza (ad esempio per gli incentivi).

I responsabili utilizzano e valorizzano tutte le professionalità presenti nella struttura favorendone lo sviluppo e la crescita e prevedendo momenti di

partecipazione a discussioni e decisioni funzionali al conseguimento degli obiettivi aziendali.

GOIRC mette a disposizione di tutti i collaboratori strumenti informativi e formativi, con l'obiettivo di valorizzare le specifiche competenze e la professionalità del personale.

GOIRC riserva particolare attenzione alla formazione sia del personale neoassunto sia del personale già operativo nell'Associazione.

GOIRC adotta, nell'esercizio dell'impresa, le misure che, correlate alla particolarità del lavoro, all'esperienza ed alla tecnica, sono idonee a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro.

GOIRC, perseguendo l'obiettivo di creare e mantenere un ambiente di lavoro sereno e produttivo, predispone misure organizzative e procedure interne, di controllo e verifica, volte a prevenire molestie, turbative o condizionamenti psicologici nelle relazioni di lavoro, interne ed esterne all'Ente stesso.

GOIRC vieta espressamente comportamenti (personalismi, favoritismi, protagonismi, competizioni) idonei a determinare, direttamente o indirettamente, situazioni pregiudizievoli per l'Associazione e per tutti i destinatari. In particolare, vieta: atteggiamenti intimidatori, ostili o di isolamento nei confronti di singoli o gruppi di lavoratori; ingiustificate ingerenze nell'esecuzione di prestazioni lavorative altrui; limitazioni a prospettive di lavoro individuali a causa di interessi personali; coercizioni, psicologiche o fisiche, che limitino l'autonomia e la dignità di singoli o gruppi di lavoratori. Vieta, infine, tutte le forme di molestia, anche sessuale, e la subordinazione di decisioni aziendali e/o di atti dovuti, relativi alla carriera o all'attività di un prestatore di lavoro, all'accettazione di favori e/o prestazioni personali non volute o gradite che ledano la dignità e la serenità del destinatario, pregiudicandone l'espressione lavorativa.

GOIRC promuove e garantisce, attraverso la condivisa applicazione dei principi etici e di comportamento enunciati nel presente Codice, un ambiente di lavoro sereno, coeso e costruttivo. Il personale ed i collaboratori esterni devono contribuire alla creazione e conservazione di un ambiente di lavoro rispettoso della sensibilità degli altri e dei valori della produttività e della capacità lavorativa.

E' vietato, pertanto, prestare servizio sotto gli effetti di abuso di sostanze alcoliche o stupefacenti o di sostanze di analogo effetto, assumere comportamenti e/o abitudini che possano cagionare qualsiasi forma di dipendenza ovvero pregiudicare o limitare le attività lavorative o aziendali e la serenità e produttività dell'ambiente di lavoro.

## **ART. 12 - PROFESSIONALITA' E DILIGENZA.**

Il personale deve garantire, in osservanza del principio di professionalità, *standard* di qualità professionale elevati e comunque funzionali alla diligente ed

efficace esecuzione di ogni prestazione ed alla correttezza e lealtà di ogni relazione.

I dirigenti, i dipendenti ed i collaboratori di GOIRC devono usare la massima diligenza in ogni azione svolta, soprattutto sotto il profilo contabile ed operativo, conformando la propria condotta al valore della ricerca continua della qualità del lavoro.

In particolare, il personale deve garantire il corretto e completo svolgimento di ogni mansione ed adottare un comportamento proattivo in termini di collaborazione lavorativa, aggiornamento professionale e miglioramento della *performance* di lavoro.

### **ART. 13 - CONTROLLO E RESPONSABILITA'.**

GOIRC promuove una cultura dell'organizzazione connotata dalla consapevolezza della necessità ed utilità dei controlli, esercitati e gestiti con riferimento ad ogni livello operativo.

GOIRC favorisce e diffonde una cultura del controllo "positiva" in ragione del contributo che i controlli e le verifiche apportano allo sviluppo ed all'efficienza aziendale.

Nessun controllo potrà determinare la violazione della legge vigente o della sfera individuale e personale né favorire atteggiamenti coercitivi, molesti o persecutori.

### **ART. 14 - TUTELA DEL PATRIMONIO AZIENDALE.**

Il personale è responsabile della protezione e della conservazione dei beni, fisici e immateriali, affidatigli per espletare i suoi compiti.

I beni e le risorse dell'Ente (strumenti di comunicazione, apparecchi telefonici, *personal computer*, mezzi di trasporto di GOIRC) sono assegnati al personale in ragione dell'attività lavorativa e devono essere utilizzati esclusivamente per gli scopi e per le esigenze di GOIRC e mai per scopi privati, senza espressa autorizzazione.

L'utilizzo di beni di GOIRC per scopi personali è consentito nei limiti e nelle situazioni di particolare necessità e comunque l'eventuale utilizzo a scopo personale non dovrà pregiudicare lo svolgimento del servizio.

Il personale osserva le norme volte alla protezione di dati personali, adottando condotte funzionali alla tutela dei principi di riservatezza, integrità e disponibilità dei dati personali e segnalando eventuali comportamenti integranti la commissione di reati informatici.

### **ART. 15 - TUTELA AMBIENTALE.**

GOIRC riserva particolare attenzione alle questioni ambientali, riducendo

al minimo i rischi ambientali e creando le condizioni per uno sviluppo sostenibile.

A tal fine, GOIRC adotta misure e strategie aziendali idonee a migliorare l'impatto ambientale delle proprie attività, nel rispetto della normativa vigente, tenendo conto delle norme tecniche e di esperienza e dello sviluppo della ricerca scientifica.

Sempre ai fini di tutela ambientale, GOIRC conforma la propria attività a criteri elevati di salvaguardia ambientale e, in particolare, provvede a:

- integrare progressivamente la tutela degli aspetti ambientali delle attività svolte con le strategie dell'Ente;
- attuare tutte le azioni necessarie ad assicurare il rispetto e l'adeguamento alle previsioni normative vigenti;
- aggiornare costantemente il personale sull'evoluzione legislativa e normativa in materia ambientale;
- sensibilizzare il personale sulle problematiche ambientali, al fine di pervenire ad elevati *standard* di professionalità.

#### **ART. 16 - RAPPORTI CON ASSOCIATI E UTENTI**

L'attività di GOIRC è volta alla soddisfazione ed alla tutela di associati e utenti nonché al miglioramento della qualità dei prodotti e dei servizi.

Nei rapporti con gli utenti è fatto obbligo al personale di GOIRC di:

- improntare lo stile di comportamento nell'ottica di un rapporto collaborativo e di elevata professionalità;
- fornire, con efficienza e cortesia, nei limiti delle previsioni contrattuali, servizi di qualità in linea con le ragionevoli aspettative degli utenti;
- fornire informazioni accurate ed esaurienti relative ai servizi forniti in modo tale da permettere agli associati e utenti di prendere decisioni consapevoli.

Nel rapporto con gli utenti GOIRC si ispira ai principi di disponibilità, qualità, trasparenza, chiarezza, completezza e sicurezza del servizio.

#### **ART. 17 - RAPPORTI CON I FORNITORI.**

GOIRC intende instaurare con i propri fornitori rapporti caratterizzati da reciproca lealtà, trasparenza e collaborazione.

La selezione dei fornitori deve effettuarsi garantendo la sussistenza dei seguenti presupposti, individuati in seguito ad una valutazione attenta ed obiettiva: utilità e convenienza in termini di prezzo e qualità; onestà ed integrità del fornitore; capacità del fornitore di garantire servizi di livello qualitativo adeguato; disponibilità di mezzi e strutture organizzative; competenza del fornitore e concreta possibilità di fidelizzazione; capacità del fornitore di cooperare con i dirigenti, dipendenti e collaboratori esterni di GOIRC;

osservanza degli obblighi di riservatezza.

La selezione dei fornitori, ove effettuata attraverso procedure ad evidenza pubblica, comporta, a carico di GOIRC, il rispetto rigoroso delle previsioni normative e regolamentari e la garanzia della parità di trattamento delle imprese proponenti nonché l'astensione dal compimento di qualsiasi trattamento preferenziale o di favore nei confronti di taluno dei fornitori.

La gestione dei rapporti con i fornitori deve effettuarsi assicurando la sussistenza dei seguenti presupposti: osservare le procedure interne per la selezione e la gestione dei rapporti con i fornitori; osservare le condizioni contrattualmente previste; condurre un dialogo corretto e leale con i fornitori; portare a conoscenza del Consiglio direttivo e degli Organi dell'Ente le eventuali criticità insorte con un fornitore in modo da consentirne la valutazione di eventuali conseguenze.

Qualora il fornitore, nello svolgimento della propria attività per GOIRC, adotti comportamenti non conformi alle norme ed ai principi del presente Codice Etico, l'Azienda può adottare opportuni provvedimenti tra i quali l'esclusione di eventuali, ulteriori collaborazioni.

#### **ART. 18 - RAPPORTI CON I COLLABORATORI.**

GOIRC deve selezionare i collaboratori esterni e gestirne il rapporto in base a questi criteri: selezionare solo persone e imprese qualificate e con buona reputazione; riferire tempestivamente all'Organo Amministrativo violazioni del Codice Etico da parte di collaboratori esterni; includere nei contratti di collaborazione esterna, qualora previsto nelle procedure, l'obbligazione, posta a carico del collaboratore esterno, di osservare i principi del Codice Etico.

#### **ART. 19 - RAPPORTI CON LE ALTRE ASSOCIAZIONI.**

L'Ente intende sviluppare il valore della condivisione e cooperazione operando secondo principi di correttezza, leale competizione e trasparenza nei confronti di tutti gli operatori presenti sul mercato.

GOIRC ritiene che la collaborazione ed il confronto siano i presupposti per la ricerca continua della qualità e per il miglioramento dei servizi dell'Ente.

GOIRC promuove e tutela il valore della concorrenza leale, astenendosi da comportamenti collusivi e/o di abuso.

#### **ART. 20 - RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE.**

Nei rapporti che il personale di GOIRC intrattiene, anche tramite terzi, con la Pubblica Amministrazione (di seguito P.A.) devono essere rispettati i seguenti principi:

- i rapporti con la P.A. devono essere improntati al rispetto della legge;

- è fatto divieto di porre in essere comportamenti che, al fine di garantire uninteresse o vantaggio dell'Ente, siano tali da integrare fattispecie di reato;

- non è ammesso, né direttamente né indirettamente, né per il tramite di persona interposta, promettere o corrispondere denaro, doni, beni o altre utilità, sotto qualsiasi forma, né esercitare illecite pressioni, né promettere qualsiasi oggetto, servizio, prestazione o favore a dirigenti, funzionari o dipendenti della P.A., anche estere, o a loro parenti o conviventi per indurre la P.A. al compimento di atti nell'interesse o a vantaggio di GOIRC;

- non è consentito presentare dichiarazioni non veritiere a organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati oppure per conseguire concessioni, autorizzazioni, licenze o altri atti amministrativi;

- è fatto divieto di destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti, a scopi diversi da quelli per i quali sono stati assegnati;

- è fatto obbligo di verificare, con tempestività e diligenza, che quanto dichiarato e/o attestato nell'interesse di GOIRC sia veritiero e corretto.

## **ART. 21 - RAPPORTI CON LA COLLETTIVITA' E CON GLI ORGANI DI INFORMAZIONE.**

Ogni attività di informazione o comunicazione dev'essere veritiera, chiara, trasparente e tempestiva ed epurata da notizie non necessarie, non utili né pertinenti ovvero da dati "sensibili" o coperti da segreto industriale.

La gestione dei rapporti tra GOIRC e gli organi di informazione dev'essere svolta dagli organi e soggetti indicati nelle specifiche procedure interne ed in coerenza con la politica di comunicazione adottata dall'Ente.

La partecipazione, in nome dell'Associazione o in rappresentanza della stessa, a comitati ed associazioni di qualsiasi tipo, scientifici, culturali o di categoria, dev'essere preventivamente autorizzata ed ufficializzata.

## **ART. 22 - RAPPORTI CON LE ORGANIZZAZIONI POLITICHE E SINDACALI.**

GOIRC non eroga contributi a partiti, a comitati e organizzazioni politiche e sindacali, a loro rappresentanti e candidati, tranne quelli dovuti in base a normative specifiche.

Eventuali contributi, se dovuti, devono essere erogati in modo rigorosamente conforme alle leggi vigenti e correttamente registrati.

E' fatto divieto di tenere comportamenti finalizzati ad influenzare, direttamente o indirettamente, esponenti politici. In tal senso, l'Associazione si astiene dall'erogare contributi nei confronti di organizzazioni con le quali potrebbe nascere un conflitto d'interessi.

## **ART. 23 - RAPPORTI CON LE AUTORITA' PUBBLICHE DI VIGILANZA.**

GOIRC s'impegna ad effettuare, con tempestività, trasparenza, veridicità e completezza, tutte le comunicazioni previste dalla legge nei confronti delle Autorità Pubbliche di Vigilanza cui è sottoposta, non operando alcun ostacolo all'esercizio delle funzioni delle predette Autorità.

In particolare, è fatto divieto di:

esporre, in tali comunicazioni e nella documentazione trasmessa, fatti non rispondenti al vero oppure occultare fatti concernenti la situazione economica, patrimoniale o finanziaria di GOIRC;

- effettuare le comunicazioni previste dalla legge nonché la trasmissione deidati e documenti specificamente richiesti da predette Autorità aventi contenuto contrario al suddetto obbligo di tempestività, trasparenza, veridicità e completezza;

- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle Autorità pubbliche di vigilanza, anche in sede di ispezione (rifiuti pretestuosi, comportamenti ostruzionistici o di mancata collaborazione);

- omettere le comunicazioni dovute alle predette Autorità.

## **ART. 24 - MISURE DISCIPLINARI**

Il presente Codice Etico costituisce specifico dovere per tutti i destinatari e le norme in esso contenute rappresentano disposizioni di servizio, in quanto tali vincolanti e obbligatorie, in aggiunta a tutte le altre disposizioni regolamentari e di servizio.

Ogni eventuale violazione sarà valutata sulla base del Sistema sanzionatorio adottato dall'Azienda e delle vigenti disposizioni disciplinari.

Fermo quanto sopra, ogni violazione del presente Codice sarà inoltre valutata in relazione alle vigenti disposizioni di legge e contrattuali quale responsabilità civile, penale e amministrativa e le sanzioni inflitte saranno proporzionali alla gravità della violazione.

Nell'ambito dei rapporti con i fornitori/committenti, saranno inserite clausole risolutive espresse in relazione ai comportamenti che risultino contrari ai principi del presente Codice.

Tutti i soggetti interessati, interni ed esterni, sono tenuti a segnalare per iscritto, le eventuali inosservanze del Codice. L'Ente si impegna a tutelare gli autori delle segnalazioni contro eventuali ritorsioni cui possono andare incontro, e a mantenerne riservata l'identità, salvi i diritti di terzi e gli specifici obblighi di legge.

In caso di accertata infrazione, GOIRC adotta i provvedimenti disciplinari

e/o le azioni legali che si rendano necessarie.

**ART. 25 - PROCEDURE DI ATTUAZIONE,  
CONTROLLO, DIFFUSIONE E AGGIORNAMENTO.**

Tutti i destinatari del Codice Etico si assumono le responsabilità della propria condotta. Nessuno di essi ha l'autorità per chiedere la violazione o la deroga del Codice Etico.

GOIRC provvede alla comunicazione e diffusione del Codice Etico, promuovendo, tra l'altro, programmi di formazione specifica di dirigenti e dipendenti.

GOIRC curerà l'aggiornamento e l'attuazione del Codice Etico, assicurandone l'effettività e la concreta applicazione; esaminerà le eventuali e potenziali violazioni del Codice Etico, promuoverà le opportune verifiche ed i più idonei rimedi.

Le comunicazioni con l'esterno e le relazioni con gli organi di informazione sono tenute esclusivamente dai soggetti all'uopo designati negli ordini di servizio, nelle deleghe o in altre disposizioni organizzative sopravvenute, con il supporto degli uffici che curano la comunicazione ed i rapporti con l'esterno, al fine di uniformare gli indirizzi aziendali.

Potranno essere concesse deroghe alla regola suindicata con l'autorizzazione di uno dei soggetti di cui al primo comma.

I destinatari del presente Codice devono astenersi da dichiarazioni pubbliche che ledano l'immagine di GOIRC.

Il dipendente, qualora sollecitato dai mezzi di comunicazione, deve indirizzare ogni richiedente agli organi competenti.

## **4. SISTEMA GENERALE DI PREVENZIONE.**

### **4.1 Principi generali di comportamento.**

**Il presente Modello 231 consta di un “Sistema generale” di prevenzione e di specifiche “Procedure operative” aventi carattere integrativo del Sistema generale.**

**L’osservanza del Sistema generale di prevenzione costituisce un primo presidio per l’efficace prevenzione dei reati ex D.Lgs. 231/01.**

Tutte le operazioni “sensibili” o a “rischio reato” devono essere svolte conformandosi alla normativa vigente, alle norme del Codice Etico, alle procedure del presente Modello 231 e agli altri Sistemi e Procedure dell’Ente.

**GOIRC deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure) improntati ai principi generali di:**

- conoscibilità all’interno dell’Ente;
- formalizzazione e chiarezza di contenuti;
- trasparente e formale delimitazione dei ruoli;
- rotazione delle cariche e funzioni, ove possibile.

**Le Procedure interne devono essere caratterizzate dai seguenti elementi:**

- separatezza, all’interno di ciascun processo, tra, da una parte, il soggetto che lo inizia, lo esegue e lo conclude e, dall’altra, il soggetto che lo controlla;
- traccia scritta di ciascun passaggio rilevante del processo;
- adeguato livello di formalizzazione;
- predisposizione delle comunicazioni associative in base a predefiniti criteri di responsabilità, tempi e modalità;
- adozione di procedure chiare e formalizzate per l’attività di formazione del bilancio e dei documenti similari.

**Principi di controllo generale finalizzati alla prevenzione dei reati presupposto:**

- sistema di deleghe e procure formalizzato;
- sistema normativo interno (policy, procedure, istruzioni operative, ecc.) che definisca ruoli e responsabilità nell’ambito delle attività aziendali più esposte a rischio;
- previsione della segregazione dei compiti;
- applicazione, ove possibile, della rotazione delle cariche;
- tracciabilità ex post dei processi;

- archiviazione della documentazione rilevante;
- applicazione di presidi di controllo specifici adeguati a prevenire la commissione dei reati;
- formazione a favore delle risorse che operano nell'ambito delle attività sensibili;
- definizione di un sistema sanzionatorio in caso di violazione del Modello 231 e delle procedure aziendali;
- previsione di attività di audit e monitoraggio;
- attivazione di un sistema di comunicazione e segnalazione (cd. whistleblowing).

**E' vietato, in via diretta, ai Ruoli/Funzioni dell'Ente (amministratori, dirigenti e dipendenti) e, tramite apposite clausole contrattuali, ai Collaboratori esterni e Partners, di porre in essere:**

- comportamenti tali da integrare le fattispecie di reato di cui al D.Lgs.n. 231/01;
- comportamenti che, sebbene risultino tali da non integrare di per sé fattispecie di reato di cui al D.Lgs. n. 231/01, possano potenzialmente diventarlo;
- qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle ipotesi di reato di cui al D.Lgs. n. 231/01.

**E' altresì vietato, con specifico riferimento ai rapporti con la P.A. e con Attività di Vigilanza e Controllo ed alle relative attività sensibili, porre in essere le seguenti attività:**

- presentare dichiarazioni non veritiere a organismi pubblici nazionali o comunitari, al fine di conseguire erogazioni pubbliche con tributi 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 erano destinate;  
indurre in errore i soci o il pubblico circa la situazione economica, patrimoniale e finanziaria, al fine di trarre un ingiusto profitto per GOIRC.

#### **4.2 Segnatamente, oggetto dell'attività di prevenzione sono i seguenti processi:**

- 4.2.1 gestione degli acquisti di beni e servizi;
- 4.2.2 selezione e gestione del personale;

4.2.3 gestione delle operazioni sul patrimonio dell'Associazione;

4.2.4 gestione dei flussi finanziari.

**GOIRC, con riferimento a tali processi, osserva i seguenti controlli finalizzati alla prevenzione dei reati – presupposto.**

#### **4.2.1 Gestione degli acquisti di beni e servizi**

Ai fini della prevenzione dei reati di cui al D.Lgs. 231/01, nell'ambito della gestione degli acquisti di beni e servizi, GOIRC adotta i seguenti presidi di controllo:

- sottoporre i fornitori ad un processo di qualifica;
- effettuare audit/visite di verifica ai fornitori rilevanti;
- definire precise regole per il subappalto dei lavori affidati;
- garantire che la selezione dei fornitori sia ispirata a criteri e principi di trasparenza, pari opportunità di accesso, professionalità, affidabilità ed economicità;
- creare una specifica anagrafica fornitori (cd. *vendor list*) onde raccogliere e censire tutte le informazioni critiche e significative degli stessi, anche nel medio/lungo periodo;
- garantire un'adeguata segregazione tra le funzioni nell'ambito del processo di selezione del fornitore/consulente;
- procedere, per gli acquisti di importo superiore ad una determinata soglia, alla selezione del fornitore attraverso il confronto di più offerte, salvo i casi particolari che dovranno essere opportunamente motivati;
- verificare l'esistenza e la vigenza delle autorizzazioni necessarie;
- garantire la tracciabilità, anche per il tramite di specifici sistemi informativi, dell'iter di selezione e qualifica del fornitore, attraverso la formalizzazione ed archiviazione della relativa documentazione;
- valutare, periodicamente, le prestazioni dei fornitori;
- verificare la rispondenza della merce o servizio ricevuti rispetto a quanto effettivamente ordinato;
- regolare l'approvvigionamento di beni e servizi attraverso contratti ovvero ordini scritti, con chiara indicazione del prezzo del bene o del corrispettivo del servizio;
- vietare l'effettuazione di qualsiasi operazione commerciale o finanziaria, sia in via diretta che per interposta persona, con soggetti (persone fisiche o giuridiche) i cui nominativi siano contenuti nelle liste disponibili presso la Banca d'Italia o altre Autorità, o da soggetti da questi ultimi controllati, quando tale rapporto di controllo sia noto;
- vietare l'effettuazione di prestazioni in favore di consulenti e fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi e riconoscere loro compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale.

**Ai fini della gestione di acquisti di beni e servizi, comprese le consulenze, GOIRC**

**acquisisce e valuta i seguenti documenti, dichiarazioni ed informazioni** che, messi a sistema, possano condurre alla decisione in ordine all'attivazione o meno della relazione, alla conclusione o meno di un'attività negoziale ed alla prestazione o ricezione della relativa prestazione/servizio:

- visura camerale;
- ultimi bilanci di esercizio;
- informazioni sugli organi di stampa e sul web;
- brochure commerciali;
- evidenza delle autorizzazioni necessarie per lo svolgimento delle attività;
- verifica (nei casi previsti) dell'iscrizione nelle whitelist antimafia

#### **4.2.2 Selezione e gestione del personale dipendente**

**4.2.2.1** Nell'ambito della selezione e gestione del personale dipendente, **GOIRC** adotta i seguenti controlli:

- garantire che la scelta dei candidati sia effettuata sulla base di considerazioni oggettive delle caratteristiche professionali e personali necessarie all'esecuzione del lavoro da svolgere evitando favoritismi di ogni sorta;
- verificare l'affidabilità del candidato e la relativa reputazione;
- garantire la segregazione del processo di selezione del personale;
- garantire la tracciabilità del processo di selezione formalizzando, tra gli altri, le motivazioni sulla scelta del candidato;
- assumere personale con regolare contratto di lavoro;
- verificare che gli orari di lavoro siano applicati nel rispetto della normativa vigente;
- assicurare che al momento dell'assunzione, sia consegnata al dipendente copia del Codice Etico e del Modello e che questi si impegni formalmente al pieno rispetto dei principi in essi contenuti;
- curare che siano assicurate all'interno dell'Ente condizioni di lavoro rispettose della dignità personale, delle pari opportunità e un ambiente di lavoro adeguato, nel rispetto della normativa contrattuale collettiva del settore e della normativa previdenziale, fiscale ed assicurativa;
- assicurare che la definizione delle condizioni economiche sia coerente con la posizione ricoperta dal candidato e le responsabilità/compiti assegnati;
- per il personale proveniente da paesi Extra-UE, verificare la validità del permesso di soggiorno ed il monitoraggio dello stesso nel corso della durata del rapporto di lavoro.

#### **4.2.2.2 Con specifico riferimento alla gestione delle consulenze esterne e degli incarichi professionali, GOIRC applica i seguenti principi di controllo:**

- deve essere prevista, per quanto possibile, l'esistenza di attori diversi operanti nelle differenti fasi del processo (in linea di principio, non vi deve essere identità tra chi richiede la

consulenza, chi la autorizza e chi esegue il pagamento della prestazione);

- devono essere previsti requisiti professionali, economici ed organizzativi a garanzia degli standard qualitativi richiesti (attestati dal consulente) e di meccanismi di valutazione complessiva del servizio reso;
- nell'impiego di consulenti esterni, nell'ambito della gestione dei rapporti con la Pubblica Amministrazione, devono essere previsti dei meccanismi di verifica preventiva della insussistenza di contemporanea collaborazione sulla stessa materia con le corrispondenti amministrazioni pubbliche (anche mediante auto-certificazione del consulente esterno);
- devono essere utilizzati idonei dispositivi contrattuali adeguatamente formalizzati;
- devono esistere – per quanto possibile - adeguati livelli autorizzativi per la stipulazione dei contratti.

#### **4.2.3 Gestione delle operazioni sul patrimonio dell'Associazione – predisposizione del bilancio.**

Con riferimento alla gestione delle operazioni sul patrimonio dell'Associazione, GOIRC

##### **4.2.3.1 implementa i seguenti presidi di controllo specifici:**

- determinazione dei criteri di selezione, stipulazione ed esecuzione di accordi di collaborazione con altri enti/associazioni/imprese;
  - trasparenza e tracciabilità degli accordi;
  - verifica della congruità economica di eventuali investimenti;
  - per ogni operazione il referente è opportuno predisponga la documentazione idonea a consentire all'Organo deliberante di valutarne la fattibilità e la convenienza strategica ed economica: (a) la descrizione quali-quantitativa del target (i.e. studio di fattibilità, analisi finanziarie, studi e statistiche sul mercato di riferimento, confronti fra diverse alternative di effettuazione dell'operazione); b) le caratteristiche ed i soggetti coinvolti nell'operazione; c) la struttura tecnica, le principali garanzie, gli accordi collaterali e la copertura finanziaria dell'operazione; d) le modalità di determinazione delle condizioni economiche dell'operazione e l'indicazione di eventuali consulenti esterni/intermediari/advisors coinvolti; e) l'impatto sulla situazione economica, finanziaria e patrimoniale prospettica; f) le valutazioni circa la congruità e la rispondenza all'interesse dell'Ente dell'operazione da deliberare.

##### **4.2.3.2 In merito alla predisposizione del Bilancio**

- devono essere adottate misure idonee a garantire che le operazioni contabili siano effettuate con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza e siano tempestivamente segnalate eventuali situazioni anomale
- chi fornisce informazioni alle unità gerarchicamente sovraordinate deve indicare i documenti o le fonti originarie dalle quali sono tratte ed elaborate le informazioni trasmesse, al fine di garantire la verificabilità delle stesse;
- deve essere previsto l'obbligo per il responsabile di funzione di fornire dati ed informazioni

alla eventuale società di revisione incaricata, accompagnando tale invio con una dichiarazione di veridicità e completezza delle informazioni trasmesse;

- qualora siano formulate richieste di variazione dei criteri di rilevazione, registrazione e rappresentazione contabile, le stesse devono essere formalizzate, motivate e adeguatamente comunicate alle Funzioni/Organi competenti.

#### **4.2.4 Gestione dei flussi finanziari.**

**Con riferimento alle attività di gestione dei flussi finanziari, GOIRC garantisce i seguenti presidi specifici:**

- prevedere controlli formali e sostanziali dei flussi finanziari e gli strumenti adeguati che garantiscono la tracciabilità delle relative movimentazioni;
- autorizzare alla gestione dei flussi finanziari solo soggetti previamente identificati e dotati di apposita procura;
- definire le funzioni coinvolte nella suddetta attività e le relative responsabilità;
- prevedere dei limiti all'utilizzo autonomo delle risorse finanziarie mediante la definizione di soglie quantitative coerenti con i ruoli e le responsabilità organizzative;
- utilizzare esclusivamente i canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione Europea o enti creditizi/finanziari situati in uno Stato extracomunitario che imponga obblighi equivalenti a quelli previsti dalle leggi sul riciclaggio e preveda il controllo del rispetto di tali obblighi;
- garantire che i pagamenti avvengano a fronte di fatture registrate, corredate dai relativi ordini e, in ogni caso, successivamente all'attestazione dell'avvenuta prestazione e all'autorizzazione del pagamento da parte della funzione richiedente il bene o il servizio;
- rispettare i limiti di utilizzo del denaro contante di cui alla normativa vigente;
- predisporre procedure adeguate a verificare la regolarità dei pagamenti, risultante dalla coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte;
- assicurare che tutte le disposizioni sui conti correnti bancari intestati all'Ente, nonché i pagamenti eseguiti con modalità differenti, siano adeguatamente documentate ed autorizzate secondo il sistema di deleghe dell'Ente.
- eventuali pagamenti ritenuti anomali devono essere segnalati al Consiglio Direttivo, agli organi di controllo e all'OdV.

### **4.3 GOIRC vieta espressamente le seguenti attività:**

- effettuare pagamenti per contanti per importi superiori ai limiti normativi o con mezzi di pagamento non tracciabili;
- effettuare pagamenti su conti correnti cifrati o conti correnti non intestati al fornitore nonché diversi da quelli previsti contrattualmente;
- effettuare pagamenti non adeguatamente documentati;
- ricevere pagamenti da soggetti che non abbiano nessun rapporto commerciale/contrattuale con l’Ente;
- creare fondi, o lasciar creare, fondi illeciti, occulti o comunque non regolarmente contabilizzati, tramite qualsiasi operazione o movimentazione finanziaria illecita, simulata, fittizia e/o non correttamente contabilizzata;
- effettuare trasferimenti di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore in euro o in valuta estera, quando il valore dell’operazione, anche frazionata, sia complessivamente pari o superiore al limite stabilito dalla normativa antiriciclaggio;
- emettere assegni bancari e postali che non rechino l’indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
- aprire conti o libretti di risparmio in forma anonima o con intestazione fittizia e utilizzare quelli eventualmente aperti presso Paesi esteri;
- effettuare bonifici senza l’indicazione della controparte;

- effettuare trasferimenti di denaro rispetto ai quali non vi sia piena coincidenza tra i destinatari/ordinanti i pagamenti e le controparti effettivamente coinvolte nelle transazioni;
- effettuare pagamenti o riconoscere compensi in favore di soggetti terzi che operino per conto dell'Associazione, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi.

**Il Sistema generale di prevenzione dei reati di cui al D.Lgs. n. 231/01 sopra esposto deve ritenersi integrato dai seguenti documenti aziendali: Codice Etico, Procedure operative specifiche nell'ambito di singole aree sensibili ed allegate al presente Modello 231, MOP (Modello Organizzativo Privacy) adottato dall'Ente,**

## 5. IL SISTEMA SANZIONATORIO

### 5.1 Introduzione

Presupposto essenziale per l'efficace attuazione del Modello 231 è l'adozione di un adeguato sistema sanzionatorio idoneo a prevenire i reati di cui al D.Lgs. n. 231/01. Infatti, l'art. 6 del D.Lgs. 231/01, comma 2 lett. e) esige che il modello organizzativo introduca un "sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello" stesso e il successivo art. 7, dedicato ai "soggetti sottoposti all'altrui direzione" e, quindi, ai lavoratori subordinati, ribadisce che l'efficace attuazione del modello richiede un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure individuate dal Modello.

Il Sistema sanzionatorio di GOIRC, quale misura tanto di deterrenza generale quanto di efficacia sanzionatoria, conferma la ferma intenzione dell'Associazione di non tollerare condotte suscettibili di integrare o agevolare la commissione dei reati presupposto.

Lo Statuto di GOIRC impegna le Unità aderenti i Soci ad accettare e rispettare, senza riserve, ed a tutti gli effetti, le disposizioni contenute nello stesso e negli eventuali regolamenti, nonché le deliberazioni dei competenti organi dell'Associazione.

**Il presente Modello costituisce un regolamento associativo vincolante.**

### 5.2 I soggetti destinatari e le condotte rilevanti

Sono ritenuti soggetti sanzionabili le persone riconducibili al personale dipendente (di qualsiasi categoria, anche dirigente) che pongano in essere condotte, commissive e/o omissive, in violazione:

- A. delle singole regole comportamentali sancite nel presente Modello 231 e nel Codice Etico;
- B. delle Procedure aziendali e delle disposizioni di servizio dell'Associazione.

In particolare, sono sanzionabili i seguenti soggetti: i lavoratori dipendenti (con qualsiasi contratto), dirigenti, amministratori, consulenti, revisori, componenti del collegio sindacale o dell'OdV, consulenti esterni.

### 5.3 Il potere sanzionatorio - Condizioni e modalità di esercizio

**I provvedimenti sanzionatori vengono adottati:**

- a) in seguito a valutazioni puntuali quanto alla gravità della condotta contestata ed alla sussistenza dello specifico elemento soggettivo, colposo e/o doloso;

- b) al termine di procedure disciplinari attivate mediante contestazione e concluse formalmente, nel rispetto, innanzitutto, dell'art. 7 della legge n. 300/70, fatto salvo il "richiamo verbale", contestabile anche nella sola forma orale;
- c) attraverso le modulistiche e le prassi già presenti in GOIRC;
- d) indipendentemente dall'eventuale instaurazione di procedimenti penali, comunque esperibili, derivanti dai fatti oggetto di contestazione che siano idonei ad integrare anchefattispecie di reato.

Il Consiglio Direttivo (o i suoi delegati) dispone della discrezionalità utile ad individuare, ricorrendone le condizioni di legge in merito alle presunte violazioni, la sanzione da applicare alle singole condotte, applicando le norme, disposizioni e procedure pertinenti al caso di specie; ove sia riscontrata la violazione a carico dell'organo amministrativo, la decisione verrà adottata dall'assemblea.

In particolare, il Consiglio Direttivo:

- nei casi di minore gravità, intima al trasgressore di non ripetere il comportamento, ammonendolo circa le conseguenze più gravi in caso di reiterazione;
- nei casi di maggiore gravità, ne dispone l'espulsione o la revoca del mandato;
- l'espulsione è prevista, a maggior ragione, in caso di commissione o tentata commissione di illecito penale; in questa ultima ipotesi resta ferma la possibilità di denunciare il fatto alla Magistratura penale.

## **6. ORGANISMO DI VIGILANZA: IMPLEMENTAZIONE, FUNZIONAMENTO E STATUTO**

### **Premessa.**

L'Organismo di Vigilanza (di seguito OdV) è presupposto indefettibile per l'efficace attuazione del Modello 231 di GOIRC e per evitare le sanzioni a carico dell'Ente in caso di commissione degli illeciti.

Il corretto svolgimento dell'attività di vigilanza costituisce presupposto fondamentale per il rispetto del D.Lgs. 231/01 e per l'effettiva validità esimente del Modello 231.

Il D.Lgs. n. 231/01 prevede, infatti, quali condizioni per la concessione dell'esimente dalla responsabilità amministrativa:

- che sia affidato ad un organismo dell'Ente dotato di autonomi poteri, di iniziativa e di controllo, il compito di vigilare sul funzionamento e sull'osservanza del Modello 231 e di curarne l'aggiornamento;
- che non vi sia stata, da parte dell'OdV, omessa o insufficiente vigilanza.

### **6.1 Costituzione, nomina e composizione dell'OdV.**

Tenuto conto della natura, delle finalità e delle sue caratteristiche, GOIRC individua, quale struttura idonea ad attuare efficacemente il Modello 231, un Organismo di Vigilanza, dotato di poteri di iniziativa e controllo, ritenuto idoneo a soddisfare:

- i requisiti di continuità di azione, agevolando i flussi informativi;
- i requisiti di indipendenza, autonomia e professionalità;
- la fluidità e tempestività dei flussi informativi.

L'OdV è nominato dal Consiglio Direttivo e resta in carica per la stessa durata del Consiglio.

La nomina avverrà con una proposta scritta contenente l'indicazione delle funzioni da svolgere, obblighi e responsabilità, durata dell'incarico, cause di revoca/sospensione/decadenza del compenso e del budget messo a sua disposizione dall'Ente.

Detta proposta viene assoggettata, sempre per iscritto, al soggetto nominato.

Al momento dell'accettazione dell'incarico, l'OdV dichiara per iscritto e sotto la propria responsabilità, al Consiglio Direttivo, l'insussistenza di cause di incompatibilità.

## **6.2 Presupposti e principi applicativi.**

GOIRC, in quanto associazione di piccole dimensioni, senza scopo di lucro, adotta, in ragione della sua struttura organizzativa e dei suoi processi sensibili, un Modello di gestione semplificato e favorisce la nomina di un OdV monocratico.

Pertanto, al momento della stesura del presente MOG 231, l'OdV di GOIRC è monocratico e non ha alcun rapporto di parentela o a contenuto economico con i membri del Consiglio Direttivo.

I principi e le regole che seguono, relativi al funzionamento dell'OdV, sono applicabili compatibilmente al carattere monocratico dell'OdV.

L'Ente potrà, ove lo ritenga opportuno, e ne sussistano le condizioni, nominare un OdV a composizione collegiale.

I principi di seguito elencati e descritti costituiscono al contempo:

- a) requisiti soggettivi dei componenti dell'OdV;
- b) presupposti indefettibili per l'efficace funzionamento del Modello 231.

### **Indipendenza dell'OdV.**

Al fine di garantirne l'indipendenza:

- In caso di nomina di esperti esterni all'Associazione, all'OdV viene riconosciuto, dall'Organo Amministrativo, un compenso, in ragione delle responsabilità assunte, della preparazione professionale richiesta e del grado di impegno esigibile;
- l'importo del compenso deve essere adeguato a consentire la normale operatività dell'OdV ed impiegato esclusivamente per l'esercizio delle funzioni proprie dell'OdV;
- si applicano all'OdV, ove compatibili, le disposizioni di cui all'art. 2399 c.c. in ordine alle condizioni di ineleggibilità e decadenza del Collegio Sindacale.

### **Autonomia dell'OdV.**

Al fine di garantirne l'autonomia:

- all'OdV sono riconosciuti poteri di indagine e di spesa; in particolare, i poteri di indagine sono di ampiezza e rilevanza tali da assicurare l'efficacia delle attività svolte dall'OdV;

- l'OdV deve avere libero accesso presso tutte le funzioni aziendali, senza necessità di consenso preventivo, onde ottenere documenti, informazioni, notizie o dati ritenuti necessari per lo svolgimento dei compiti previsti dal D.Lgs. 231/01;
- le attività dell'OdV non devono essere preventivamente autorizzate da nessun organo;
- l'OdV ha accesso a tutte le informazioni relative all'Ente, anche quelle su supporto informatico, e può chiedere direttamente informazioni a tutto il personale;
- la mancata collaborazione con l'OdV costituisce un illecito disciplinare.

### **Professionalità dell'OdV**

Qualora i componenti dell'OdV Collegiale o il singolo OdV monocratico non possiedano adeguate competenze, necessarie per lo svolgimento di attività aziendali in settori specialistici, sarà possibile incaricare consulenti esterni.

I componenti dell'OdV Collegiale e/o l'OdV monocratico e/o il suo Consulente tecnico, in possesso, preferibilmente, di laurea magistrale, sono scelti tra soggetti particolarmente qualificati e dispongono di adeguate competenze in ambito giuridico, amministrativo-contabile e di controllo interno e di gestione dei rischi (ad es.: avvocati in ragione della finalità penal-preventiva del modello organizzativo; commercialisti con particolare riguardo alla prevenzione dei reati societari, tributari o doganali; ingegneri, soprattutto per reati in materia di salute e sicurezza sul lavoro).

E' titolo preferenziale il possesso di una comprovata e pluriennale esperienza certificata e documentata, in posizione di rilievo funzionale.

**Onorabilità dell'OdV**, garantita da specifiche cause di ineleggibilità dei componenti e di incompatibilità alla permanenza nella carica, di seguito specificate:

- una delle circostanze descritte nell'art. 2382 c.c.;
- una delle situazioni in cui può essere compromessa l'autonomia e l'indipendenza del componente;
- avvio di indagine nei suoi confronti su reati menzionati dal D.Lgs. 231/01;
- sentenza di condanna o di patteggiamento, anche non definitiva, per aver compiuto uno dei reati sanzionati dal D. Lgs. 231/01, o l'interdizione, a titolo di sanzione, dalla titolarità di cariche pubbliche o da uffici direttivi di persone giuridiche;
- allorché sia coniuge, parente o affine entro il secondo grado, ovvero socio in affari, di qualunque soggetto sottoposto al suo controllo nonché abbia interessi in comune o in contrasto con lo stesso;

- allorché svolga altra attività e/o incarichi (compresi quelli di consulenza, rappresentanza, gestione e direzione) per conto dell'Ente o semplicemente in contrasto con esso;
- allorché venga dichiarato interdetto, inabilitato o fallito;
- allorché venga condannato, con sentenza irrevocabile ai sensi dell'art. 648 c.p.p.: per fatti connessi allo svolgimento del suo incarico; per fatti che incidano significativamente sulla sua moralità professionale; per fatti che comportino l'interdizione dai pubblici uffici, dagli uffici direttivi delle imprese e delle persone giuridiche, da una professione o da un'arte nonché incapacità di contrattare con la P.A. o, in ogni caso, per avere commesso uno dei reati-presupposto di cui al D.Lgs. 231/01.

L'Organismo di Vigilanza cessa il suo ruolo per rinuncia, sopravvenuta incapacità, morte o revoca.

Il componente dell'Organismo di Vigilanza o l'OdV monocratico possono essere revocati:

- in caso di inadempienze reiterate ai compiti ovvero inattività ingiustificata;
- in caso di lavoro sleale o non corretto tale da non garantire l'indipendenza di giudizio;
- in caso di intervenuta irrogazione, nei confronti di GOIRC, di sanzioni interdittive, a causa dell'inattività del o dei componenti;
- quando siano riscontrate violazioni del Modello 231 da parte dei soggetti obbligati e vi sia altresì inadempimento nel riferire tali violazioni e nella verifica dell'idoneità e dell'efficace attuazione del Modello al fine di proporre eventuali modifiche;
- qualora subentri, dopo la nomina, una delle cause di ineleggibilità di cui sopra;
- in caso di violazioni del presente Modello 231.

La revoca è deliberata dal Consiglio direttivo.

In caso di rinuncia, sopravvenuta incapacità, morte o revoca del componente effettivo dell'O.d.V. o dell'OdV monocratico, GOIRC adotterà, senza indugio, le decisioni del caso.

### **6.3 L'attività dell'OdV: funzioni e poteri.**

In linea generale, all'OdV di GOIRC è affidato il compito di vigilare:

- sulla reale efficacia e sull'effettiva capacità del Modello 231 di prevenire, in relazione alla struttura aziendale, la commissione dei reati di cui al D.Lgs. n. 231/01;

- sull'osservanza delle prescrizioni del MOG 231 da parte dei destinatari, in relazione alle diverse tipologie di reati contemplate dal D.Lgs. n. 231/01;
- sull'opportunità di aggiornare il Modello 231 qualora si riscontrino esigenze di adeguamento dello stesso in relazione a modifiche dell'assetto aziendale o del dato normativo o a mutate condizioni socio-ambientali.

L'OdV, quale Garante del Modello, deve svolgere tutte le attività idonee a rendere efficiente ed operativo il Modello 231, così distinte:

- a) attività di Vigilanza sull'attuazione del Modello 231;
- b) attività di Aggiornamento del Modello 231;
- c) attività di Formazione in merito al Modello 231.

#### **a) Attività di Vigilanza sull'attuazione del Modello 231.**

**L'attività di vigilanza deve essere svolta rispettando i seguenti requisiti di prestazione:**

##### **- Continuità d'azione.**

Al fine di garantire l'efficace e costante attuazione del Modello 231, l'Organismo di Vigilanza opera senza soluzione di continuità.

Le attività dell'OdV devono svolgersi in modo continuativo, ancorché periodico, e senza interruzione, indipendentemente dalla variazione della composizione dell'Organismo.

##### **-Tracciabilità.**

L'OdV è tenuto a curare la conservazione e la tracciabilità della documentazione inerente le attività svolte, anche al fine di comprovare la continuità di azione.

Le verifiche vengono effettuate tramite un approccio sistematico che consenta a chiunque di pervenire alle medesime conclusioni in modo da garantire, all'occorrenza, un'agevole ricostruzione dei fatti *ex post*.

##### **-Riservatezza.**

L'OdV è tenuto alla massima riservatezza ed al segreto professionale in ordine alle informazioni e notizie ricevute nell'espletamento dell'attività ed ogni informazione in possesso dell'OdV viene trattata in conformità al Reg. UE 2016/679 ed al D.Lgs. n. 196/03, come modificato dal D.Lgs. n. 101/18.

##### **-Obiettività.**

L'OdV conduce le proprie attività con obiettività, autonomia, indipendenza ed imparzialità ovvero in assenza di pregiudizi ed interessi personali.

##### **-Efficacia.**

L'Organismo garantisce un corretto ed efficace livello di vigilanza sull'adeguatezza, sul funzionamento e sull'osservanza del Modello 231 nonché sull'aggiornamento dello stesso.

L'OdV dispone di ampi ed effettivi poteri di indagine e segnalazione e può avvalersi, sotto la sua diretta sorveglianza e responsabilità, dell'analisi di tutte le strutture dell'Associazione ovvero di consulenti esterni.

#### **-Adeguatezza.**

All'OdV sono formalmente assegnati poteri idonei allo svolgimento della propria attività (ad es., accesso alla documentazione aziendale ed alle strutture aziendali) al fine di garantire la prevenzione dei reati e l'autonomia d'azione.

#### **-Tutela.**

L'OdV ha il dovere di agire assumendo tutte le cautele necessarie al fine di garantire i c.d. *whistleblowers* da ogni forma di penalizzazione, ritorsione o discriminazione.

#### **- Correttezza.**

L'OdV si astiene dal ricercare e/o utilizzare informazioni riservate per scopi non conformi alle funzioni proprie dell'Organismo.

#### **- Cooperazione con gli organi di controllo.**

Lo scambio di informazioni e la fattiva collaborazione con gli altri attori del sistema di controllo è requisito indispensabile per il proficuo svolgimento dell'attività di vigilanza.

In particolare, GOIRC attuerà una stretta collaborazione ed una frequente integrazione tra l'OdV ed i referenti interni competenti ai fini del proficuo scambio di informazioni e della condivisione delle attività di controllo, consentendo all'OdV di acquisire dai referenti interni competenti informazioni e documenti utili per lo svolgimento delle attività di verifica e di valutazione del sistema generale dei controlli.

#### **Nell'ambito delle attività di vigilanza, l'Organismo è tenuto ad effettuare i seguenti interventi, indicati e descritti a titolo non esaustivo:**

- verifiche sul rispetto del Modello 231, sui protocolli comportamentali e sulle procedure in esso richiamate, da parte di tutti i destinatari;
- controlli sulle operazioni di gestione finanziaria e di tesoreria, al fine di evitare la costituzione di fondi neri o riserve occulte;
- verifiche periodiche sulle operazioni di maggior rilievo (ad es., per valore economico, coinvolgimento della P.A., ecc.);
- controlli in caso di ispezioni o accertamenti della P.A.;
- verifiche sulle regolarità formali richiamate dal Modello 231 e sull'invio dei flussi

informativi all'OdV; in particolare, i flussi informativi previsti nelle singole Procedure Operative;

L'OdV dovrà evitare, per quanto possibile, di interferire con i processi decisionali aziendali, ma dovrà intervenire prontamente, con i mezzi a sua disposizione per prevenire ogni comportamento che sia in contrasto con il presente MOG 231.

#### **b) Attività di aggiornamento del Modello.**

**Nell'ambito dell'attività di aggiornamento, l'OdV è tenuto ad eseguire i seguenti interventi, indicati e descritti a titolo non esaustivo:**

- condurre ricognizioni dell'attività aziendale al fine di individuare ed aggiornare le aree di attività a rischio reato nell'ambito del contesto aziendale;
- individuare e valutare l'opportunità dell'inserimento di clausole risolutive nei contratti con consulenti, collaboratori, *partner* contrattuali e terzi che intrattengono rapporti con GOIRC, nell'ambito delle attività aziendali esposte alla commissione dei reati di cui al D.Lgs.231/01 e provvedere all'eventuale modifica/integrazione delle clausole stesse;
- predisporre la documentazione organizzativa interna idonea al funzionamento del Modello 231, contenente istruzioni, chiarimenti o aggiornamenti;
- sollecitare il Consiglio direttivo per l'attivazione delle strutture aziendali competenti, nell'ipotesi in cui si renda necessario e/o opportuno effettuare l'elaborazione/modifica di Procedure Operative e di controllo che regolamentino lo svolgimento delle attività.

#### **c) Attività di formazione ed informazione.**

**Nell'ambito delle attività di formazione ed informazione l'OdV è tenuto ad effettuare i seguenti interventi, indicati e descritti a titolo non esaustivo:**

- promuovere idonee iniziative per la diffusione della conoscenza e della comprensione del Modello 231;
- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello 231;
- attuare, in conformità al Modello 231, un efficace flusso informativo che consenta all'OdV di riferire agli organi sociali competenti;
- promuovere la conoscenza dei principi contenuti nel Codice Etico e la loro traduzione in comportamenti coerenti da parte dei diversi attori aziendali individuando, con il supporto delle strutture societarie competenti, gli interventi formativi e di comunicazione più opportuni nell'ambito dei relativi piani annuali.

#### **6.4 Modalità di svolgimento dell'attività.**

**L'OdV svolge la propria attività, con diligenza, tempestività, trasparenza e riservatezza, osservando le seguenti modalità operative:**

- formalizza i propri controlli e verbalizza le proprie riunioni;
- registra, archivia e custodisce le copie dei verbali;
- allega ai propri verbali i resoconti delle attività di verifica e di controllo finalizzate all'attuazione del Modello 231;
- svolge attività di verifica direttamente, o tramite altri soggetti, anche terzi, appositamente incaricati di eseguire le istruzioni impartite dall'Organismo;
- redige, in seguito alle verifiche, una breve relazione, contenente i rilievi emersi, con separata indicazione delle carenze e delle eventuali integrazioni da adottare.

#### **6.5 Flussi informativi e reporting**

Presupposto indefettibile per l'efficace funzionamento dell'OdV e del Modello 231 è un adeguato sistema di disciplina di flussi informativi "provenienti" dall'OdV ed "indirizzati" all'OdV.

A tal fine, l'OdV istituisce uno specifico mezzo di comunicazione (una casella di posta elettronica deputata) idoneo a garantire:

- la "confidenzialità" di quanto segnalato, evitando eventuali atteggiamenti ritorsivi nei confronti del segnalante;
- la "bidirezionalità" dei flussi informativi che assicurino la ricezione degli stessi verso l'OdV ed il relativo riscontro indirizzato dall'OdV verso il segnalante.

**6.5.1 I flussi informativi diretti all'ODV si distinguono in:**

- a) flussi informativi "predefiniti", aventi ad oggetto le informazioni provenienti dalle figure aziendali che gestiscono le attività sensibili di GOIRC;
- b) flussi informativi, attivati al verificarsi di "particolari eventi", relativi a segnalazioni di violazioni, sospette o accertate di reati-presupposto.

**I flussi informativi diretti all'OdV provengono dai seguenti soggetti:**

- i destinatari del Modello 231 (consulenti, fornitori, *partners* e società di *service*)
- dipendenti;
- dipendenti con incarichi apicali;

Pertanto, **tutti coloro che operano**, a tutti i livelli, dell'Ente (dipendenti, organi sociali,

consulenti, fornitori, *partners* e società di *service*), devono informare l'OdV, mediante apposite segnalazioni, in merito a eventi che potrebbero ingenerare responsabilità di GOIRC ai sensi del D.Lgs. 231/01 e, in particolare, in merito a:

- tutti i dati, fatti ed informazioni aziendali rilevanti ai sensi del D.Lgs. 231/01, comunicando, ove possibile, la relativa documentazione;
- eventuali, ulteriori situazioni delle attività aziendali che possano esporre GOIRC a rischio;
- evoluzioni delle attività nelle aree a rischio e, in generale, qualsiasi situazione, evento o cambiamento, nell'organizzazione o nell'operatività di GOIRC, che possa influire sul corretto funzionamento del Modello 231.

Segnatamente, **i dipendenti** devono:

- trasmettere, obbligatoriamente ed immediatamente, all'OdV, eventuali segnalazioni e/o comunicazioni relative alla commissione (o alla ragionevole convinzione di commissione) di condotte illecite rilevanti ai sensi del D.Lgs. 231/01 che possano integrare i reati ivi previsti;
- informare l'OdV in ordine a comportamenti non conformi con il D.Lgs. n. 231/01 di cui siano venuti a conoscenza in ragione delle funzioni svolte;
- trasmettere le seguenti, più specifiche, informazioni:
- i provvedimenti e/o notizie provenienti da organi di Polizia giudiziaria (o da qualsiasi altra Autorità) dai quali si evinca lo svolgimento di indagini per i reati previsti nel D.Lgs. 231/01, anche nei confronti di ignoti, qualora tali indagini coinvolgano GOIRC o suoi dipendenti, organi societari, fornitori, consulenti, *partners*, società di *service*;
- i rapporti predisposti dai responsabili di altre funzioni e/o ruoli di GOIRC nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D.Lgs. 231/01;
- le notizie relative ai procedimenti sanzionatori svolti ed alle eventuali misure irrogate ovvero provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora esse siano connesse alla commissione di reati o violazioni delle regole di comportamento o procedurali del Modello 231;
- le conclusioni delle verifiche ispettive disposte da funzioni di controllo interno o da commissioni interne da cui derivino responsabilità per la commissione di reati di cui al D.Lgs. 231/01;
- le richieste di assistenza legale proposte da soci, amministratori, dirigenti per la commissione di reati rilevanti ai sensi del D.Lgs. 231/01;
- le comunicazioni in ordine alla variazione della struttura organizzativa, delle deleghe dei poteri e delle aree di rischio;
- la realizzazione di operazioni considerate a rischio in base al D.Lgs. 231/01 ed alla normativa di riferimento.

**I dipendenti con incarichi apicali** hanno l'obbligo di segnalare all'OdV, oltre che dati, notizie ed informazioni sopra elencati e descritti, eventuali violazioni poste in essere da dipendenti, organi sociali, fornitori, società di *service*, consulenti e *partners*, di cui essi siano venuti a conoscenza;

Gli altri **destinatari del Modello 231** di GOIRC (consulenti, fornitori, *partners* e società di *service*) sono sottoposti ad obblighi di segnalazione specificati in appositi documenti firmati da tali soggetti o in clausole inserite nei contratti conclusi tra tali soggetti e GOIRC.

**6.5.2 I flussi informativi diretti dall'ODV agli altri organi di GOIRC** si distinguono, analogamente ai flussi informativi di cui al precedente par. 5.1, in:

- a) flussi informativi "predefiniti", aventi ad oggetto le informazioni dirette alle figure aziendali apicali nonché a quelle che gestiscono le attività sensibili di GOIRC;
- b) flussi informativi, di carattere "straordinario", attivati al verificarsi di eventi relativi ai sensi del D.Lgs. 231/01.

**I flussi informativi provenienti dall'OdV e diretti agli altri organi dell'Ente sono di seguito elencati e descritti:**

**a) Relazione annuale**, inviata all'Organo Amministrativo ed agli organi di controllo, quale resoconto sull'attuazione del MOG 231 e delle attività di verifica e controllo funzionali alla sua attuazione effettiva, contenente, in particolare, i seguenti elementi:

- attività svolta durante il precedente anno;
- eventuali criticità emerse in termini sia di condotte sia di episodi verificatisi;
- interventi correttivi pianificati ed il loro stato di realizzazione;
- necessità di eventuali aggiornamenti del Modello 231;
- necessità di eventuali integrazioni del Modello 231 e delle procedure finalizzate alla prevenzione dei reati, evinta da ispezioni effettuate, variazioni organizzative o modifiche normative;
- il *budget* richiesto per le attività previste;

**b) tempestiva comunicazione** ai citati organi aziendali di situazioni straordinarie inerenti, ad esempio, ad eventuali segnalazioni di violazioni del Modello 231.

**I flussi informativi suindicati sono integrati da quelli riportati nelle singole Procedure della Parte Speciale.**

## **6.6 Whistleblowing (WB)**

L'importanza dei flussi informativi, già riconosciuta nelle diffuse prassi aziendali e negli

standard di settore, ha ricevuto espresso riconoscimento normativo, avendo la Legge 179/17, in modifica del D.Lgs. 231/01 ed il D.Lgs. 24/2023 previsto che i modelli organizzativi debbano prevedere, tra l'altro:

- uno o più canali che consentano di presentare segnalazioni circostanziate di condotte illecite, fondate su elementi di fatto precisi e concordanti;
- almeno un canale alternativo di segnalazione idoneo a garantire la riservatezza dell'identità del segnalante.

**Le seguenti previsioni hanno mero valore ricognitivo e confermativo di quanto disposto dall'Ente nella propria PROCEDURA WHISTLEBLOWING, volta a disciplinare il funzionamento del *Whistleblowing*:**

le segnalazioni e/o comunicazioni devono essere formulate per iscritto, circostanziate e fondate su elementi di fatto rilevanti, precisi e concordanti;

- GOIRC garantisce i segnalanti in buona fede contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, diretta o indiretta, per motivi collegati alla segnalazione;
- GOIRC assicura la riservatezza dell'identità del segnalante fatti salvi gli obblighi di legge e la tutela dei diritti di GOIRC o delle persone accusate erroneamente e/o in mala fede.

L'OdV, nel rispetto della citata Procedura WB e dell'attività delegata al nominato Gestore del WB in Azienda, valuta le segnalazioni ricevute:

- a) assumendo, se del caso, informazioni;
- b) intraprendendo, ove opportuno, con gli altri organi di controllo aziendali, eventuali azioni ispettive;
- c) informando del risultato le funzioni coinvolte.

## **7. DIFFUSIONE DEL MODELLO ED ATTIVITA' FORMATIVA.**

### **7.1 Attività di formazione.**

Ai fini dell'efficace attuazione del Modello 231 occorre provvedere alla formazione del personale, curata da GOIRC unitamente all'OdV.

#### **L'attività di formazione, distinta in base ai soggetti destinatari, è rivolta:**

- al personale dipendente, non rientrante nel personale apicale;
- al personale apicale o fornito di poteri di rappresentanza;
- ai collaboratori esterni .

#### **Formazione del personale dipendente.**

Ai fini dell'attuazione del Modello 231, la formazione del personale dipendente, non rientrante nel personale apicale, è gestita dal Consiglio Direttivo, o da soggetti delegati o incaricati da tale Organo, unitamente all'OdV, e viene svolta attraverso: note informative interne; informative inserite o allegate alla lettera di assunzione; corsi di formazione; utilizzo della rete intranet; e-mail di aggiornamento.

#### **Formazione del personale apicale.**

La formazione del personale apicale e del personale fornito di poteri di rappresentanza viene effettuata, oltre che mediante gli strumenti e le modalità sopra indicate, attraverso un seminario di aggiornamento annuale.

#### **Informazione a collaboratori esterni e fornitori.**

Ai soggetti che collaborano con GOIRC dovranno fornirsi specifiche informative sulle procedure adottate e comunicare, in collaborazione con l'OdV, il Codice Etico.

Le violazioni del presente MOG 231, che comportino il rischio di commissione di un reato di cui al D.Lgs 231/01, potranno determinare, in virtù di specifiche clausole inserite nei contratti, la risoluzione del rapporto contrattuale.

## **Contenuti dei programmi formativi**

**I programmi formativi riguardano: la disciplina normativa, la giurisprudenza, le prassi aziendali, la casistica con analisi di casi comparabili**

**GOIRC predispone un piano formativo articolato nel seguente modo:**

- corsi formativi mirati, con personale docente esterno ed interno in possesso di consolidata esperienza;
- attività di formazione “continua” distinta in una prima fase, organica e strutturata, ed in una seconda fase dedicata all’aggiornamento sulle tematiche più importanti;
- attività di formazione “specifica”, relativa: alle aree a rischio-reato; alle specifiche esigenze di GOIRC; alle specifiche Procedure Operative inerenti le aree a rischio- reato.

**L’attività formativa sarà concentrata sui seguenti argomenti:**

- cultura della legalità e dell’etica pubblica;
- struttura normativa e problemi applicativi del D.Lgs. n. 231/01;
- codice etico e sistema sanzionatorio;
- attività sensibili poste in essere da GOIRC;
- sistema di prevenzione dei reati 231/01, procedure operative e protocolli;
- *whistleblowing* e relative applicazioni.

## **Procedure e modalità di formazione**

**Contenuto obbligatorio dei corsi formativi:** Spiegazione frontale o mediante slide/corso on line; test di valutazione intermedia; test di comprensione finale; firme di adesione al corso in entrata e uscita.

La frequenza e la partecipazione ai corsi è obbligatoria.

**Monitoraggio operativo:** al fine di prevenire i reati di cui al D.Lgs. n. 231/01 e rafforzare l’efficacia esimente del Modello, l’OdV svolge funzione di controllo preventivo e di verifica sui programmi di formazione prima della somministrazione ed al termine dei corsi.

## **7.2 Diffusione del Modello 231.**

GOIRC si adopera per informare ed aggiornare tutti i Destinatari del presente Modello 231 in merito al contenuto, alle prescrizioni ed alle sanzioni collegate al Modello stesso.

Il Modello 231 viene comunicato e messo a disposizione di ogni dipendente ed apicale mediante il sistema informativo aziendale mentre ai soggetti esterni all'Ente viene comunicato attraverso specifica informativa e pubblicazione sul sito istituzionale.

**GOIRC**

**Modello Organizzativo D.lgs 231/01**

**PARTE SPECIALE**

**MODELLO 231**

**GOIRC**

## 1. La Parte speciale del D.lgs 231/2001

L'art. 24 rappresenta la norma di apertura della Sezione III del Capo I del D.lgs 231/2001, rubricata "Responsabilità amministrativa da reato"

Dopo aver disciplinato i principi generali e i criteri di attribuzione della responsabilità dell'ente (Sezione I) e le sanzioni (Sezione II), il D.Lgs. 231/2001 passa quindi a enucleare le fattispecie presupposto, sulla base di un'indicazione tassativa delle norme incriminatrici. L'estensione del principio di legalità alle persone giuridiche, nella sua duplice connotazione del "*nullum crimen*" e "*nulla poena sine praevia lege*", comporta la necessità che vengano previamente ed espressamente indicate le fattispecie costituenti reato per le persone fisiche – e che compongono la lista dei reati presupposto – e la relativa pena prevista a carico della persona giuridica

## 2. Origini della norma e successive modifiche

Il legislatore delegato del 2001, si è limitato a introdurre un numero limitato di condotte criminose nel catalogo dei reati presupposto agli artt. 24 e 25 (sostanzialmente, reati contro la Pubblica Amministrazione).

Il catalogo dei reati presupposto si è esteso progressivamente con una media di 53 nuove introduzioni all'anno dal 2001 al 2021.

L'art. 24 contempla la responsabilità dell'ente collettivo per i reati di malversazione a danno dello Stato (art.316 – bis c.p ), indebita percezione di erogazioni a danno dello Stato (art.316 – ter c.p), turbata libertà degli incanti (art.353 c.p) e turbata libertà del procedimento di scelta del contraente (art.353 bis c.p ), frode nelle pubbliche forniture (art. 356 c.p), truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art.640, comma 2, numero 1 c.p), truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 – bis c.p), frode informatica in danno dello Stato o di altro ente pubblico (art.640 ter c.p), frode ai danni del Fondo europeo agricolo (art. 2. L.23 dicembre 1986, n.898).

Se, in prima analisi, le diverse ipotesi enucleate nell'art.24 appaiono eterogenee. Non di meno sono raggruppate in un contesto unitario fattispecie lesive del buon andamento della pubblica amministrazione, sotto il profilo dell' integrità del patrimonio pubblico e comunitario e della corretta allocazione delle risorse pubbliche, andando a perseguire reati a tutela del corretto impiego degli strumenti a sostegno delle attività economiche di pubblico interesse.

L'art. 24, in sintesi, sanziona le ipotesi truffaldine idonee all'ottenimento indebito di sovvenzioni o che comportino lo sviamento delle predette somme rispetto all'effettiva e lecita destinazione originaria. In tal modo viene apprestata una specifica tutela alle erogazioni pubbliche sia sotto il loro profilo genetico che operativo.

Di recente sono stati introdotti i reati di turbata libertà degli incanti di cui all' art. 353 c.p e di turbata libertà del procedimento di scelta del contraente, di cui all' art.353 – bis c.p, quali reati presupposto connotati da una frode del soggetto attivo e da un corrispettivo danno a carico della pubblica amministrazione.

In ogni caso, i reati presupposto di cui all'art.24 costituiscono ipotesi di reati "peculiarissimi" dell'impresa, manifestazioni tipiche di comportamenti illeciti rinvenibili nell'attività imprenditoriale. Invero, reati ricompresi nell'art. 24 sono integrati in ambiti di attività d'impresa nei quali si innesta un rapporto con la pubblica amministrazione.

Pertanto, il requisito dell' interesse o vantaggio richiesto dall'art. 5 può essere dimostrato agevolmente, dato il profilo patrimoniale dei reati e la loro strettissima connessione all'attività imprenditoriale nei confronti dei terzi.

La Corte di Cassazione, ha statuito che “ integra il concetto di interesse o vantaggio dell'ente l'ipotesi in cui il profitto del reato di truffa sia inizialmente conseguito dalla società indagata attraverso l'accreditamento in suo favore delle somme erogate dalla pubblica amministrazione, restando irrilevante ai fini della responsabilità dell'ente l'eventuale successiva distrazione delle medesime somme sui conti personali dell'amministratore ” (Cass. Pen., Sez. II, [30.01.2006, n. 3615](#)),. Si esclude invece, la configurabilità del reato di truffa ai danni dello Stato per finanziamento in assenza delle condizioni richieste qualora “ si dimostri che il finanziamento illecitamente ottenuto sia stato immediatamente distratto a vantaggio esclusivo dei soci ” (Cass. Pen., Sez. II, [23.04.2021, n. 23300](#)).

I delitti di frode a tutela di erogazioni pubbliche risultano piuttosto diffusi, le modalità di integrazione dei reati presupposto concernono tutte le fasi di contatto con la pubblica amministrazione, dalla preparazione della richiesta, alla ricezione delle somme, alle fasi esecutive e all' utilizzo dei fondi. Pertanto, il presente MOG 231 dedica particolare attenzione alle procedure e ai protocolli in esso contenuti relativi ai rapporti con la pubblica amministrazione.

Nelle linee guida di Confindustria del 2021, sono individuate, quali specifiche aree a rischio reato in relazione all'art. 24:

- presentazione di istanze alla pubblica amministrazione, al fine di ottenere il rilascio di un atto o provvedimento amministrativo (licenza, autorizzazione, etc.) di interesse aziendale (ad esempio, mediante la produzione di documenti falsi attestanti l'esistenza di condizioni e/o requisiti essenziali);
- attività aziendali che prevedano l'accesso nei confronti di sistemi informativi gestiti dalla pubblica amministrazione, quali, a titolo esemplificativo:
- la partecipazione a procedure di gara che prevedono comunque una gestione informatica (ad esempio, mediante l'alterazione di registri informatici della pubblica amministrazione per far risultare esistenti condizioni essenziali per la partecipazione);
- la presentazione in via informatica alla pubblica amministrazione di istanze e documentazione di supporto, al fine di ottenere il rilascio di un atto o provvedimento amministrativo (licenza, autorizzazione, ecc.) di interesse aziendale (ad es. contenenti attestazioni/ certificazioni non veritiere in merito all'esistenza di condizioni e/o requisiti essenziali);
- i rapporti con soggetti della pubblica amministrazione competenti in materia fiscale o previdenziale in relazione alla ipotesi di modifica in via informatica dei dati di interesse dell'azienda, già trasmessi alla pubblica amministrazione;
- partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e il loro concreto impiego di operatività della formazione, della ricerca ed innovazione tecnologica,
- partecipazione a procedure competitive negoziazione, stipula, gestione di contratti attivi;
- selezione dei fornitori di beni, servizi ed opere intellettuale e negoziazione stipula e gestione dei relativi contratti.

### 3. Individuazione delle attività a rischio reato.

In relazione alle attività a rischio reato, il presente MOG 231 ha individuato:

- specifici presidi attività di controllo gerarchico nell'ambito di un coerente sistema di deleghe;
- separazione funzionale tra chi gestisce le attività di realizzazione e chi presenta la documentazione di avanzamento;
- specifiche attività di controllo gerarchico sulla documentazione da presentare alla pubblica amministrazione;
- formalizzazione di una reportistica relativa al rapporto con la pubblica amministrazione;
- modalità di raccolta, verifica e approvazione della documentazione da trasmettere ai pubblici ufficiali;
- monitoraggio sull'avanzamento del progetto realizzato
- controllo sull'effettivo impiego dei fondi erogati dagli organismi pubblici, in relazione agli obiettivi dichiarati.

### 4. Fattispecie normative e criteri di predisposizione del MOG 231

**Di seguito verranno elencate e descritte le fattispecie di reato, presupposto più rilevanti, illustrando, per ciascuna di esse, i criteri di implementazione del presente MOG 231.**

L'art. 24 D.Lgs. 231/01 disciplina le ipotesi di indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato di un ente pubblico e frode nelle pubbliche forniture

L'art. 24 bis riguarda i delitti Informatici e il trattamento illecito dei dati; le norme richiamate sono le seguenti: artt. 615 – ter , 617-quater, 617-quinquies 635-bis, 635-ter, 635 quater e 635 quinquies del codice penale.

#### **- Accesso abusivo a sistema informatico (615 ter c.p)**

L'art. 615 ter c.p. viene, commesso da chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La norma protegge il cosiddetto «domicilio informatico» inteso come spazio ideale di pertinenza della persona, che deve essere salvaguardato al fine di impedire la violazione della riservatezza o dei dati personali (art. 4 Reg. UE 679/2016 ) nonché qualsiasi intrusione o permanenza non autorizzata nel sistema medesimo, indipendentemente dalla tipologia di informazioni od oggetti ivi registrati/conservati (Cass. Pen., II, [29.05.2019, n. 26604](#)). Si intende per abusivo l'introduzione non autorizzata, ovvero la permanenza contro la volontà del titolare dello *ius excludendi alios*.

Le misure di sicurezza poste a protezione del sistema informatico possono essere costituite da meccanismi logici, tecnologici ed organizzativi che tendono ad impedire la commissione di reati; non è necessario che le misure di sicurezza siano rappresentate da passwords , assumendo rilevanza qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso anche quando si tratti di strumenti esterni rispetto al sistema.

Il reato non sussiste se non vi siano misure di protezione interne o esterne o se queste non siano attive al momento dell'ingresso.

Risponde del delitto in esame colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico protetto violando le condizioni e i limiti risultanti dalle prescrizioni del titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema (Cass. Pen., S.U., [07.02.2011, 4694](#)).

Costituisce accesso abusivo al sistema informatico la condotta del dipendente che in vista dell'interruzione del rapporto di lavoro provvede a copiare ingenti quantità di dati supporti informatici per poi portarli all'esterno ed utilizzarli per finalità diverse da quelle consentite (Cass. Pen. I, [17.06.2019, n. 26625](#)).

#### **- Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater, c.p.)**

Il delitto è commesso da chiunque, al fine di procurare a sé un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o comunque fornisca indicazioni o istruzioni idonee al predetto scopo.

Si configura il reato sia quando il soggetto sia in possesso legittimamente delle credenziali di accesso (è il caso, ad esempio, dell'amministratore di sistema) e le comunichi indebitamente a terzi, sia nel caso in cui il soggetto se le procuri indebitamente. La condotta è abusiva quando i codici di accesso siano ottenuti a seguito della violazione di una norma o di una clausola contrattuale che vieti quella condotta, ma anche in caso di violazione di policy, procedure o regolamenti aziendali.

Sussiste la responsabilità dell'ente nel caso di un attacco di social engineering commesso tramite l'analisi dei comportamenti di un individuo al fine di sottrarre credenziali di accesso ad un sistema concorrente fingendosi una persona vicina alla "vittima" (tramite l'invio di un'email phishing, simulando un'email aziendale, induca la vittima a credere di compiere una normale azione e invece la induce ad inserire le proprie credenziali in un database creato ad arte proprio allo scopo di carpire illecitamente tali credenziali).

#### **- Diffusione di apparecchiature, dispositivi, o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)**

Il delitto viene commesso da chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici. In tale fattispecie rientrano l'utilizzo di programmi come virus, worm (programmi che si replicano all'interno di un sistema informatico e ne impediscono l'utilizzo), malware (programmi malevoli che infettano il sistema contro la volontà dell'utente), backdoor (programmi che consentono l'accesso al programma informatico senza l'autorizzazione dell'utente), spyware (programmi che consentono di raccogliere informazioni sui programmi in cui sono installati), keylogger (programmi malevoli che trasmettono i dati relativi ai tasti digitati su una tastiera da un utente).

A titolo di esempio, per determinare la responsabilità dell'ente, il reato presupposto potrebbe configurarsi qualora il dipendente della Società al fine di alterare i dati relativi ad un concorrente o distruggere i sistemi sui quali i concorrenti conservano la documentazione aziendale, effettui attacchi di *cracking* (che consistono nelle azioni di cd. *reverse engineering* necessarie per

comprendere il funzionamento del software, studiarne i meccanismi di funzionamento, al fine di ricostruirlo in violazione delle norme sul diritto d'autore) o di hacking (tecniche volte a conoscere, accedere o modificare un sistema informatico).

**- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater, c.p.)**

Il delitto consiste nella fraudolenta intercettazione ovvero nell'impedimento, interruzione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi. Ricorre questa ipotesi qualora l'Amministratore di Sistema, eluda gli sbarramenti all'accesso delle comunicazioni dei dipendenti sfruttando gli strumenti a sua disposizione (Cass. Pen., Sez. V, [30.01.2015, n. 29091](#)).

Le condotte di impedimento o interruzione illecita di comunicazione, corrispondono a ipotesi in cui, tramite particolari software, si impedisce o si interrompe la navigazione alla rete, determinando la disconnessione dell'utente dalla stessa, con la conseguente interruzione delle comunicazioni in corso.

Integra il reato in esame anche la condotta dell'Amministratore di Sistema che, sfruttando i suoi privilegi, entra nell'account di posta del dipendente (Cass. Pen. Sez.V, [31.07.2007, n. 31135](#)). Si configura la responsabilità dell'ente nel caso in cui il reato venga commesso allo scopo di intercettare fraudolentemente le comunicazioni di enti concorrenti nella partecipazione alle gare di appalto allo scopo di conoscere l'entità dell'offerta dei concorrenti o strategie di mercato di enti concorrenti; nell'impedimento o interruzione di una comunicazione per impedire al concorrente di trasmettere i dati/l'offerta per partecipare ad una gara o comunque per ritardare l'esecuzione delle prestazioni verso i clienti.

**- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)**

Il delitto può essere commesso da chiunque installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico.

Il delitto viene commesso in caso di installazione di apparecchiature dirette ad intercettare o impedire comunicazioni informatiche da parte del personale incaricato della gestione degli apparati e dei sistemi componenti l'infrastruttura di rete aziendale.

**- Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.) e 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.)**

Il delitto consiste nella distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui. Il delitto in esame è integrato anche quando «la manomissione ed alterazione dello stato di un computer sono rimediabili soltanto attraverso un intervento recuperatorio postumo, comunque, non reintegrativo dell'originaria configurazione dell'ambiente di lavoro.

Il reato sussiste quando è stato cancellato, mediante l'apposito comando e dunque senza determinare la definitiva rimozione dei dati, un rilevante numero di file, poi recuperati grazie all'intervento di un tecnico informatico specializzato.

Rientra nell'ambito applicativo della disposizione normativa anche la cancellazione che non escluda la possibilità di recupero se non con l'uso – anche dispendioso – di particolari procedure così integrando gli estremi oggettivi della fattispecie delittuosa.

**- Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.) e danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)**

Il delitto in esame viene commesso, salvo che il fatto costituisca più grave reato, da chiunque mediante le condotte di cui al 635-bis c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia o rende inservibili i sistemi informatici altrui o ne ostacola il funzionamento. Il danneggiamento deve interessare l'intero sistema, ossia l'hardware. Ad esempio l'ipotesi in cui il reato sia commesso mediante malware atti a cagionare uno degli eventi di distruzione, danneggiamento, procurata inservibilità, o di ostacolo al funzionamento degli stessi. Costituiscono esempio di tali condotte gli attacchi *ransomware*.

Rappresentano esempi di possibile responsabilità dell'ente, le ipotesi in cui vengano danneggiate delle infrastrutture tecnologiche dei concorrenti al fine di impedirne l'attività o per danneggiarne la loro immagine.

Il d.l. n. 105/2019 agli artt. 1, commi 11 e 11-bis (di seguito "d.l. Cyber Security") ha esteso il catalogo dei reati di cui all'art. 24-bis anche alla fattispecie di ostacolo o condizionamento dei procedimenti per la Sicurezza Cibernetica e delle relative attività ispettive e di vigilanza

Il nuovo reato di violazione delle norme in materia di perimetro di sicurezza nazionale cibernetica è un reato proprio che può essere commesso solo da coloro che rientrano nel perimetro di sicurezza nazionale e cibernetica che, essendo assoggettati al rispetto degli obblighi previsti da tale normativa in questione, nonché alla vigilanza delle preposte autorità, potranno realizzare le condotte incriminate.

Sussiste pertanto, la responsabilità dell'ente nell'ipotesi di trasmissione di informazioni false o omissione di informazioni dovute in relazione all'attività di formazione degli elenchi delle reti, dei sistemi informativi e dei servizi informatici rientranti nel perimetro di sicurezza nazionale cibernetica, ovvero in caso di ostacolo alle funzioni di vigilanza da parte della Presidenza del Consiglio dei Ministri o del Ministero dello sviluppo economico.

**Al fine di prevenire adeguatamente questi reati presupposto, nel presente MOG 231 la prevenzione dei crimini informatici si realizza attraverso adeguate misure organizzative tecnologiche assicurando che l'attività dell'OdV venga correttamente indirizzata anche attraverso specifiche forme di controllo.**

Sono previsti controlli di carattere generale mediante la:

- previsione nel codice etico di specifiche indicazioni volte a impedire la commissione dei reati informatici;
- pianificazione di programmi di formazione;
- previsione di idonee clausole contrattuali con i provider dei servizi legati *all'information technology*;
- definizione di un elenco di applicativi ammessi e soprattutto di quelli il cui uso è vietato ai dipendenti;

Il Sistema di controllo implementato nel presente Modello 231 prevede i seguenti principi di controllo

- separazione dei ruoli;
- tracciabilità degli accessi e delle attività svolte dai sistemi informatici;
- procedure e livelli autorizzativi da associarsi alle attività critiche;
- raccolta, analisi e gestione di segnalazioni di fattispecie a rischio di reati informatici;

– procedure di escalation per la gestione di fattispecie a rischio di reato

Tra gli altri controlli predisposti si evincono:

- politiche e procedure di gestione degli asset aziendali;
- politiche procedure di controllo degli accessi logici;
- politiche di gestione della sicurezza fisica;
- politiche di gestione sicura delle comunicazioni
- politiche procedure di gestione delle terze parti

Nella specifica procedura dedicata a questi reati presupposto viene costantemente richiamato il rispetto della disciplina in materia di protezione dei dati personali nonché l'adozione di un Modello Organizzativi privacy (MOP).

- **L'art. 25 de Decreto riguarda i seguenti delitti:** peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione (artt. 318,321,322 346 bis del codice penale e 364-bis del codice penale, Artt.319, 319-ter, Art.317)

I reati contro la Pubblica Amministrazione hanno costituito, e ancora oggi costituiscono, il nucleo centrale del catalogo dei reati presupposto di cui al d.LGS 231/2001

- **Con la l.190/2012** (c.d “legge anti-corruzione” o “legge severino”). si è assistito all'eliminazione delle lacune del sistema repressivo attraverso l'inclusione di nuovi delitti contro la P.A. e la riformulazione delle fattispecie originarie nel testo dell'art.25 d.lgs 231/01.

L'ente può oggi rispondere dei reati di induzione indebita a dare o promettere utilità di cui all'art.319 quater e di corruzione tra privati ex art. 2635 c.c (collocato, nel sottosistema dei reati societari la nuova disposizione di cui all' art.319 quater c.p punisce la condotta concussiva mediante induzione.

La novità, e la punibilità, non solo del pubblico ufficiale o dell'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità, ma anche, seppur in forma minore, del soggetto indotto (figura intermedia tra la vittima e il complice del pubblico ufficiale).

La condotta del soggetto apicale o sottoposto che, pur a seguito di un comportamento abusivo o di pressione morale, presta acquiescenza alle richieste del pubblico ufficiale potrà determinare, ove ricorrano gli altri presupposti previsti dal dl.gs 231/2001, anche una responsabilità dell'ente a cui il privato in dotto appartiene.

Successivamente con la **legge n.3/2019 (c.d legge “spezzacorrotti”)**. il legislatore è tornato ad ampliare il perimetro della responsabilità amministrativa da reato con riferimento ai delitti contro la pubblica amministrazione; la novità più rilevante è rappresentata dall'inserimento del delitto di traffico di influenze illecite all'interno delle fattispecie previste dalla norma in commento.

L'art . 346 – bis c.p, punisce colui che, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio, indebitamente fa dare o promettere, a se o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri.

Un ultimo ampliamento dei delitti presupposto previsti dall'art.25 è intervenuto con il **d.lgs 75/2020** il quale ha introdotto, la responsabilità dell'ente per le ipotesi di peculato (art.314 co. 1

c.p.), di peculato mediante profitto dell'errore altrui (art.316 c.p) e di abuso d'ufficio (art. 323 c.p).

L'impatto di tale modifica normativa, tuttavia, appare oggettivamente limitato.

Il legislatore è nuovamente intervenuto con l'art.9, comma 2 – ter, del D.L **4 luglio 2024, n.92 (c.d Decreto Carcere)**. convertito con modificazioni dalla Legge 8 Agosto 2024 n.112, il quale, ha eliminato il riferimento al reato di abuso d'ufficio e ha inoltre introdotto nel catalogo dei reati presupposto il nuovo delitto di indebita destinazione di denaro o cose mobili previsto dall art.314 – bis c.p.

Le Linee Guida di Confindustria individuano, con riferimento ai delitti contro la pubblica amministrazione, una serie di aree a rischio , a cui vengono associati specifici controlli preventivi che l'ente può predisporre al fine di prevenire il verificarsi di episodi delittuosi. Assumono rilevanza la partecipazione a procedure di gara o di negoziazione diretta per la vendita di beni e servizi ovvero finalizzate alla realizzazione di opere a favore della P.A. (anche in realizzazione di accordi di partnership con terzi soggetti o attraverso il ricorso di attività di intermediazione), nonché la successiva attività di erogazione del servizio e/o della prevista prestazione contrattuale. Per gestire queste aree di rischio, nel presente MOG 231 sono stati introdotti i seguenti controlli preventivi:

- monitoraggio delle offerte economiche relative a gare e a trattative private con la P.A.;
- monitoraggio delle fasi evolutive dei procedimenti di gara o di negoziazione diretta;
- verifiche, a cura di idonee funzioni aziendali distinte da quella commerciale, sull'effettiva erogazione delle forniture e/o sulla reale prestazione dei servizi, inclusi i controlli sui livelli qualitativi attesi;
- controlli, laddove l'ente faccia ricorso ad agenti o altri collaboratori esterni, della congruità delle provvigioni pagate rispetto a quelle praticate nell'area geografica di riferimento.

Inoltre il Modello 231, ripone attenzione, considerato il reato di traffico di influenze illecite, alla gestione dei rapporti con enti/soggetti terzi che svolgano attività di lobbying o mediazione nei confronti della pubblica amministrazione, prevedendo, strumento di controllo preventivo:

- un'attività di due diligence preventiva e periodica su banche date e/o fonti aperte al fine di evidenziare l'esistenza o l'insorgere di segnali dall'allarme (c.d. red flags ) a carico del terzo incaricato;
- l'inserimento, nei relativi contratti, di specifiche previsioni volte ad assicurare il rispetto, da parte dei terzi, di principi di controllo e di regole etiche e di condotta nelle relazioni con i pubblici ufficiali o incaricati di pubblico servizio
- la fissazione di parametri per la definizione dell'ammontare del compenso;
- una rigorosa verifica dell'attività condotta dal terzo.

In caso di relazioni esterne o istituzionali con pubblici ufficiali e/o incaricati di pubblico servizio, il Modello 231 assicura la trasparenza e la tracciabilità delle attività svolte.

Con riferimento alle procedure per l'ottenimento di licenze, autorizzazioni, i MOG prevede, oltre ad una successiva attività di monitoraggio preventiva un'attività di programmazione volta a definire

- le modalità di raccolta e verifica delle informazioni necessarie per la predisposizione della documentazione relativa all'istanza,

- le modalità di verifica e approvazione della documentazione da presentare da parte di adeguati livelli autorizzativi,
- le modalità di verifica circa l'effettivo impiego dei fondi erogati dagli organismi pubblici, rispetto agli obiettivi dichiarati.

Sono altresì disciplinate nel Mog 231 le attività di selezione, negoziazione, stipula ed esecuzione di contratti con soggetti privati, specie laddove essi abbiano ad oggetto beni o servizi di natura immateriale, quali consulenze direzionali, commerciali, amministrativo-legali e collaborazioni a progetto pubblicità o sponsorizzazioni; spese di rappresentanza, attraverso la predisposizione di specifiche procedure organizzative, che assicurino:

- verifiche preventive sulle controparti o sui beneficiari;
- definizione di criteri quantitativi e qualitativi con adeguati livelli di autorizzazione per le spese di rappresentanza;
- distinzione dei ruoli;
- stratificazione dei poteri di firma;
- tracciabilità dei flussi finanziari.

**- L'art. 25 bis.1 è relativo ai delitti contro l'industria e il commercio – artt. 513,515,516,517, 517 ter e 517 quater , 513-bis e 514.**

I delitti contro l'industria e il commercio sono stati inseriti, nell'ambito del D.Lgs 231/01 con l'articolo 15 comma 7 lett. b della Legge 99 del 2009 contro l'industria e il commercio

I delitti contro l'industria e il commercio possono distinguersi in due macro categorie:

delitti che tutelano il corretto e normale svolgimento dell'industria e il commercio (e quindi l'ordine economico) andando a reprimere condotte che cadono sui diritti connessi alla sussistenza di segni distintivi e titoli di proprietà industriale; per la configurazione di questi reati, occorre segno distintivo (ditta, marchio, insegna) o, più in generale, un titolo di proprietà industriale.

Per questa prima categoria di reati (ossia i delitti che richiedono comunque condotte che incidono sui segni distintivi o sui titoli di proprietà industriale), vengono in rilievo i concetti di contraffazione, alterazione usurpazione.

Una seconda categoria di reati tutela i beni giuridici qui in rilievo da condotte violente o comunque insidiose e truffaldine, sia a tutela della concorrenza che dei consumatori, **a prescindere dall'eventuale contraffazione, alterazione di segni distintivi o usurpazione di un titolo di proprietà industriale**

La condotta di chi altera la concorrenza ricorrendo a mezzi fraudolenti integra lo specifico delitto soltanto se si ripercuote sull'ordine economico, ossia quando è posta in essere al fine specifico di turbare o impedire il normale svolgimento dell'industria o del commercio e di attentare in tal modo alla libertà di iniziativa economica (Cass. Pen., III,24.03.2015, n. 12227).

L'articolo 515 c.p. (frode nell'esercizio del commercio), viene interpretato estensivamente ritendendo configurato il reato anche nelle ipotesi in cui la diversità riguardi qualità non essenziali del bene consegnato (Cass. Pen., III, 05.12.2005, n.44274).

Il presente modello organizzativo non gestisce la prevenzione di questi reati presupposto mediante specifica Procedura, rinviando alla Sistema generale di prevenzione e ai controlli ivi previsti, in ragione del fatto che l'Organizzazione non opera nella commercializzazione dei prodotti.

Con riguardo, alla seconda categoria, reati contraddistinti semplicemente dalla "frode" senza alcun riflesso necessario sui segni distintivi e sui marchi (ad es. art.515 c.p), la prevenzione del

rischio viene attuata mediante la corretta formazione del personale impiegato nell'area commerciale e nei rapporti con la clientela.

**- L'art. 25 ter riguarda i reati societari: artt. 2621 c.c, 2621 bis c.c, 2622 c.c ,2623c.c, 2624 c.c, 2625c. ,2628 c.c 2629 c.c 2632 c.c , 2636c.c..**

#### **False comunicazioni sociali**

L'art. 25- ter prende in considerazione, le fattispecie di false comunicazioni sociali ( art.2621 c.c) e false comunicazioni sociali delle società quotate (art.2622 c.c). Inoltre, la lett. a- bis) richiama l'ipotesi di falso in bilancio per i fatti di lieve entità disciplinata dall'art.2621-bis c.c.

Gli art. 2621 e 2622 c.c contemplano due fattispecie di reato del tutto sovrapponibili. In entrambe le ipotesi, infatti, la condotta rilevante è la medesima: l'esposizione, consapevole, di “fatti materiali rilevanti non rispondenti al vero” ovvero l'omissione di “fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore”.

#### **- I reati a tutela del corretto funzionamento della società**

Le lett. h) e q) dell'art. 25- ter prevedono, quali reati presupposto i reati di impedito controllo ex art. 2625, comma 2, c.c. e di illecita influenza sull'assemblea ex art.2636 c.c.

La prima sanziona gli amministratori che ostacolano le attività di controllo che la legge riconosce ai soci o ad altri organi sociali, a condizione che la condotta abbia cagionato un danno ai soci. L'art.2636 c.c. rubricato “illecita influenza sull'assemblea”, sanziona chi determina la maggioranza in assemblea mediante atti simulati o fraudolenti, allo scopo di procurare a sé o ad altri un ingiusto profitto.

#### **- I reati a tutela del capitale e del patrimonio sociale**

La fattispecie di formazione fittizia del capitale prevede le seguenti condotte tipiche che possono essere realizzate dagli amministratori o dai soci: attribuzione di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti o del patrimonio della società nel caso di trasformazione.

Il delitto di illegale ripartizione degli utili e delle riserve sanziona le condotte degli amministratori che ripartiscono utili non effettivamente conseguiti o destinati per legge a riserva o che ripartiscono riserve che per legge non possono essere distribuite.

La fattispecie di cui all'art. 2633 c.c rubricato “indebita ripartizione dei beni sociali da parte dei liquidatori ” sanziona le condotte dei liquidatori che in fase di liquidazione della Società, distribuiscono i beni sociali ai soci, prima di procedere alla soddisfazione o all'accantonamento delle somme per i creditori sociali.

#### **- I reati di agiotaggio e di omessa comunicazione del conflitto di interessi**

L'art. 2637 c.c punisce la diffusione di notizie false nonché il compimento di operazioni simulate o l'utilizzo di altri artifici. Trattasi di condotte che devono essere idonee “ a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati”

#### **- I reati a tutela del corretto espletamento delle funzioni di vigilanza**

Tra questi rientra l' art. 2638 c.c. relativo all'ostacolo all'esercizio delle attività pubbliche di vigilanza.

#### **- La fattispecie di corruzione tra privati**

la fattispecie di corruzione tra privati di cui al terzo comma dell'art.2635 c.c e di istigazione alla

corruzione tra privati di cui al primo comma dell'art. 2635- bis c.c.,

**Il rischio di commissione delle fattispecie di reato richiamate dall' art 25 – ter D.lgs 231/01 è ravvisabile nell'attività di qualsiasi soggetto economico.**

Le aree sensibili rispetto alle quali potrebbe verificarsi la commissione dei reati societari:

la gestione dei rapporti con altri organi sociali (in particolare, con i soci e l'organo di controllo) e con l'Autorità di Vigilanza, la redazione del bilancio e delle altre comunicazioni sociali, la gestione della contabilità e degli adempimenti fiscali.

Si tratta di “rischi trasversali (o generali)”, ai quali, cioè, sono esposti tutti gli enti collettivi indipendentemente dal settore merceologico di attività, “nella misura in cui ciascuna persona giuridica (o anche associazioni prive di personalità giuridica) e tenuta a redigere documenti di rappresentazione della propria situazione economico-patrimoniale o finanziaria, a indirizzare ‘comunicazioni sociali’ a soci o terzi, ed è sottoposta ad un sistema di controlli (interni e/o esterni)”.

Il livello del rischio dovrà essere misurato “sulla base delle caratteristiche concrete dell'attività dell'ente – dunque sarà proporzionato, ad esempio, alla ‘complessità’ della rappresentazione bilancistica e al numero degli stakeholder e degli interessi in gioco – nonché sulla base di situazioni contingenti, in grado di rendere particolarmente delicati e sensibili i contenuti dell'informativa societaria”.

Dal livello del rischio così valutato dipenderà la pervasività dei presidi di controllo interno che l'ente sarà chiamato ad adottare nell'implementazione del Modello per prevenire la commissione dei principali reati societari.

In particolare, l'Ente istituisce, con specifico riferimento al processo di redazione del bilancio e delle altre comunicazioni sociali un sistema di controllo interno volto a garantire la completezza, la correttezza, l'attendibilità e la chiarezza delle informazioni comunicate al mercato sulla situazione, i risultati e le prospettive della società, in coerenza con le previsioni di legge.

Nel presente MOG 231 pertanto sono state formalizzate specifiche indicazioni sul metodo da utilizzare per valutare le voci di bilancio oggetto di stima, sulla predisposizione di adeguata documentazione a supporto delle scelte contabili effettuate.

In relazione alla gestione dei rapporti con gli altri organi sociali e con le Autorità di vigilanza, il modello al fine di prevenire la commissione dei reati societari adotta presidi volti a garantire:

- i) la gestione delle richieste di informazioni, di dati e di documenti ricevute dai soci, improntate ai principi di trasparenza, collaborazione e completezza
- ii) l'individuazione della persona preposta alla trasmissione della documentazione agli organi sociali e all'Autorità di Vigilanza;
- iii) l'istituzione di riunioni periodiche tra l'organo di controllo e l'OdV allo scopo di verificare l'osservanza della disciplina in tema di normativa societaria e di corporate governance.

Inoltre sono adottate ulteriori misure volte alla prevenzione dei reati di corruzione tra privati ( di cui agli artt. 2635 c.c e 2635 bis c.c e connesso all'eventualità che gli obiettivi d'impresa – quali la massimizzazione del profitto – siano perseguiti mediante comportamenti corruttivi.)

I soggetti collettivi Strumenti organizzativi che regolano le principali aree sensibili, quali la gestione dei rapporti con partner commerciali e industriali, individuando per la negoziazione e gestione di contratti attivi: l' iter di definizione e attuazione delle politiche commerciali; previsioni contrattuali standardizzate in relazione alla natura e tipologia di contratti; la verifica della completezza ed accuratezza della fattura rispetto al contenuto del contratto e rispetto ai beni e

servizi prestati.

Con riferimento al processo di approvvigionamento di beni e servizi procedure di autorizzazione delle ri- chieste di acquisto che specifichino:

- i) criteri e modalità di assegnazione del contratto;
- ii) un modello di valutazione delle offerte informato alla trasparenza e a criteri il più possibile oggettivi.

Da ultimo, l'adozione di misure preventive a presidio del processo di selezione, assunzione e gestione del personale che prevedano:

- i) la pianificazione delle risorse da assumere che tenga conto del fabbisogno;
- ii) l'individuazione dei requisiti minimi necessari per ricoprire il ruolo e il relativo livello di retribuzione;
- iii) la definizione di un processo di selezione del personale che disciplini la ricerca di una pluralità di candidature in

funzione della complessità del ruolo da ricoprire, la gestione dei conflitti di interesse tra il selezionatore e il candidato, la verifica della coerenza delle candidature con il profilo definito.

**- L'art. 25 Septies è dedicato alla tutela della salute e sicurezza sul lavoro.**

L'art. 30 del testo unico in materia di sicurezza (D.Lgs 81/08) indica una serie di elementi in presenza dei quali il Modello 231 può ritenersi idoneo **“ad avere efficacia esimente della responsabilità amministrativa”** di cui al Dlgs. 231/2001

Il presente Modello 231 tiene conto dell'esistenza del documento di valutazione dei rischi per la tutela della salute e della sicurezza dei lavoratori, dell'avvenuta individuazione del datore di lavoro e del conferimento di obblighi specifici in relazione alla sicurezza nei luoghi di lavoro.

Il Modello prevede la verifica in merito a: l'esistenza del Documento di valutazione dei rischi per la tutela della salute e della sicurezza dei lavoratori; l'avvenuta individuazione del datore di lavoro ed il conferimento di eventuali deleghe e sub-deleghe, la redazione del documento programmatico di tutte le misure di sicurezza necessarie ed infine che i presidi previsti vengano effettivamente attuati; inoltre, verifica della corretta attuazione di procedure e dei protocolli adottati.

**- L'art. 25 octies riguarda le seguenti ipotesi di reato: ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché di autoriciclaggio.**

Il D.lgs 231/2007 ha, introdotto nell'ordinamento italiano una normativa volta da un lato a prevenire il fenomeno del riciclaggio nell'ambito del sistema finanziario (ponendo in capo ai destinatari obblighi di controllo sulla clientela e sulle operazioni poste in essere) e dall'altro ad ampliare il sistema repressivo in ambito antiriciclaggio. Di conseguenza si deve individuare un collegamento sistematico tra le norme di cui al D.lgs 231/2007 e la responsabilità Amministrativa degli enti di cui al D.lgs 231/2001, nel senso che gli obblighi di prevenzione del fenomeno del riciclaggio previsti dal D.lgs 231/2007 ben possono ispirare le regole di condotta da introdurre nei Modelli di Organizzazione e gestione idonee ad eliminare o comunque ridurre il più possibile il rischio di commissione dei reati elencati all'articolo 25 – ostie D.lgs 231/01.

**I reati presupposto: i delitti di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio.**

A seguito degli interventi normativi operati dal D.lgs 195/2021, il quadro è modificato, innanzitutto con l'ampliamento della categoria dei reati presupposto dai quali origina il provento oggetto delle fattispecie di ricettazione e riciclaggio in senso ampio.

Per quanto concerne il delitto di **riciclaggio**, il rilievo penale, prima riconosciuto ai soli delitti non colposi, è stato esteso a tutti i delitti nonché alle contravvenzioni punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi (nuovo comma 2, art. 648 – bis cod.pen).

Il reato di **reimpiego** di cui all'articolo 648-ter già prima della riforma prevedeva la tipicità penale di condotte a oggetto denaro, beni o altre utilità provenienti da delitto (anche colposo).

#### **Le utilità quali provento oggetto del reato di riciclaggio e auto riciclaggio.**

La giurisprudenza di legittimità ammette pacificamente che il reato tributario possa costituire reato presupposto del delitto di riciclaggio, perché il risparmio di imposta ben può rientrare nella nozione di “altre utilità oggetto della condotta riciclatoria” (da ultimo Cass. Pen., II,05/11/2020, n.30889). Nella locuzione “altre utilità” devono farsi rientrare non solo quegli elementi che incrementano il patrimonio dell'agente ma anche tutto ciò che costituisca il frutto di quelle attività fraudolente a seguito delle quali si impedisce che il patrimonio s'impoverisca: il che è quanto accade quando viene perpetrato un reato fiscale a seguito del quale l'agente, evitando di pagare le imposte dovute, consegue un risparmio di spesa che si traduce, in pratica, in un mancato decremento del patrimonio e, quindi, in una utilità di natura economica.

#### **- L'art. 25 novies è relativo ai delitti in materia di violazione del diritto di autore**

Salvo quanto previsto dall'art. 171 bis e dall'art. 171 ter, è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma: mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa.

I reati presupposto inseriti nell'art. 25- novies non sono fattispecie di reato che possono essere commesse solo da imprese operanti nello specifico settore software/audiovisivo, ma, al contrario, riguardano la quasi totalità dei soggetti economici.

Ciò in quanto lo scopo di contenere i costi connessi all'acquisto di software e altre opere d'autore analizzate sopra, potrebbe indurre qualsiasi ente a commettere le condotte illecite di cui trattasi.

Tali reati infatti, ad esempio, potrebbero essere commessi nel perseguimento degli interessi della società, a prescindere dall'eventuale impiego di beni aziendali (come gli strumenti informatici, i sistemi di diffusione di informazioni e le attrezzature per la duplicazione di testi), ma anche con strumenti personali, nell'ipotesi in cui dall'installazione di un software in assenza di adeguata licenza, consegua comunque per l'ente il risparmio del costo di acquisto della stessa. Sebbene non siano diffuse ipotesi di condanna di enti per tali fattispecie di reato, al fine di prevenire la commissione dei reati di cui trattasi il presente Mog prevede l'adozione delle seguenti misure:

- Predisporre documenti aziendali contenenti l'invito generale al rispetto delle norme in materia di proprietà intellettuale;

– inserire all'interno dei contratti commerciali specifiche clausole che impongano il rispetto anche da parte del terzo contraente delle norme in materia di proprietà intellettuale;

– vietare espressamente da parte dei dipendenti l'uso per scopi aziendali di beni acquisiti in violazione delle norme a tutela del diritto d'autore e in generale con modalità difformi da quelle previste dal titolare.

Ciò risulta da specifici principi etici dedicati all'interno del codice etico e prevedendo attività formative e di diffusione della cultura aziendale volta alla promozione del rispetto delle norme in materia di diritto di autore. Al fine di prevenire reati ipotizzabili con l'utilizzo di beni aziendali, oltre ai controlli di cui sopra, è previsto:

- vietare l'impiego di beni aziendali (come foto, copiatrici, sito web, copisterie o altro) al fine di porre in essere condotte che violino la tutela dei diritti d'autore, quale che sia il vantaggio perseguito;
- controllare i mezzi di comunicazione interni ed esterni alla società (es. sito web, radio ufficiale, stampa, social network, etc.)

Un principio generale da seguire nella prevenzione di tali ipotesi di reato è quello della *segregation of duty*, incaricando esclusivamente gli amministratori di sistema del compito di configurare ed installare software e programmi informatici. Essi poi dovranno verificare a campione sui pc aziendali i programmi installati e prevedere degli specifici filtri rispetto ai siti consentiti, firewall di controllo e protezione perimetrale, nonché effettuare controlli periodici dei livelli di traffico in entrata ed uscita.

Un ulteriore presidio rilevante anche in questo ambito è l'identificazione e nomina di amministratori di sistema che curino lo svolgimento di tutte le attività connesse ai processi sensibili e supervisionino la corretta applicazione dei processi e policy aziendali adottate.

Procedure e policy dedicate al corretto trattamento di dati personali che sono certamente coinvolti nell'ambito di cui si discute. L'adozione infatti di un Modello Organizzativo privacy integrato.

**- L'art. 25 decies è relativo alla induzione a non rendere dichiarazioni o rendere dichiarazioni mendaci all'autorità giudiziaria**

Con tale fattispecie il legislatore ha voluto contrastare possibili strumentalizzazioni della facoltà di tacere concessa agli imputati, con possibile pregiudizio per il contraddittorio nella formazione di prova.

Oggetto della condotta può essere il denaro o altra utilità, nozione più ampia che vi comprende anche prestazioni di fare (condotte attive) o di non fare (condotte passive) capaci di soddisfare un bisogno umano.

Destinatario della condotta del soggetto che usa violenza, minaccia o fa offerta o promessa di denaro o altra utilità, e colui che è chiamato "a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale".

Non risulta realistica del resto la condotta ben potrebbe tradursi nella pressione esercitata da un superiore gerarchico nei confronti di un dipendente (vale a dire, una figura apicale rispetto ad un soggetto sottoposto all'altrui direzione o vigilanza) chiamato a rendere testimonianza in un processo, per far apparire situazioni diverse dalla realtà o per nascondere possibili connivenze, a vantaggio nell'interesse dell'ente.

Tale attività, d'altro canto, potrebbe essere esercitata anche nei confronti di un consulente, un fornitore, un cliente.

Nel modello organizzativo sono previste le aree di rischio in cui potenzialmente può essere commesso il reato. In particolare queste possono, essere identificate:

- Gestione dei rapporti con l'autorità giudiziaria;
- Gestione del contenzioso giudiziale;
- Dichiarazioni nell'ambito di un procedimento giudiziario.

I principali attori si identificano nell'amministratore delegato e nel responsabile legale dell'ente. Sono previsti controlli diretti ad identificare la conformità delle attività aziendali ai principi espressi nel modello organizzativo.

L'art. 25 undecies disciplina i reati ambientali e dunque le seguenti ipotesi:

- violazione dell'articolo 452-bis; violazione dell'articolo 452-quater; violazione dell'articolo 452-quinquies; delitti associativi aggravati ai sensi dell'art.452 octies; delitto di traffico e abbandono di materiale ad alta radioattività ai sensi dell'articolo 452- sexies; violazione dell'articolo 727-bis; violazione dell'articolo 733 –bis; in relazione alla commissione dei reati previsti dal decreto legislativo 3 aprile 2006 n.152; per i reati di cui all'articolo 137; per i reati di cui all'articolo 256; per i reati di cui all'articolo 257; per la violazione dell'articolo 258, comma 4, secondo periodo; per la violazione dell'art.259, comma 1; per il delitto di cui all'art.260; per la violazione dell'art.260 bis; per la violazione dell'art.279, comma 5; in relazione alla commissione dei reati previsti dalla legge 7 febbraio 1991 n.150; per la violazione degli articoli 1, comma 1,2 commi 1 e 2 e 6 comma 4; per i reati del codice penale dell'articolo 3 bis, comma 1 della medesima legge n.150 del 1992

#### **- L'art. 25 – quinquiesdecies riguarda i reati tributari**

I reati-presupposto, sotto il profilo tributario sono connessi al Decreto legislativo 10 Marzo 2000 n.74:

- a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
- b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti
- c) per il delitto di dichiarazione fraudolenta mediante altri artifici,
- d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti,
- e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti,
- f) per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10,
- g) per il delitto di sottrazione fraudolenta al pagamento di imposte.

Con il d.l 124/2019 il legislatore ha inserito l'art. 25- quinquiesdecies , rubricato “reati tributari”, con cui ha ampliato il catalogo degli illeciti presupposto 231 alle due dichiarazioni fraudolente (art. 2 e 3 d.lgs. 74/2000), all'emissione di fatture o altri documenti per operazioni inesistenti (art.8 d.lgs 74/2000)), alla di- struzione ed occultamento di documenti contabili ( art.10 d.lgs 74/2000) e alla sottrazione fraudolenta al pagamento delle imposte.

Una delle più rilevanti fattispecie punisce coloro che distruggono od occultano, in tutto o in parte, documenti contabili, di cui è obbligatoria la conservazione, con il fine di evadere o di consentire a terzi di evadere le imposte, in modo tale da non permettere agli accertatori di ricostruire i redditi e il volume d'affari del contribuente

Le due fattispecie di sottrazione fraudolenta al pagamento delle imposte contenute nell'art 11 D.lgs 74/2000. Il primo comma della disposizione disciplina l'ipotesi classica del soggetto che, gravato da un debito tributario pari ad almeno 50.000 euro, riduca fittiziamente il proprio patrimonio, attraverso alienazioni simulate o altri atti fraudolenti, al fine di sottrarsi al pagamento delle imposte. Il secondo comma punisce, invece, chi, nel contesto di una transazione fiscale, al fine di ottenere un pagamento parziale dei tributi e degli accessori, indica nella documentazione relativa alla procedura minori elementi attivi effettivi o elementi passivi fittizi

Entrambe le fattispecie sono realizzate nell'interesse o a vantaggio dell'ente, che si sottrae (o, meglio, trattandosi di reati di pericolo concreto, compie atti diretti a sottrarsi) al pagamento delle imposte dovute

Ultimo requisito necessario affinché sorga la responsabilità dell'ente per i delitti di infedele e

omessa dichiarazione e di indebita compensazione e ` che dalla condotta “ consegua o possa conseguire un danno pari o superiore ai 10 milioni di euro”.

**Il presente MOG 231 contiene procedure e controlli volti ad impedire la commissione di reati tributari.**

Il modello tiene conto della bipartizione tra rischi diretti e indiretti nei processi aziendali: i primi “ includono l'attività di natura fiscale, come la presentazione delle dichiarazioni fiscali, la liquidazione e il versamento dei tributi, la regolare tenuta e custodia della documentazione obbligatoria”; i secondi riguardano “ le attività non di natura fiscale, ma con riflessi significativi sui processi direttamente ascrivibili alla sfera fiscale (gestione degli acquisisti di beni, servizi e delle commesse, delle vendite e ciclo degli incassi e pagamenti)

Pertanto, il modello 231 non si limita a verificare la presentazione della dichiarazione o il pagamento nei termini previsti dal Legislatore fiscale ma considera e a monte, le condotte da cui potrebbe scaturire l'evasione.

Particolare attenzione, allora, dovrà essere, ad esempio, dedicata alla verifica dei fornitori e al controllo della congruità dei prezzi pagati, all'effettivo pagamento e ricezione del bene o del servizio, alla corretta contabilizzazione.

Ancora, particolari rapporti contrattuali, notoriamente utilizzati per evadere il fisco vengono vagliati con maggiore attenzione: sponsorizzazioni, consulenze e rimborsi spese.

Identificati i processi a rischio e le procedure da adottare, viene implementata la formazione del personale coinvolto.

Ulteriori presidi sono:

- la correttezza dei flussi informativi, efficace ed attento disbrigo delle mansioni attribuite,
- l'adeguatezza delle responsabilità
- l'albo dei fornitori dell'ente, al fine di escludere eventuali soggetti con indici critici di affidabilità.
- la rotazione tra i dipendenti responsabili dell'autorizzazione degli incarichi di sottoscrizione di contratti di acquisto di impegno e spesa
- la sussistenza di criteri oggettivi al fine dell'accettazione di determinate proposte contrattuali
- la documentazione delle prestazioni di consulenza commerciale
- la rendicontazione puntuale delle note per le spese.

**GOIRC**  
**Modello Organizzativo D.Lgs. 231/01**

**PROCEDURA: PRO PA**

**REATI INERENTI LA PUBBLICA AMMINISTRAZIONE**  
**E LE AUTORITA' DI VIGILANZA E CONTROLLO**

**INDICE**

- 1. Finalità ed ambito di applicazione.**
- 2. Individuazione delle Responsabilità.**
- 3. Individuazione e Classificazione delle aree a rischio di commissione del reato.**
- 4. Principi generali di comportamento.**
- 5. Attività a rischio di commissione dei reati ex D.Lgs. 231/01.**
- 6. Protocolli generali di prevenzione.**
- 7. Protocolli specifici di prevenzione.**
- 8. Controllo operativo**
- 9. Flusso informativo all'Organismo di Vigilanza.**

## **PROCEDURA: PRO PA - AVC**

### **REATI INERENTI LA PUBBLICA AMMINISTRAZIONE E LE AUTORITA' DI VIGILANZA E CONTROLLO**

#### **1. Finalità ed ambito di applicazione.**

##### **La presente procedura:**

- disciplina gli aspetti relativi alla gestione ed al controllo delle attività che possono determinare la commissione dei reati relativi ai rapporti con la PA e con le autorità di vigilanza e controllo previsti negli artt. 24, 24 ter, 25 e 25 decies D.Lgs. 231/01.
- costituisce parte integrante del Modello 231 di organizzazione, gestione e controllo di GOIRC;
- agevola il monitoraggio dell'applicazione del Modello 231 da parte dell'OdV.

**Scopo della Procedura è prevenire la commissione, da parte dei soggetti indicati nel D.Lgs. 231/01, dei reati di cui al D.Lgs. 231/01, inerenti ai rapporti con la p.a. e, in particolare, previsti negli artt. 24, 24 ter, 25, 25 decies.**

**Nella presente Procedura il riferimento alla "PA", ai "soggetti pubblici" e agli "Enti pubblici" deve intendersi comprensivo della Pubblica Amministrazione e di tutte le Autorità di vigilanza e controllo cui è sottoposto GOIRC (Aifa, Garante per la protezione dei dati personali). Con il termine "Organo amministrativo" si intende il "Consiglio direttivo",**

#### **2. Individuazione delle Responsabilità.**

I reati esaminati e presidiati nella presente Procedura possono configurarsi nello svolgimento delle attività operative poste in essere da dipendenti e apicali di GOIRC e da tutti i destinatari del presente Modello 231.

Sono riportate, qui di seguito, in maniera specifica, le singole attività sensibili e le funzioni/ruoli responsabili.

**- Gestione di attività per la negoiazione o stipula di contratti e convenzioni con soggetti pubblici e relativi rapporti con gli stessi soggetti.**

In particolare:

- acquisizione di contratti o convenzioni per lo svolgimento di servizi affidati a GOIRC;
- negoziazione e stipula di eventuali convenzioni con Enti pubblici e altre Autorità per la gestione di attività e servizi svolti da GOIRC.

**- Gestione di attività per l'esecuzione dei contratti o convenzioni con soggetti pubblici e relativi rapporti con gli stessi soggetti.**

In particolare:

- esecuzione di convenzioni con Enti pubblici per la gestione delle attività di GOIRC;
- rendicontazione delle attività erogate verso il committente.

**- Attività di acquisizione e gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concessi da soggetti pubblici e relativi rapporti con gli stessi.**

In particolare:

- le attività volte a conseguire sovvenzioni o finanziamenti per la gestione di studi clinici e l'eventuale realizzazione di investimenti inerenti le strutture o il personale dell'Associazione.

**- Gestione di adempimenti necessari per il conseguimento e/o il rinnovo di autorizzazioni e/o certificati rilasciati da soggetti pubblici per l'esercizio dell'attività e dei relativi rapporti con gli stessi soggetti.**

In particolare:

- gestione delle attività necessarie per il rilascio del certificato di agibilità in caso di apertura di nuove sedi o stabilimenti di GOIRC;
- gestione delle attività necessarie per il rilascio delle autorizzazioni o per il rinnovo delle certificazioni e/o autorizzazioni da parte di Autorità di vigilanza e controllo.

**- Gestione delle procedure in occasione di appalti di forniture per beni e servizi connessi all'esercizio delle attività associative.**

In particolare:

- gestione dei bandi di gare/procedure negoziate/appalti relativamente all'acquisizione di beni o servizi.

**- Gestione delle attività di assunzione del personale ed incarichi professionali.**

In particolare:

- attività di selezione e assunzione delle risorse umane in osservanza della normativa vigente per gli Enti no profit e relativamente al profilo ricercato;
- attività relativa alla progressione del personale;
- banditura del concorso di selezione per l'assunzione del personale e gestione delle attività concorsuali.

**- Gestione dei rapporti con la P.A. in occasione di adempimenti in materia di lavoro, previdenza ed assistenza e nei casi di ispezioni, verifiche ed accertamenti relativi agli adempimenti stessi.**

In particolare:

- attività di supporto agli organi di controllo durante la verifica presso l'Ente;
- produzione di documenti, atti, delibere e quant'altro richiesto dall'Organo di controllo.

**- Gestione dei rapporti con la P.A. in occasione di adempimenti in materia fiscale e tributaria e nei casi di ispezioni, verifiche ed accertamenti relativi agli adempimenti stessi.**

In particolare:

- attività di supporto agli organi di controllo fiscali durante la verifica presso l'Azienda;
- produzione di documenti, atti, fatture, bilanci e quant'altro richiesto dall'Organo di controllo.

**- Gestione del contenzioso giudiziale e stragiudiziale e dei relativi contatti con l'Autorità giudiziaria.**

In particolare:

- gestione del contenzioso ordinario ove GOIRC sia parte processuale attiva del procedimento;
- gestione del contenzioso ordinario ove GOIRC sia parte processuale passiva del procedimento;
- gestione delle attività stragiudiziali connesse al contenzioso ordinario;
- attività di riscossione dei crediti ed avvio delle relative procedure esecutive.

**- Gestione dei rapporti con l'Autorità giudiziaria per indagini sull'Ente.**

In particolare:

- attività di supporto agli organi di controllo durante la fase di indagini che coinvolgono l'Associazione;
- gestione del procedimento legale in seguito all'avvio di un procedimento giudiziario nei confronti dell'Ente;
- gestione delle attività stragiudiziali connesse ai procedimenti giudiziari nei confronti dell'Associazione.

**- Gestione dei rapporti con la P.A. in occasione di adempimenti in materia societaria.**

In particolare:

- gestione delle attività di pubblicazione del bilancio di esercizio;
- attività di supporto agli organi di controllo durante la fase di verifica su operazioni di bilancio.

**- Altri rapporti con la P.A..**

In particolare:

- gestione delle attività che comportano contatti periodici o una tantum con la p.a.;
- gestione delle attività che comportano rapporti con la p.a. mediante l'intervento di consulenti o intermediari.

**3. Individuazione e Classificazione dei rischi di commissione del reato.**

La sottostante tabella riporta l'esito della classificazione del rischio di commissione del reato.

<b><u>Classificazione del rischio Reati</u></b>	<u>Molto basso</u>	<u>Basso</u>	<u>Medio</u>	<u>Alto</u>	<u>Molto alto</u>
Art. 318, 321, 322 c.1 e 3 c.p.		<u>x</u>			
Art. 319, 319		<u>x</u>			

ter, c. 1, 321, 322 c.2 e 4 cp					
Art. 317, 319 ter c.2, 319 quarter c.p.			<u>x</u>		
Art. 316 ter c.p.		<u>x</u>			
Art. 640 c.p.		<u>x</u>			
Art. 640 bis c.p.		<u>x</u>			
Art. 640 ter c.p.		<u>x</u>			
Art. 416 ter c.p.			<u>x</u>		
Art. 377 bis c.p.		<u>x</u>			
Art. 346 bis c.p.			<u>x</u>		

#### **4. Principi generali di comportamento.**

**Al fine di prevenire i reati relativi ai rapporti con la P.A., ciascun lavoratore e tutti i destinatari del Modello 231 devono osservare i principi contenuti nel Codice Etico, con specifico riferimento a quelli relativi ai rapporti con la p.a., nonché i seguenti principi generali di comportamento:**

- il sistema dei poteri e delle deleghe individua i soggetti che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno dell'Associazione e, in mancanza di delega specifica, nessun soggetto potrà operare con la P.A;
- i soggetti che, nella fase di gestione dei rapporti negoziali, intrattengono rapporti con la P.A. per conto di GOIRC, devono essere espressamente autorizzati;
- il personale non può dare seguito a richieste di indebiti vantaggi o tentativi di concussione o corruzione di cui dovesse essere destinatario o venire a conoscenza;
- i rapporti e gli adempimenti nei confronti della P.A. devono svolgersi con la massima trasparenza, diligenza e professionalità, fornendo indicazioni chiare, accurate, complete, fedeli e veritiere; evitando e, in ogni caso, segnalando situazioni di conflitto di interesse;
- in caso di ispezioni degli organi di P.A., partecipano agli incontri con i funzionari della P.A. almeno due soggetti, salvo che l'Autorità non richieda la presenza di un solo soggetto; il personale deve collaborare con gli organi di controllo durante le ispezioni nell'Ente rendendo dichiarazioni veritiere, conformi alla realtà associativa ed evitando, anche in sede di produzione documentale, di influenzare direttamente o indirettamente l'attività degli stessi organi di controllo.
- le spese per omaggi, consentite se di modico valore e tali da non pregiudicare l'integrità e la

reputazione di una delle parti, possono essere offerte o ricevute a condizione che siano: relative ad uno scopo legittimo, quali attività informative e/o divulgative delle attività e dei servizi di GOIRC; fornite senza l'aspettativa di decisioni favorevoli o vantaggi indebiti; ragionevoli, non frequenti e di modesto valore (per le spese di valore non modesto il personale deve ricevere formale autorizzazione da parte del Consiglio direttivo e le spese non possono essere pagate in contanti o con mezzi di pagamento equivalenti); eticamente appropriate e conformi alle abitudini ed alle prassi operative diffuse in GOIRC; approvate dall'organo amministrativo; documentate e contabilizzate correttamente nei libri contabili e nei registri; tracciate in apposito registro nel quale devono documentarsi: lo scopo dell'omaggio, le generalità della persona che le riceve, il nome dell'organizzazione ed il ruolo ricoperto dal destinatario, una descrizione degli omaggi, le generalità di altri partecipanti; l'importo;

- i servizi di GOIRC relativi alla gestione di beneficenze o sponsorizzazioni devono: effettuarsi soltanto in favore di enti regolarmente costituiti ai sensi di legge; essere conformi ai principi etici di GOIRC ed essere approvati dall'Organo Amministrativo; escludere situazioni di conflitto di interesse tra il soggetto beneficiario, i dirigenti di GOIRC e le P.A. coinvolte nelle attività;

- tutti gli omaggi, regalie, doni, di non modico valore, ricevuti da parte di soggetti esterni a GOIRC devono essere comunicati all'Organo amministrativo e le relative comunicazioni devono essere indirizzate all'OdV;

- il rilascio di autorizzazioni, concessioni, licenze a favore di GOIRC deve conseguirsi in seguito a puntuale osservanza della normativa vigente e, in particolare, la documentazione tecnica e amministrativa dovrà essere redatta secondo legge ed in base a criteri di liceità, correttezza e veridicità, non producendo documenti falsi o non rispondenti alla realtà.

#### **Con specifico riferimento all'attività contrattuale, occorre:**

garantire il confronto concorrenziale, definendo requisiti, chiari ed adeguati, di partecipazione alle gare, anche ufficiose, e di valutazione delle offerte; verificare la congruità dei prezzi di acquisto di beni e servizi effettuati mediante comparazione con i prezzi correnti di mercato rilevabili e dandone atto nei provvedimenti di spesa; conferire incarichi di consulenza, studio e ricerca a soggetti esterni soltanto previa verifica dell'eventuale presenza di professionalità interne; acquisire all'atto dell'insediamento di nuovi dipendenti apicali o collaboratori dichiarazioni di inesistenza di rapporti di parentela o di lavoro o professionali con i partecipanti alla gara od al concorso.

#### **Al medesimo fine (prevenzione dei reati relativi ai rapporti con la P.A.) è vietato:**

esibire documenti incompleti e/o comunicare dati falsi o alterati alle P.A.; tenere una condotta ingannevole che possa indurre la P.A. in errore; chiedere o indurre la P.A. a trattamenti di favore o sussidi o finanziamenti agevolati, attraverso la promessa di denaro o di altre utilità; promettere o effettuare elargizioni in denaro a pubblici funzionari, pagamenti o compensi sotto qualsiasi forma, per indurre, facilitare o remunerare una decisione, al fine di promuovere o favorire interessi dell'Ente; effettuare pagamenti in contanti; accordare vantaggi di qualsiasi natura (promesse di assunzioni, ecc.) in favore di rappresentanti della P.A. che influenzino l'indipendenza di giudizio o inducano ad assicurare un vantaggio per l'Ente; effettuare prestazioni o riconoscere compensi in favore della P.A. controparte negoziale che non trovino adeguata giustificazione nell'ambito del rapporto contrattuale e/o di collaborazione con la stessa; intrattenere rapporti economici, diretti o indiretti, di collaborazione o di consulenza con fornitori dell'Ente di beni, appalti o lavori ovvero con

soggetti abilitati al controllo delle attività erogate da GOIRC che possano effettuare i controlli sulla sua attività; stabilire rapporti di consulenza con soggetti che hanno subito condanne relative a reati inerenti ai rapporti con la P.A.; impedire il controllo da parte degli organismi di controllo; affidare incarichi a consulenti esterni o fornitori esterni eludendo criteri documentabili e obiettivi incentrati su competitività, utilità, prezzo, integrità; favorire indebitamente gli interessi dell'Ente inducendo a tacere o a mentire la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale.

## **5. Attività a rischio commissione reati ex D.Lgs. 231/01.**

Le attività, svolte da GOIRC nell'ambito dei rapporti intercorrenti con la P.A., che possono determinare situazioni a rischio di reato sono state precedentemente indicate nella Parte Generale del MOG 231 di GOIRC e vengono più specificamente descritte nella presente Procedura.

## **6. Protocolli generali di prevenzione.**

GOIRC ha predisposto i seguenti protocolli generali di prevenzione, distinti nelle fasi progressive di: formazione delle decisioni, attuazione delle decisioni, controllo delle decisioni:

### **6.1 Formazione delle decisioni.**

Nelle fasi di trattazione e di istruttoria degli atti funzionali all'adozione delle decisioni, è necessario: rispettare, ove ne sussistano le condizioni, l'ordine cronologico di acquisizione e/o protocollo dell'istanza; predeterminare i criteri di assegnazione delle pratiche ai collaboratori; agevolare lo svolgimento del procedimento e dell'azione dell'Ente; distinguere, ove ne ricorrano le condizioni, l'attività istruttoria dall'adozione dell'atto conclusivo, coinvolgendo nel procedimento, ove possibile, due soggetti: motivare gli atti in modo congruo, adeguato e proporzionato al margine di discrezionalità; osservare i principi di semplicità e di chiarezza nella redazione degli atti, scritti con linguaggio semplice e comprensibile a tutti, utilizzando, per quanto possibile, uno stile comune e riportando nella premessa dei provvedimenti conclusivi il preambolo (descrive il procedimento svolto e indica tutti gli atti prodotti e considerati per pervenire alla decisione finale) e la motivazione (precisa, chiara e completa nonché adottata in base all'istruttoria, contiene i presupposti di fatto e le ragioni giuridiche della decisione).

### **6.2 Attuazione delle decisioni.**

La fase di attuazione delle decisioni deve espletarsi con puntuale osservanza della normativa vigente al fine di consentire, tra l'altro, la tracciabilità dei provvedimenti adottati.

A tal fine, occorre:

- verificare ed integrare, con continuità, l'elenco dei Fornitori, compresi i prestatori d'opera intellettuale;
- redigere ed integrare il funzionigramma dell'Associazione in modo puntuale, definendo con chiarezza i ruoli ed i compiti dei singoli dipendenti, apicali e collaboratori;
- completare la digitalizzazione dell'attività, garantendo la totale trasparenza e tracciabilità;
- rilevare i tempi medi dei pagamenti e di conclusione dei procedimenti;

- istituire un registro dei contratti dell'Associazione, in formato elettronico, nel quale annotare, in modo progressivo, i dati relativi alla controparte, l'importo del contratto e la durata ed allegare la scansione dei contratti sottoscritti;
- vigilare sull'esecuzione dei contratti di appalto di lavori, beni e servizi, compresi i contratti d'opera professionale, applicando, se del caso, penali e clausole risolutive, e proporre, ove necessario, azione per l'inadempimento e/o di danno.

### **6.3 Controllo delle decisioni.**

Nell'ambito dello svolgimento della fase di controllo delle decisioni occorre osservare le seguenti prescrizioni: garantire il rispetto delle Procedure e dei Regolamenti di GOIRC.

### **7. Protocolli specifici di prevenzione.**

I seguenti protocolli specifici di prevenzione sono volti a prevenire la commissione dei reati ex D.Lgs. 231/01 inerenti la P.A. nell'ambito delle aree sensibili, individuate attraverso l'analisi dei rischi svolta.

#### **7.1 Attività relative all'acquisizione, negoziazione e stipula di contratti o convenzioni con la PA.**

Il processo di acquisizione, negoziazione e stipula si articola nelle seguenti fasi: gestione dei rapporti pre-contrattuali con la P.A. che possano condurre ad un contratto; perfezionamento del contratto con la P.A., con predisposizione delle informative necessarie alla successiva fase di gestione del contratto stesso.

Al fine di prevenire i reati inerenti la P.A., GOIRC deve osservare: la presente Procedura e, dunque, i Principi generali ed i Protocolli generali di prevenzione sopra esposti, il Sistema generale di prevenzione di cui al presente Modello 231 e quanto prescritto nel Codice Etico e nelle Procedure aziendali applicabili alle attività sensibili individuate.

**Gli atti e documenti suindicati e le prassi utilizzate da GOIRC devono essere integrate, osservando, in modo puntuale, le seguenti prescrizioni:**

- terminata la fase pre-contrattuale, gli atti, provvedimenti e documenti utili alla conclusione del contratto vengono trasmessi ai Consulenti esterni e all'Organo Amministrativo per l'approvazione necessaria alla stipula del contratto;
- la stipula del contratto viene formalizzata e perfezionata mediante redazione e sottoscrizione di contratto nella forma giuridica prevista dalla normativa vigente per la sua validità ed efficacia;
- l'atto negoziale stipulato contiene tutti gli elementi essenziali richiesti per legge e, in particolare: oggetto dei lavori, forniture e servizi affidati; importo del corrispettivo delle prestazioni di servizi assunte da GOIRC; condizioni di esecuzione; inizio e termine del contratto; modalità di pagamento; penalità e diritto di risolvere il contratto in caso di inadempimento; elementi ulteriori richiesti dalla normativa applicabile.

## **7.2 Attività relative all'esecuzione dei contratti o convenzioni con soggetti pubblici.**

Stipulato il contratto con la P.A., tale attività diventa oggetto dei servizi erogati da GOIRC, rivolti ad altri enti pubblici.

Il processo di esecuzione dei rapporti contrattuali con la P.A. si articola, all'interno di GOIRC, nelle seguenti fasi:

- pianificazione delle risorse ed attività per la corretta esecuzione del servizio;
- esecuzione del contratto;
- rendicontazione sull'esecuzione del contratto.

## **7.3 Attività di acquisizione e gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concessi da soggetti pubblici.**

A) La gestione delle attività inerenti all'acquisizione di contributi, sovvenzioni o finanziamenti in favore di GOIRC per la realizzazione di obiettivi previsti nell'atto costitutivo e nello statuto comporta l'esposizione di GOIRC a reati connessi ad un'eventuale corruzione dell'ente erogatore al fine di ottenere i contributi o i finanziamenti.

Il personale di GOIRC deve espletare con particolare attenzione le seguenti procedure:

- richiesta di investimento, modalità di finanziamento, costi per GOIRC, descrizione dell'investimento e obiettivi attesi dallo stesso;
- valutazione comprovante che la scelta del finanziamento proposta sia la meno onerosa per GOIRC (confronti tra strumenti di finanziamento alternativi quali mutui, prestiti bancari, *leasing*, ecc.).

B) Il processo di acquisizione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concessi da soggetti pubblici si articola nelle seguenti fasi:

- proposta a cui si riferisce l'investimento, sull'opportunità di avvalersi di un'agevolazione pubblica con redazione di una Relazione di valutazione;
- approvazione da parte dell'Organo Amministrativo della proposta di investimento.

Tutta la documentazione deve essere correttamente archiviata in apposito fascicolo per consentirne la puntuale verifica nel tempo.

C) In caso di valutazione positiva sull'opportunità di richiedere la sovvenzione pubblica, GOIRC dovrà curare l'istruttoria della pratica e verificare, in particolare, la coerenza con le richieste del "bando" di tutti i dati attinenti all'Ente e la coerenza tra la documentazione da presentare e quella specifica richiesta dal "bando".

Accertato l'esito del finanziamento ed ottenuti gli estremi della delibera dell'Associazione, GOIRC avvia l'investimento o la spesa entro i termini previsti.

**Lo svolgimento corretto delle attività di gestione degli adempimenti necessari per il conseguimento e/o il rinnovo di autorizzazioni e/o certificati rilasciati da soggetti pubblici per l'esercizio delle attività dell'Associazione,** presuppone che siano individuate, documentate e tracciate le responsabilità nelle fasi di:

predisposizione della documentazione; invio della documentazione richiesta ed archiviazione della pratica; gestione dei rapporti con gli enti pubblici; assistenza in occasione di sopralluoghi ed accertamenti da parte degli enti; gestione dei rapporti con gli enti pubblici per il ritiro dell'autorizzazione e l'esecuzione degli adempimenti.

**Le prassi utilizzate da GOIRC devono essere integrate riportando, in modo chiaro ed inequivoco, le seguenti indicazioni:**

- copia della documentazione consegnata per la richiesta di autorizzazione o per l'esecuzione di adempimenti deve essere conservata presso l'Ente riportando le responsabilità ed i luoghi dell'archiviazione;
- è necessario rispettare le procedure e le regole previste nel Codice Etico per consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate;
- è necessario provvedere alla corretta archiviazione e conservazione della documentazione di competenza prodotta, inerente l'esecuzione degli adempimenti svolti in sede di attività relative alla richiesta di autorizzazioni alla P.A..

#### **7.4 Gestione delle attività di assunzione del personale ed incarichi professionali.**

L'attività di gestione delle assunzioni del personale può determinare il configurarsi di reati rilevanti ai sensi del D.Lgs. 231/01 in ragione di potenziali condotte corruttive realizzate all'interno dell'Associazione.

In particolare, tali reati potrebbero configurarsi in seguito ad una gestione non trasparente del processo di selezione ed assunzione del personale consistenti in una condotta idonea a favorire soggetti, candidati o consulenti esterni, che hanno rapporti con l'Ente, per ottenere condizioni economiche più favorevoli con riduzione dei costi per GOIRC.

**Le attività specifiche che possono integrare i reati sopra indicati sono riconducibili alle seguenti:**

- acquisizione e progressione del personale;
- affidamento di incarichi professionali a consulenti/esperti esterni a GOIRC.

La gestione delle attività di acquisizione e progressione del personale è regolata nella normativa vigente ove applicabile a tali attività sensibili.

I Regolamenti, le procedure e le prassi operative dell'Ente integrano la disciplina sopra esposta, prevedendo regole e procedure idonee alla corretta gestione delle fasi di selezione (pre-selezione, selezione e prove di esame), valutazione e nomina dei candidati volta a garantire il rispetto, da parte di GOIRC, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità.

#### **7.5 Gestione dei rapporti con la P.A. in occasione di adempimenti in materia di lavoro, previdenza ed assistenza e nei casi di ispezioni, verifiche ed accertamenti relativi agli adempimenti stessi.**

L'espletamento di tali attività può esporre GOIRC a situazioni in cui i soggetti sottoposti all'ispezione possano avviare processi corruttivi per pregiudicare l'indipendenza di giudizio degli Organi di controllo.

In materia di lavoro si individuano le seguenti specifiche attività:

- attività di supporto agli organi di controllo durante lo svolgimento di verifiche presso l'Ente;
- produzione di documenti, atti, delibere, in risposta alle richieste dell'organo di controllo.

L'attività dev'essere effettuata seguendo la normativa vigente, il Sistema generale di prevenzione del presente Modello 231 e le regole operative dettate dal Codice Etico.

In caso di ispezione da parte di rappresentanti della P.A. il Responsabile del servizio interessato dall'ispezione inoltra immediatamente segnalazione al Consiglio direttivo.

Durante i controlli devono essere presenti, ove possibile, almeno due persone appartenenti all'Associazione.

Il Responsabile dell'area verificata e, in ogni caso, l'Organo amministrativo, deve:

identificare l'ente pubblico al quale il personale ispettivo appartiene; fornire la massima collaborazione all'Ente Pubblico richiedente; garantire che tutti i documenti indirizzati a soggetti pubblici o terzi siano firmati da un dirigente entro i limiti della delega conferitagli; garantire, nel corso dell'attività ispettiva, massima collaborazione all'espletamento degli accertamenti; non indurre alcun lavoratore a fornire dichiarazioni mendaci alla P.A. che effettua il servizio; redigere una specifica nota sull'andamento dell'ispezione, ove la P.A. non dovesse rilasciare alcun verbale o in accompagnamento a questo; provvedere alla corretta conservazione dei verbali redatti dalle pubbliche autorità.

**A questi fini, è fatto divieto a qualunque dipendente o apicale:**

- esibire documenti incompleti e/o comunicare dati falsi o alterati alle Autorità di controllo in materia di lavoro e previdenza;
- tenere una condotta ingannevole che possa indurre l'Organo che effettua l'ispezione in errore;
- promettere o effettuare elargizioni in denaro a pubblici funzionari, pagamenti o compensi sotto qualsiasi forma, per indurre, facilitare o remunerare una decisione o il compimento di un atto di ufficio della P.A..

#### **7.6 Gestione dei rapporti con la P.A. in occasione di adempimenti in materia fiscale e tributaria e in casi di ispezioni, verifiche ed accertamenti relativi agli adempimenti stessi.**

Le attività di gestione dei rapporti con la P.A. può esporre GOIRC a situazioni in cui i soggetti sottoposti all'ispezione possano avviare processi corruttivi al fine di pregiudicare l'indipendenza di giudizio da parte degli Organi di controllo.

Le attività specifiche relative agli adempimenti in materia fiscale possono essere:

- attività di supporto agli organi di controllo fiscale durante la verifica presso l'Organizzazione;
- produzione di documenti, atti, fatture, bilanci, delibere e quant'altro richiesto all'Ente in risposta alle richieste dell'organo di controllo.

In ordine ai principi ed al controllo, ai comportamenti da assumere durante le ispezioni ed ai comportamenti vietati, si applica quanto prescritto nel punto relativo alla gestione dei rapporti con la P.A. in occasione di adempimenti in materia di lavoro, previdenza ed assistenza.

#### **7.7 Gestione del contenzioso giudiziario e stragiudiziario e dei relativi contatti con l'Autorità Giudiziaria.**

L'attività di gestione dei contenziosi giudiziari che coinvolgono GOIRC può esporre l'Ente a situazioni in cui gli incaricati di gestire i rapporti possano avviare processi corruttivi, anche in atti giudiziari, al fine di far rendere il giudizio a proprio favore.

Le attività di questo genere sono, a titolo esemplificativo:

- gestione del contenzioso ordinario ove GOIRC sia parte attiva del procedimento;
- gestione del contenzioso ordinario ove GOIRC sia parte passiva del procedimento;

- gestione delle attività stragiudiziali legate al contenzioso ordinario;
- attività di riscossione dei crediti e procedure di esecuzione per la riscossione coattiva.

Qualora GOIRC, o un suo dipendente nell'ambito della sua attività lavorativa, sia coinvolto in un procedimento giudiziale, devono essere scrupolosamente osservate tutte le inerenti norme, sostanziali e procedurali, nonché dei rispettivi codici deontologici.

### **7.8 Attività di gestione dei rapporti con l'Autorità Giudiziaria per le indagini che coinvolgono l'Ente.**

Le attività di gestione dei rapporti con l'Autorità Giudiziaria sono inquadrabili nell'ambito della procedura relativa alla gestione del contenzioso giudiziale e stragiudiziale e dei relativi contatti con l'Autorità Giudiziaria.

In caso di indagini e rapporti con l'Autorità giudiziaria che coinvolgono GOIRC, l'Ente può, infatti, incorrere in situazioni in cui i soggetti incaricati di gestire i rapporti con l'Autorità Giudiziaria possano avviare processi corruttivi, anche in atti giudiziari, al fine di modificare la decisione dell'Autorità Giudiziaria.

Le attività di questo genere sono, a titolo esemplificativo:

- attività di supporto agli organi di controllo durante le fasi di indagini ed istruttoria che coinvolgono GOIRC;
- gestione del procedimento legale in seguito all'avvio di un procedimento giudiziario nei confronti dell'Organizzazione;
- gestione delle attività stragiudiziali legate ai procedimenti giudiziari nei confronti dell'Ente.

Si osservano le medesime prescrizioni di cui al precedente punto

### **7.9 Gestione dei rapporti con la P.A. in occasione di adempimenti associativi**

Le attività specifiche relative agli adempimenti in materia associativa sono di seguito elencate: gestione delle attività di pubblicazione del bilancio di esercizio; attività di supporto agli organi di controllo durante la fase di verifica su operazioni di bilancio.

A tal proposito assumono rilevanza i rapporti tra GOIRC e gli Organi di controllo in occasione delle attività di verifica e controllo svolte da tali Organi in osservanza alla legge.

GOIRC applica le Procedure Operative relative ai reati in materia societaria, tributaria e di antiriciclaggio.

GOIRC adeguerà il proprio comportamento a quanto sopra esposto nel presente protocollo; in ogni caso, i responsabili dei servizi di GOIRC sono tenuti alla massima diligenza, professionalità, trasparenza, collaborazione, disponibilità ed al pieno rispetto del ruolo istituzionale degli stessi, dando puntuale e sollecita esecuzione alle prescrizioni ed agli eventuali adempimenti degli Organi di controllo.

### **7.10 Gestione delle attività che comportano contatti periodici o una tantum con la p.a..**

In particolare: gestione delle attività che comportano rapporti con la p.a. mediante l'intervento di consulenti o intermediari.

GOIRC effettua periodicamente una ricognizione dei diversi consulenti/intermediari ingaggiati, al

fine di mappare in maniera completa tutte le attività attualmente in essere che comportano rapporti con la P.A. mediante il loro supporto, assicurando che ciascuna di esse abbia il proprio fondamento in appositi contratti o lettere di incarico che disciplinino compiutamente l'oggetto e le attività che il consulente/intermediario può svolgere.

Nel caso di impiego di consulenti o intermediari nella stipula di rapporti contrattuali con la P.A., nell'espletamento di attività inerenti la richiesta di autorizzazioni, nell'esecuzione di adempimenti verso la P.A. e/o nella gestione di contenziosi con la P.A., GOIRC acquisisce in originale una lettera di incarico/affidamento dell'attività, unitamente alla lettera di incarico accettata dalla Ditta o dal professionista, lettera che deve contenere: apposita dichiarazione di conoscenza della presente procedura; impegno espresso al rispetto delle norme prescrittive in essa contenute.

- L'Associazione verifica periodicamente la fase di contrattualizzazione del rapporto negoziale con i consulenti/intermediari, accertando il rispetto del sistema dei poteri autorizzativi e di firma all'interno dell'Ente/Organizzazione di controparte e verificando il contenuto del contratto ed il profilo di rischio specifico.

**Nella gestione delle attività relative a rapporti con le P.A.-AVC non richiamati nel presente Protocollo si fa riferimento alle regole esposte nel Codice Etico e nel Sistema generale di prevenzione.**

## **8. Controllo Operativo.**

Il controllo operativo viene effettuato in conformità alle Procedure aziendali ed al presente Modello 231 e, in particolare, ai Protocolli Generali della presente Procedura PRO – PA (segnatamente fasi di formazione, attuazione e controllo decisioni), oltre che mediante puntuale ed idonea gestione dei flussi informativi con l'OdV.

## **9. Flusso informativo all'Organismo di Vigilanza.**

Verso l'**Organismo di Vigilanza** di GOIRC devono essere inviati i seguenti documenti, atti, notizie, informazioni, dai soggetti di seguito indicati:

**dall'Organo Amministrativo e/o dai Dirigenti** (con cadenza annuale):

- un report dei finanziamenti, contributi, sovvenzioni ricevute dalla P.A.;
- elenco dei report degli omaggi ricevuti dall'Azienda o dai dipendenti che superino il modico valore;

**dall'Organo Amministrativo e/o dai Dirigenti (al verificarsi degli eventi):**

- copia dei provvedimenti, verbali di accertamento, sanzionatori o atti ingiuntivi emanati e notificati dalle Autorità competenti di controllo in materia di lavoro, previdenza, ambiente, sicurezza, fisco, tributi, società.

In merito alle attività che comportano contatti periodici o una tantum con la p.a. devono essere garantiti i flussi informativi della presente procedura.

In ordine all'affidamento di beni e servizi aziendali va rispettato il flusso informativo previsto nella Presente Procedura.

**GOIRC**  
**Modello Organizzativo D.Lgs. 231/01**

**PROCEDURA: PRO SIC**  
**REATI SICUREZZA**  
**NEI LUOGHI DI LAVORO**

## **INDICE**

- 1. Finalità ed ambito di applicazione.**
- 2. Individuazione delle Responsabilità.**
- 3. Individuazione e classificazione dei rischi di commissione del reato.**
- 4. Principi generali di comportamento.**
- 5. Attività a rischio di commissione dei reati previsti nel D.Lgs. 231/01.**
- 6. Protocolli generali di prevenzione.**
- 7. Protocolli specifici di prevenzione.**
- 8. Controllo Operativo.**
- 9. Attività dell'Organismo di Vigilanza e flussi informativi.**

## **PROCEDURA: PRO - SIC**

### **REATI SICUREZZA** **NEI LUOGHI DI LAVORO**

#### **1. Finalità ed ambito di applicazione.**

##### **La presente procedura:**

- disciplina gli aspetti relativi alla gestione ed al controllo delle attività che possono determinare la commissione dei reati in materia di sicurezza nei luoghi di lavoro previsti nell'art 25 septies D.Lgs. 231/01;
- costituisce parte integrante del Modello 231 di GOIRC;
- agevola il monitoraggio dell'applicazione del Modello 231 da parte dell'Organismo di Vigilanza.

**Scopo della Procedura è prevenire la commissione, da parte dei soggetti indicati nel D.Lgs. 231/01, dei seguenti reati:**

Art. 25 septies D.Lgs 231/01: “Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro”.

- Art. 589 c.p. - “Omicidio colposo”;
- Art. 590, comma 3, c.p. - “Lesioni colpose”.

#### **2. Individuazione delle responsabilità.**

I reati esaminati e presidiati nella presente Procedura possono configurarsi nello svolgimento delle attività operative poste in essere dai singoli lavoratori e da ogni destinatario del Modello 231.

#### **3. Individuazione e Classificazione dei rischi di commissione del reato.**

La sottostante tabella riporta l'esito della classificazione del rischio di commissione del reato descritta nel Modello 231 per i soggetti responsabili indicati nel paragrafo precedente

##### **Classificazione dei rischi di commissione del reato.**

<b><u>Classificazione rischio Reati</u></b>	<b><u>Molto basso</u></b>	<b><u>Basso</u></b>	<b><u>Medio</u></b>	<b><u>Alto</u></b>	<b><u>Molto alto</u></b>
Art. 589 bis c.p.		<u>x</u>			
Art. 590 c. 3 c.p.		<u>x</u>			

#### **4. Principi generali di comportamento.**

**Al fine di prevenire i reati in materia di salute e sicurezza dei lavoratori, ciascun lavoratore e ogni destinatario del Modello 231 dovrà innanzitutto rispettare i principi di comportamento ed i divieti di seguito esposti.**

##### **4.1 Principi generali di comportamento:**

- adottare comportamenti diligenti e prudenti quanto alla salvaguardia della propria salute e della propria sicurezza, conformi alla propria formazione ed esperienza nonché alle istruzioni e ai mezzi forniti ovvero predisposti dal datore di lavoro;
- osservare la normativa e le procedure aziendali interne al fine della protezione collettiva ed individuale, esercitando in particolare, tutti i controlli e le attività idonee a salvaguardare la salute e la sicurezza dei collaboratori esterni e/o di persone estranee, eventualmente presenti sul luogo di lavoro;
- segnalare immediatamente ai livelli opportuni (in ragione delle responsabilità attribuite) le anomalie dei mezzi e dei dispositivi nonché le altre eventuali condizioni di pericolo di cui viene a conoscenza;
- adoperarsi direttamente, a fronte di un pericolo rilevato e nei soli casi di urgenza, compatibilmente con le proprie competenze e possibilità;
- sottoporsi ai controlli sanitari previsti;
- contribuire all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

##### **4.2 Divieti:**

- rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- compiere di propria iniziativa operazioni o manovre non di propria competenza ovvero che compromettano la sicurezza propria o di altri lavoratori.

#### **5. Attività a rischio di commissione dei reati previsti nel D.Lgs. 231/01**

L'individuazione delle aree sensibili effettuata in seguito all'analisi dei rischi ha permesso di identificare le attività a rischio reato (il relativo elenco è soggetto a costante aggiornamento), svolgendo le quali potrebbero configurarsi i reati inerenti alla salute e sicurezza sul lavoro previsti nel D.Lgs. 231/01.

#### **6. Protocolli generali di prevenzione.**

**6.1** GOIRC assicura il miglioramento continuo dell'identificazione, valutazione e gestione degli aspetti che possono influenzare o influenzano la salute e la sicurezza dei lavoratori attraverso:

- l'assegnazione di precise regole e responsabilità connesse al rispetto delle prescrizioni legali in materia di salute e sicurezza sul lavoro;
- il monitoraggio, ove necessario, degli aspetti che influenzano tali rischi e la conseguente attività di analisi e di miglioramento.

**6.2** Per prevenire eventuali situazioni a rischio di reato in materia di sicurezza occorre

**eseguire, in modo corretto, le seguenti attività operative:**

- valutazione preliminare ed eventuale aggiornamento di tutti i rischi;
- individuazione delle misure di tutela e delle risorse necessarie all'eliminazione o al contenimento dei rischi per la salute e sicurezza dei lavoratori;
- definizione delle responsabilità dell'Ente in materia di sicurezza;
- formazione del personale, generale e specifica.

**6.3 In merito alle misure di prevenzione per le attività a rischio di reato, il Modello 231 è adottato ed attuato al fine di garantire l'adempimento di tutti gli obblighi giuridici relativi ai seguenti aspetti generali:**

- attività di informazione e formazione dei lavoratori;
- attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- acquisizione di documenti e certificazioni obbligatorie di legge;
- periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate;
- necessarie comunicazioni, ove previsto, alle autorità competenti.

## **7. Protocolli specifici di prevenzione.**

**Al fine di prevenire i reati inerenti la sicurezza nei luoghi di lavoro, GOIRC si impegna a rispettare i seguenti protocolli specifici di prevenzione:**

### **7.1 Valutazione dei rischi**

L'Organo Amministrativo valuta tutti i rischi per la salute e la sicurezza dei lavoratori nel rispetto degli standard tecnico-strutturali di legge relativi ad attrezzature, luoghi di lavoro, agenti chimici, fisici e biologici.

Individuati i pericoli in funzione della possibile esposizione dei lavoratori, si provvede all'identificazione dei rischi.

L'identificazione, rielaborata periodicamente al fine di tenere sotto controllo i pericoli, viene effettuata previa definizione di un criterio specifico che prevede la definizione del danno e la probabilità di accadimento.

Le attività relative all'identificazione dei pericoli e alla valutazione dei rischi sono aggiornate in relazione a nuovi processi o fasi o ad intervenute modifiche rilevanti degli stessi.

**In particolare, la valutazione dei rischi viene effettuata attraverso tre fasi fondamentali:**

- **identificare le sorgenti di rischio:** cioè individuare tutti gli agenti potenziali che possono provocare danni di tipo infortunistico o alla salute dei lavoratori sulla base di considerazioni legate al tipo dei processi tecnologici o attività effettuate dall'Ente, alle apparecchiature impiegate, alle caratteristiche generali degli ambienti di lavoro ed al numero di dipendenti operanti nei vari ambienti di lavoro;
- **stimare i rischi di esposizione,** cioè valutare l'entità del rischio, per ogni sorgente individuata, in base alla probabilità di accadimento dell'evento negativo ed all'entità del danno da esso provocato; questa stima va condotta tenendo in considerazione le misure preventive o protettive già presenti e deve pertanto dare informazioni sull'entità dei rischi residui;
- **decidere se il rischio è tollerabile:** si tratta di giudicare, per ogni pericolo individuato, se le esistenti misure di sicurezza garantiscono che il pericolo sia adeguatamente controllato e che siano rispettate le prescrizioni legislative applicabili.

## **7.2 Definizione delle specifiche responsabilità – Attuazione delle misure preventive**

I soggetti eventualmente individuati per la gestione di problematiche inerenti la salute e sicurezza nei luoghi di lavoro devono possedere specifici requisiti tecnico-professionali, mantenuti nel tempo, acquisiti prima dell'attribuzione dell'incarico e conseguiti anche attraverso specifici interventi formativi.

In ogni caso, GOIRC deve:

1. Disporre e adottare tutte le prescritte e necessarie misure e apparati stabiliti dalla vigente normativa generale e specifica in materia di prevenzione degli infortuni di igiene e sicurezza del lavoro e, in particolare, del D.Lgs. 81/08 necessari e/o opportuni in relazione alle attuali acquisizioni scientifiche e/o tecnologiche, in modo tale da garantire la piena incolumità dei lavoratori dipendenti nonché di quelli autonomi e, comunque, dei terzi eventualmente presentati, e da evitare il verificarsi di qualsivoglia danno a persone e cose;

2. Assumere tutte le iniziative che riterrà più confacenti ed opportune per:

- accertare la conoscenza delle norme vigenti in materia di sicurezza sul lavoro, adoperandosi, se del caso, a scopo di completamento e di approfondimento, che vengano illustrate metodicamente le necessarie nozioni;

- aggiornare tempestivamente tutti i dipendenti sulle innovazioni legislative e/o tecniche che comportino o suggeriscano l'adozione di nuove o diverse misure antinfortunistiche;

- eseguire e disporre opportuni controlli, sopralluoghi o visite onde accertare, con la necessaria periodicità, l'applicazione puntuale e costante delle più idonee misure antinfortunistiche da parte dei preposti;

- adottare, se del caso, provvedimenti disciplinari nei confronti dei dipendenti che incorrano in violazioni delle norme e delle istruzioni da applicare;

- mantenere i contatti, curare gli adempimenti, svolgere ogni pratica necessaria nei confronti degli istituti assicurativi, pubblici e privati, degli enti di prevenzione di infortuni e di controllo (INAIL, DPL, ASL, ecc) rappresentando l'Ente per quanto occorra con facoltà all'uopo di delegare di volta in volta altri dipendenti;

- rappresentare l'Associazione nelle ispezioni amministrative e nelle richieste giudiziarie.

3. Dare attuazione alle norme del D.Lgs. n. 81/08 e, in particolare, dell'art. 30.

## **7.3 Formazione.**

GOIRC verifica, con periodicità annuale, le esigenze formative di tutto il personale in materia di sicurezza.

La formazione deve avvenire, quantomeno, all'atto della costituzione del rapporto di lavoro o all'atto del trasferimento o cambiamento di mansioni e dell'introduzione di nuove attrezzature di lavoro o di nuove tecnologie, di nuove sostanze e preparati pericolosi.

## **8. Controllo Operativo.**

L'Associazione realizza efficacemente un controllo strategico degli adempimenti in materia di sicurezza, provvedendo, tra l'altro, con cadenza temporale prefissata, alla verifica sul posto di lavoro

dell'applicazione delle misure di salute e sicurezza nonché all'organizzazione della simulazione di emergenza.

## **9. Attività dell'Organismo di Vigilanza e flussi informativi.**

**A conferma ed integrazione della regolamentazione dei flussi informativi effettuata nello Statuto dell'Odv di cui alla Parte generale del presente Modello 231, si prevede che all'Organismo debbano pervenire i seguenti documenti, notizie ed informazioni:**

**Verso l'Organismo di Vigilanza** devono essere inviati i seguenti documenti, atti, notizie, informazioni, da parte dei soggetti di seguito indicati:

- proveniente dal RSPP e/o da altro responsabile e/o referente interno, relazione (con cadenza annuale), che dia conto di:
  - eventuali violazioni, da parte dei lavoratori, delle prescrizioni relative all'utilizzo dei DPI;
  - eventuali malfunzionamenti dei DPI;
  - eventuali sanzioni inflitte ai lavoratori per omesso uso dei DPI;
  - aggiornamenti ed integrazioni della valutazione dei rischi e/o di analoghi documenti;
- provenienti dall'Organo Amministrativo e da RSPPe/o da altro responsabile e/o referente interno (al verificarsi degli eventi o con cadenza annuale):
  - verbale di riunione periodica sicurezza e report incidenti (con cadenza annuale);
  - relazione in merito agli eventi formativi dei dipendenti e report relativi ai sopralluoghi ed alle simulazioni di emergenza effettuate (con cadenza annuale);
  - segnalazioni e registrazioni di eventi di emergenza in materia di sicurezza sul lavoro (al verificarsi dei singoli eventi o con cadenza annuale).

**GOIRC**

**Modello Organizzativo ai sensi del D.Lgs. 231/01**

**PROCEDURA: PRO - INF**

**REATI DA DELITTI INFORMATICI**  
**E TRATTAMENTO ILLECITO DEI DATI**

## **INDICE**

- 1. Finalità ed ambito di applicazione.**
- 2. Individuazione delle Responsabilità.**
- 3. Individuazione e Classificazione dei rischi di commissione del reato.**
- 4. Attività a rischio di commissione dei reati ex D.Lgs. 231/01.**
- 5. Principi generali di comportamento.**
- 6. Protocolli generali di prevenzione.**
- 7. Protocolli specifici di prevenzione;**
- 8. Controllo Operativo**
- 9. Flusso informativo all'Organismo di Vigilanza.**

## **1. Finalità ed ambito di applicazione.**

La presente Procedura:

- disciplina gli aspetti relativi alla gestione ed al controllo delle attività che possono determinare la commissione dei reati informatici e trattamento illecito nonché in tema di violazione dei diritti d'autore previsti nel D.Lgs. 231/01;
- costituisce parte integrante del Modello 231/01 di GOIRC;
- agevola il monitoraggio dell'applicazione del Modello 231 da parte dell'OdV.

**Scopo della Procedura è prevenire la commissione, da parte dei soggetti indicati nel D.Lgs. 231/01, dei seguenti reati:**

- Art. 635 ter c.p. - “Danneggiamento”;
- Art. 635 bis c.p. - “Danneggiamento di informazioni, dati e programmi informatici”;
- Art. 635 quater c.p. - “Danneggiamento dei sistemi informatici o telematici”;
- Art. 635 quinquies c.p. - “Danneggiamento di sistemi informatici o telematici di pubblica utilità”;
- Art. 25 novies D.Lgs 231/2001 - “Reati in materia di diritti d'autore”;
- Art. 171 Bis - “Violazione dei Diritti d'Autore mediante duplicazione di programmi”;
- Art. 615 ter c.p. - “Accesso abusivo ad un sistema informatico o telematico”;
- Art. 615 quarter c.p. - “Detenzione e diffusione abusiva di codici di accesso a sistemi telematici ed informatici”;
- Art. 615 quinquies c.p. - “Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico”;
- Art. 640 ter c.p. - “Frode informatica in danno dello Stato o di altro ente pubblico”;
- Art. 640 quinquies c.p. - “Frode informatica del soggetto che presta servizi di certificazione di firma elettronica”;
- Art. 617 quarter c.p. - “Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche”;
- Art. 617 quinquies c.p. - “Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche”;
- Art. 491 bis c.p. - “Falsità in un documento informatico pubblico o avente efficacia probatoria”.
- La presente procedura si applica alle attività operative svolte all'interno di GOIRC e, in particolare, quelle che presuppongono l'utilizzo di strumenti informatici sia hardware che software.

La presente Procedura deve ritenersi integrata dal **MOP (Modello Organizzativo Privacy)** e dalla **Procedura Whistleblowing (PWB)** adottati dall'Ente.

## **2. Individuazione delle responsabilità e descrizione dei reati**

I reati derivanti da delitti informatici, dal trattamento illecito dei dati o dalla violazione dei diritti d'autore previsti dal D.Lgs. 231/01 possono configurarsi nell'ambito dello svolgimento delle attività operative poste in essere dai singoli lavoratori e da ogni destinatario del Modello 231.

In particolare:

a) la gestione del sistema informativo di GOIRC, comprensivo di hardware, software e gestione della rete può comportare la commissione di reati rilevanti ex D.Lgs. n. 231/01 (artt. 635 bis c.p., 635 quarter c.p., 171 bis l. 633/41 (L.A.), 615 ter e quarter, 640 ter e 491 – bis c.p. ) ad opera di tutti i soggetti che svolgono funzioni aziendali;

b) l'installazione di apparecchiature ed hardware può comportare la commissione dei reati rilevanti ex D.Lgs. n. 231/01 (art. 635 bis c.p., 635 quarter c.p., 171 bis L.A.) ad opera delle funzioni amministrative e dei componenti dei vari organi di controllo.

**I reati derivanti dalla gestione e controllo delle attività associative che possono portare alla commissione dei cosiddetti reati informatici previsti dall'art. 24 bis e 25-novies del D.Lgs 213/01 possono configurarsi nello svolgimento delle seguenti attività operative.**

Gestione del sistema informativo aziendale, comprensivo di hardware, software e gestione della rete; in merito ai reati ex artt. 635 bis, 635 quater c.p. e 171 bis violazione dei diritti d'autore; 615 ter e quarter, 640 ter e 491 – bis c.p.

### **3. Individuazione e Classificazione delle aree a rischio di commissione del reato.**

La sottostante tabella riporta l'esito della classificazione del rischio di commissione del reato descritta nel Modello 231.

#### **Classificazione dei rischi di commissione del reato.**

<b><u>Classificazione del rischio Reati</u></b>	<u>Molto basso</u>	<u>Basso</u>	<u>Medio</u>	<u>Alto</u>	<u>Molto alto</u>
Art. 635 bis c.p.		x			
Art. 635 quarter c.p.		x			
Art. 171 bis		<u>x</u>			
Art. 640 ter c.p.			<u>x</u>		
Art. 491 bis c.p.		x			
Art. 615 ter e 615 quater c.p.			<u>x</u>		

### **4. Attività a rischio di commissione dei reati previsti nel D.Lgs. 231/01.**

Effettuata l'analisi dei rischi ai fini del D.Lgs. n. 231/01, GOIRC ha individuato quali aree sensibili le seguenti attività a rischio reato, svolgendo le quali potrebbero configurarsi alcuni dei reati informatici o i reati relativi ai diritti d'autore:

a) installazione di apparecchiature per il danneggiamento dei dati contenuti nel sistema informativo aziendale;

b) danneggiamento volontario di sistemi informatici o telematici;

c) frode informatica, falsità in documenti informatici pubblici o aventi efficacia probatoria; accesso abusivo a sistemi informatici; detenzione o diffusione abusive di codici di accesso a sistemi informatici

## **5. Principi generali di comportamento.**

**Gli strumenti elettronici ed informatici devono essere utilizzati:**

- a) in osservanza dei diritti degli altri utenti e di terzi;
- b) in osservanza della normativa, generale e di settore, degli obblighi contrattuali e delle prassi aziendali diffuse;
- c) preservando l'integrità dei sistemi e delle relative risorse fisiche;
- d) con consapevolezza e responsabilità e senza commettere abusi.

Assegnato il posto di lavoro, costituito da personal computer, completo di quanto necessario per svolgere le proprie funzioni, è vietato modificare la configurazione del software installato, funzionale all'espletamento delle specifiche attività lavorative.

E' proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema (AdS) o il soggetto a ciò deputato.

GOIRC, al fine di prevenire ogni possibile utilizzo non consentito degli strumenti elettronici e della rete aziendale, adotta le misure, tecniche ed organizzative, idonee a garantire la sicurezza dei dati in relazione al grado di rischio correlato alle singole operazioni di trattamento, osservando quanto previsto nel Reg. UE 2016/679 (GDPR) e nel D.Lgs. n. 196/03, come modificato dal D.Lgs. n. 101/08.

Segnatamente, l'Associazione osserva quanto prescritto nella Policy del MOP (Modello Organizzativo Privacy) dedicata alla prevenzione e gestione dei Data Breach (violazione dei dati personali) ed all'utilizzo degli strumenti informatici e telematici.

## **6. Protocolli generali di prevenzione.**

Con specifico riferimento a tali attività sensibili, e con valenza generale ai fini di tutela dell'Ente rispetto alla potenziale commissione di tutti i reati considerati nella presente Procedura, GOIRC adotta i seguenti Protocolli di prevenzione.

GOIRC, nell'ambito dell'attività di adeguamento al GDPR, provvede alla gestione del trattamento dei dati personali dell'Ente, adottando misure, tecniche ed organizzative, idonee a garantire la sicurezza, l'integrità e la disponibilità dei dati.

In particolare, tali misure consistono nella scrupolosa protezione delle aree e dei locali, nella puntuale custodia ed archiviazione di atti, documenti e supporti, nell'adozione di misure fisiche e tecnologiche di sicurezza, nell'utilizzo di mezzi idonei a garantire il tempestivo ed integrale ripristino dei dati.

GOIRC osserva la normativa comunitaria e nazionale nonché le Linee Guida dell'EDPB e del Garante Privacy italiano; applica, in particolare, le Linee Guida emanate dal Garante sulla disciplina della navigazione in internet e sulla gestione della posta elettronica nei luoghi di lavoro, con specifico riferimento alla regolamentazione delle modalità di accesso e di utilizzo degli strumenti informatici da parte degli amministratori, dipendenti e collaboratori di GOIRC.

La normativa ed i provvedimenti suindicati e le prescrizioni contenute nel MOP contengono i principi e le regole interne di gestione dell'Ente.

GOIRC provvede a sensibilizzare il personale su altri aspetti rilevanti nella gestione dei sistemi

informatici aziendali: a) rispetto della normativa sulla tutela legale del software; b) rispetto della normativa sulla tutela del know-how aziendale, ove le informazioni di proprietà dell'Associazione siano custodite nel sistema informatico.

L'adozione delle misure di cui all'art. 32 Reg. UE 2016/679 e delle procedure di informativa-consenso di cui agli art. 13 e 14 Reg. UE 2016/679 e la tutela dei diritti degli interessati sanciti negli art. 15 e 22 del medesimo Regolamento costituiscono un efficace strumento per limitare il rischio di insorgenza della responsabilità amministrativa a carico dell'Ente, inerente ai reati presupposto della presente procedura.

La designazione di referenti e consulenti privacy consente lo svolgimento delle funzioni di informazione e consulenza, sorveglianza sull'osservanza del GDPR, consulenza in merito alla valutazione di impatto sulla protezione dei dati, cooperazione con l'Autorità di controllo.

## **7. Protocolli specifici di prevenzione.**

L'individuazione delle aree sensibili, a rischio reato, effettuata in seguito alla svolta analisi dei rischi ha indotto ad adottare i seguenti protocolli specifici di prevenzione:

### **a) Installazione di apparecchiature per il danneggiamento dei dati contenuti nel sistema informatico aziendale.**

Gli strumenti elettronici sono affidati ad ogni dipendente all'interno di GOIRC.

Ogni utilizzo non inerente l'attività lavorativa può determinare il configurarsi dei reati presupposto esplicitamente richiamati nella presente Procedura.

La gestione del PC e degli strumenti elettronici aziendali deve effettuarsi in osservanza del MOP (Modello Organizzativo Privacy) dell'Ente nonché dei provvedimenti e delle istruzioni del Garante privacy italiano ed in conformità al GDPR ed al riformato Codice della Privacy.

Al fine di evitare l'utilizzo di postazioni informatiche e di accessi alla rete è proceduralizzata una gestione delle Password e delle postazioni.

GOIRC osserva i principi *privacy by design* e *privacy by default* sanciti nell'art. 25 Reg. UE 679/16, adottando: a) misure, tecniche ed organizzative, adeguate, volte ad attuare in modo efficace la protezione dei dati, quali la pseudonimizzazione e la minimizzazione; b) misure, tecniche ed organizzative, adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità di trattamento.

### **b) Danneggiamento volontario di sistemi informatici o telematici.**

Le regole ed i protocolli per l'attività suindicata, "Installazione di apparecchiature per il danneggiamento dei dati contenuti nel sistema informatico aziendale", sono utilizzabili anche per la prevenzione di eventuali danneggiamenti del sistema informatico e telematico.

GOIRC adotta procedure volte a garantire la sicurezza e l'integrità dei dati e la tutela degli interessati in caso di *data breach* o di violazione dei dati personali (prevedendo le modalità operative da utilizzare per evitare che il danneggiamento di una postazione o della rete abbia effetti irreversibili e possa essere ripristinata la regolare operatività) e verifica, ove occorra, l'opportunità di effettuare la valutazione di impatto sulla protezione dei dati (VIP o DPIA) ex art.35 GDPR, osservando, sul punto, quanto prescritto nelle Linee Guida del Gruppo art. 29 e nel successivo Provvedimento emesso dal Garante italiano ad integrazione delle stesse.

### **c) Accesso abusivo a sistemi informatici; detenzione o diffusione abusive di codici di accesso a sistemi informatici; frode informatica, falsità in documenti informatici.**

La prevenzione dei reati sopra indicati si attua mediante l'osservanza di: Principi generali di comportamento, Protocolli generali di prevenzione, Protocolli specifici di prevenzione predisposti per gli altri reati sopra illustrati; adempimento delle istruzioni, direttive ed informative del nominato. In particolare, GOIRC: rispetta le misure, tecniche ed organizzative, idonee a garantire la sicurezza, l'integrità e la disponibilità dei dati; adotta costantemente adeguate misure fisiche e tecnologiche di sicurezza; garantisce la sicurezza delle misure di accesso ai dati, correlandole al grado di rischio specifico delle singole operazioni di trattamento; assicura il tempestivo ed integrale ripristino dei dati; osserva la normativa comunitaria e nazionale e le Linee Guida del Garante Privacy italiano per la protezione dei dati personali sulla disciplina della navigazione in internet e sulla gestione della posta elettronica nei luoghi di lavoro, con specifico riferimento alla regolamentazione delle modalità di accesso e di utilizzo degli strumenti informatici da parte degli amministratori, dipendenti e collaboratori; rispetta i principi di efficace protezione dei dati sin dalla progettazione e per impostazione predefinita (art. 25 reg. UE 679/16).

### **8. Controllo Operativo.**

Il controllo operativo degli aspetti relativi ai reati cosiddetti "informatici" è effettuato secondo il sistema previsto dal MOP (Modello Organizzativo Privacy) nel quale sono esplicitate le funzioni di controllo e di sorveglianza rispetto alle attività vietate e le modalità di intervento sul sistema informativo di GOIRC nonchè in osservanza del Reg. UE 2016/679 (GDPR) e del D.Lgs. 196/03 come modificato dal D.Lgs. 101/18.

## **9. Flusso informativo all'Organismo di Vigilanza.**

All'OdV devono pervenire,

provenienti dalla Funzione amministrativa e/o dal team di sicurezza e/o dagli IT e/o AdS compatibilmente con le norme del Reg. UE 679/16 le seguenti informazioni:

- notizie relative agli attacchi da parte di virus o altre minacce al sistema informatico (al verificarsi dell'evento o, in mancanza di eventi, con cadenza annuale);

- relazione sull'andamento dei controlli e sul funzionamento del sistema informativo (con cadenza annuale o al verificarsi dell'evento);

provenienti dal team di sicurezza e/o dai designati AdS (Amministratori di Sistema):

- le anomalie relative, tra l'altro, a:

back up dei dati; sistema di sicurezza logica e fisica del sistema informativo;

incidenti verificatisi durante la procedura di *incident* e ripristino;

gestione degli strumenti informatici;

danneggiamento o rimozione di software in service per la gestione delle attività;

danneggiamento o rimozione di hardware in service per la gestione delle attività;

uso della rete locale e remota (al verificarsi dell'evento o, in mancanza di eventi, con cadenza annuale).

**GOIRC**  
**Modello Organizzativo D.Lgs. 231/01**

**PROCEDURA: PRO RIC**  
**REATI RICETTAZIONE E RICICLAGGIO**

## **INDICE**

- 1. Finalità ed ambito di applicazione.**
- 2. Individuazione delle Responsabilità.**
- 3. Individuazione e classificazione delle aree a rischio di commissione del reato.**
- 4. Principi generali di comportamento.**
- 5. Attività a rischio di commissione dei reati ex D.Lgs. 231/01.**
- 6. Protocolli di prevenzione.**
- 7. Controllo Operativo.**
- 8. Flusso informativo all'Organismo di Vigilanza.**

## **PROCEDURA: PRO RIC REATI RICETTAZIONE E RICICLAGGIO**

### **1. Finalità ed ambito di applicazione.**

#### **La presente procedura:**

- disciplina gli aspetti relativi alla gestione ed al controllo delle attività che possono determinare la commissione dei reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita previsti nell'art. 25 octies D.Lgs. 231/01;
- costituisce parte integrante del Modello 231 di GOIRC;
- agevola il monitoraggio dell'applicazione del Modello 231 da parte dell'OdV.

#### **Scopo della presente procedura è prevenire la commissione, da parte dei soggetti indicati nel D.Lgs 231/01, dei seguenti reati:**

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

### **2. Individuazione delle Responsabilità.**

I reati esaminati e presidiati nella presente Procedura (ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio previsti dall'art. 25 octies D.lgs 231/01) possono configurarsi nello svolgimento delle attività operative poste in essere dai singoli lavoratori e da ogni destinatario del Modello 231.

Sono riportate, qui di seguito, in maniera specifica, per ogni singola attività sensibile, i ruoli/funzioni responsabili.

#### **A) Attività in economia di servizi e forniture:**

- di pertinenza di Organo Amministrativo, Consulente, Presidente, Tesoriere;
- reati di: ricettazione (art. 648 c.p.); impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.); autoriciclaggio (art. 648 ter 1, c.p.).

#### **B) Gestione dei pagamenti dei fornitori:**

- reati di: riciclaggio (art. 648 bis c.p.); impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.); autoriciclaggio (art. 648 ter 1, c.p.)

#### **C) Gestione delle sponsorizzazioni, spese di beneficenza:**

- reati di: riciclaggio (art. 648 bis c.p.).

### **3. Individuazione e Classificazione delle aree a rischio di commissione del reato.**

La sottostante tabella riporta l'esito della classificazione del rischio di commissione del reato descritta nel Modello 231 per i soggetti responsabili indicati nel paragrafo precedente.

<b><u>Classificazione del rischio</u></b>	<u>Molto basso</u>	<u>Basso</u>	<u>Medio</u>	<u>Alto</u>	<u>Molto alto</u>
---	--------------------	--------------	--------------	-------------	-------------------

<b>Reati</b>					
Art. 648 bis c.p. Riciclaggio			X		
Art. 648 c.p. Ricettazione		X			
Art. 648 ter Impiego di denaro, bei o utilità di provenienza illecita			X		
Art. 648 ter c. 1 c.p. Autoriciclaggio			X		

#### **4. Principi generali di comportamento.**

Al fine di prevenire i reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, i lavoratori, a qualsiasi livello aziendale, e tutti i destinatari del Modello 231 dovranno attenersi ai seguenti principi di comportamento:

- a) le operazioni che comportano impiego di risorse economiche o finanziarie devono avere una causale espressa ed essere documentate e registrate in conformità ai principi di correttezza professionale e contabile;
- b) gli operatori finanziari utilizzati dall'Ente devono essere abilitati, secondo legge, alla realizzazione di qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie.

#### **E' espressamente vietato:**

- a) disporre/accettare pagamenti relativi a beni non consegnati o servizi non erogati o da soggetti diversi dalla controparte contrattuale;
- b) avere conti correnti cifrati intestati all'Ente (tutti i conti correnti aperti presso istituti di credito o assimilati sono contrattualmente regolati dalle vigenti norme in materia);
- c) disporre/accettare pagamenti da soggetti intestatari di conti correnti registrati in paradisi fiscali e/o Paesi appartenenti alle cosiddette "Black list" o con particolari regimi fiscali, salvo che si tratti di Paesi ove questi hanno residenza o in quello ove è stata effettuata la prestazione;
- d) utilizzare istituti di credito privi di insediamenti fisici e non sottoposti a sistema di controllo da parte della Banca d'Italia e Banca Centrale Europea (es. Istituti virtuali); effettuare pagamenti in contanti o altro strumento finanziario al portatore, osservando i relativi divieti della normativa nazionale (fatti salvi i pagamenti effettuati, quali spese minute, attraverso la piccola cassa, nei limiti consentiti dalla vigente normativa e nel rispetto delle regole fissate nei Protocolli e Procedure), per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie;

- e) utilizzare conti correnti o libretti di risparmio in forma anonima o con intestazione fittizia;
- f) accettare pagamenti in contanti per i servizi e le prestazioni rese dall'Ente in favore dell'utenza;
- g) effettuare operazioni in violazione dell'obbligatoria tracciabilità dei flussi finanziari in conformità alla legge vigente.

**E' obbligatorio:**

- a) garantire, nell'ambito dei rapporti con i consulenti, fornitori, partner commerciali e, in genere, con le controparti contrattuali, il rispetto dei principi di correttezza, trasparenza e buona fede;
- b) redigere per iscritto, con l'indicazione dei contenuti e delle condizioni economiche pattuite, gli incarichi conferiti ad eventuali aziende di servizi e/o persone fisiche che curino gli interessi economico/finanziari di GOIRC;
- c) garantire il controllo dell'avvenuta regolarità dei pagamenti nei confronti di tutte le controparti e, in particolare, verificare che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme;
- d) assicurare il controllo, sia formale che sostanziale (verifica della sede legale della società controparte, degli istituti di credito utilizzati, verifica relativamente all'utilizzo di società fiduciarie), con riferimento ai flussi finanziari ed ai pagamenti verso terzi;
- e) rispettare i requisiti minimi fissati ai fini della selezione dei soggetti offerenti i beni e/o servizi che GOIRC intende acquisire e fissare i criteri di valutazione delle offerte.

**5. Attività a rischio di commissione dei reati previsti nel D.Lgs. 231/01.**

L'individuazione delle aree sensibili consente di identificare, a titolo non esaustivo, le seguenti attività a rischio reato svolgendo le quali possono configurarsi i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita:

- a) acquisizione di servizi e forniture;
- b) gestione dei pagamenti dei fornitori;
- c) gestione delle sponsorizzazioni.

**6. Protocolli di prevenzione.**

I rischi connessi a ciascuna delle attività sensibili individuate e sopra descritte sono presidiati, nel presente Modello 231 e, in particolare, nel Sistema generale di prevenzione, con specifico riferimento al paragrafo relativo alla gestione del sistema finanziario, nel Codice Etico, nelle Procedure relative ai reati in materia di riciclaggio e rapporti con la P.A. e AVC e nei seguenti Protocolli di prevenzione:

**a) Acquisizione di servizi e forniture**

Tali modalità operative sono regolate, innanzitutto, nella Procedura PA – AVC.

Ad integrazione delle richiamate norme e procedure è necessario:

- espletare, nella selezione di fornitori e appaltatori, ove la commessa sia di importo superiore ad una somma prestabilita, gli adempimenti richiesti dalla normativa antimafia;
- garantire il completamento dei controlli e degli adempimenti volti all'espletamento dell'acquisto;
- verificare, nella scelta del fornitore e dell'appaltatore, l'adesione al Codice Etico e al presente Modello 231, richiedendone espressa accettazione (anche ai fornitori attuali sarà richiesta adesione al Codice Etico ed al Modello 231).

#### **b) Gestione dei pagamenti ai fornitori**

La gestione e il pagamento delle fatture avviene secondo quanto previsto nelle Procedure e prassi aziendali relative alla contabilizzazione, redazione bilancio, pagamenti, fatturazione attiva e passiva.

Il mandato di pagamento dovrà essere approvato dal Consiglio Direttivo, previa esibizione di documentazione comprovante l'importo, il beneficiario e gli elementi identificativi del contratto sottostante.

Eventuali variazioni di tale importo dovranno essere approvati dall'Organo Amministrativo.

Dell'attività di contabilizzazione viene redatta e trasmessa all'Organo Amministrativo una nota che evidenzia l'avvenuto pagamento con relativa istruttoria di liquidazione.

#### **c) Gestione delle sponsorizzazioni, spese di beneficenza**

GOIRC, in merito alla stipula dei contratti di sponsorizzazione, è tenuta ad osservare, a conferma ed integrazione di quanto disposto nel Codice Etico, nel Sistema generale di prevenzione e nella Procedura PA – AVC, le seguenti regole:

i contratti di sponsorizzazione devono essere stipulati solo nel caso in cui vi sia un interesse, concreto ed attuale, di GOIRC; l'oggetto del contratto deve essere determinato e devono essere individuate, in maniera specifica, le attività relative alla sponsorizzazione richiesta; l'organo amministrativo deve verificare sempre la congruità tra contributo versato per la sponsorizzazione e la controprestazione promozionale ricevuta in base ai prezzi di mercato; non è consentito stipulare contratti di sponsorizzazione con associazioni non riconosciute o non aventi rilievo nazionale o con scopi non conformi all'oggetto sociale di GOIRC.

GOIRC, quanto alle spese di beneficenza, è tenuta ad osservare, ad integrazione ed in conformità a quanto disposto nel Codice Etico, nel Sistema generale di prevenzione e nella Procedura PA – AVC, le seguenti regole di comportamento: le erogazioni di beneficenza possono essere effettuate solo agli Enti regolarmente costituiti ai sensi di legge e che non contrastino con i principi etici conformi a quelli dell'Ente; tutte le iniziative devono essere approvate dall'Organo Amministrativo.

### **7. Controllo Operativo.**

Il controllo operativo degli aspetti relativi ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita e di antiriciclaggio avviene mediante

l'applicazione della presente Procedura, del Sistema generale di prevenzione del presente Modello 231 e delle Procedure Operative relative ai reati societari ed ai rapporti con la P.A..

#### **8. Flusso informativo relativo all'Organismo di Vigilanza.**

All'OdV devono pervenire, dall'Organo Amministrativo - al verificarsi dell'evento o, in mancanza di eventi, con cadenza annuale - copia delle fatture da parte dei soggetti beneficiari delle sponsorizzazioni con allegati i relativi documenti comprovanti l'avvenuto pagamento.

#### **L'OdV deve:**

vigilare sull'osservanza della normativa antiriciclaggio attraverso la predisposizione di controlli preventivi specifici;

comunicare le possibili infrazioni relative alle operazioni di registrazione, segnalazione e ai limiti all'uso di strumenti di pagamento e deposito - di cui venga a conoscenza nell'esercizio delle proprie funzioni o nelle ipotesi in cui ne abbia comunque notizia - all'interno dell'Azienda ed all'esterno.

Il flusso informativo sopraesposto costituisce integrazione dei flussi informativi individuati nello Statuto dell'OdV e nelle altre sezioni del Modello 231/01 afferenti ai flussi informativi dell'OdV.

**GOIRC**  
**Modello Organizzativo D.Lgs. 231/01**

**PROCEDURA: PRO SOC**  
**REATI SOCIETARI**

## **INDICE**

- 1. Finalità ed ambito di applicazione.**
- 2. Individuazione delle Responsabilità.**
- 3. Individuazione e Classificazione delle aree a rischio di commissione del reato.**
- 4. Principi generali di comportamento.**
- 5. Attività a rischio di commissione dei reati ex D.Lgs. 231/01.**
- 6. Protocolli di prevenzione.**
- 7. Controllo Operativo.**
- 8. Flusso informativo all'Organismo di Vigilanza.**

## **PROCEDURA: PRO SOC**

### **REATI SOCIETARI**

#### **1. Finalità ed ambito di applicazione.**

La presente Procedura:

- disciplina gli aspetti relativi alla gestione ed al controllo delle attività che possono determinare la commissione dei reati societari previsti nell'art 25 ter D.Lgs. 231/01;
- costituisce parte integrante del Modello 231 di GOIRC;
- agevola il monitoraggio dell'applicazione del Modello 231 da parte dell'OdV.

**Scopo della presente procedura è prevenire la commissione, da parte dei soggetti indicati nel D.Lgs 231/01, dei reati richiamati dall'art. 25 ter D.Lgs. 231/01, di seguito descritti:**

#### **Art. 25 ter D.Lgs 231/01**

- Art. 2621 c.c - False comunicazioni sociali;
- Art. 2621 bis e 262 c.c. – Falsità nelle relazioni e nelle comunicazioni agli organi di controllo;
- Art. 2624 c.c. – Illecita influenza sull'assemblea;
- Art. 2625 c.c. - Impedito controllo;
- Art. 2626 c.c. - Indebita restituzione dei conferimenti;
- Art. 2629 c.c. - Operazioni in pregiudizio dei creditori;
- Art. 2632 c.c. – Formazione fittizia del capitale;
- Art .2635 c.c. -Delitto di corruzione tra privati;
- Art. 2636 c.c. – Illecita influenza sull'assemblea;
- Art. 2637 c.c. – omessa comunicazione di conflitti di interesse;
- Art. 2638 c.c. - Ostacolo alle funzioni delle Autorità pubbliche di vigilanza.

#### **2. Individuazione delle Responsabilità.**

I reati esaminati e presidiati nella presente Procedura possono configurarsi nello svolgimento delle attività operative poste in essere dai dipendenti e apicali di GOIRC e da ogni destinatario del Modello 231.

Sono riportate, di seguito, in maniera specifica, le singole attività sensibili oggetto della Procedura.

- a) tenuta della contabilità, redazione del bilancio di esercizio;
- b) gestione dei rapporti con i soci e con gli organi di controllo;
- c) gestione dei rapporti con la P.A. in occasione di adempimenti in materia fiscale e tributaria ed in casi di ispezioni, verifiche ed accertamenti relativi agli adempimenti stessi.

#### **3. Individuazione e Classificazione delle aree a rischio di commissione del reato.**

La sottostante tabella riporta l'esito della classificazione del rischio di commissione del reato descritta nel Modello 231 per i soggetti responsabili indicati nel paragrafo precedente

<b><u>Classificazione del rischio</u></b>	<u>Molto basso</u>	<u>Basso</u>	<u>Medio</u>	<u>Alto</u>	<u>Molto alto</u>

<u>Reati</u>					
Art. 2621 c.c.			<u>x</u>		
Art. 2625 c.c.			x		
Art. 2626 c.c.	x				
Art. 2629 c.c.		x			
Art. 2632 c.c.		x			
Art. 2635 c.c.			x		
Art. 2636 c.c.	<u>x</u>				
Art. 2638 c.c.			<u>x</u>		

#### **4. Principi generali di comportamento.**

**Al fine di prevenire i reati considerati nella presente Procedura occorre rispettare alcuni principi generali di comportamento.**

**In particolare è vietato:**

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che possano integrare le fattispecie di reato richiamate nell'art. 25 ter.D.Lgs. n. 231/01;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, ancorchè non costituiscano di per sé reato, possano potenzialmente diventarlo;
- rappresentare o trasmettere, per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o non conformi alla realtà, sulla situazione economica, patrimoniale e finanziaria di GOIRC;
- omettere dati ed informazioni richiesti dalla legge sulla situazione economica, patrimoniale e finanziaria dell'Associazione;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- effettuare riduzioni del patrimonio dell'associazione, fusioni o scissioni, in violazione delle norme a tutela dei creditori, provocando ad essi un danno;
- distrarre i beni dell'associazione, in sede di liquidazione della società, dalla loro destinazione ai creditori, ripartendoli fra i soci prima del pagamento dei creditori o dell'accantonamento delle somme necessarie a soddisfarli;
- adottare comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che ostacolino lo svolgimento all'attività di controllo o di revisione della gestione sociale da parte dei soggetti a ciò deputati.

**Inoltre è obbligatorio:**

- a) adottare comportamenti corretti, trasparenti e collaborativi, in osservanza delle norme di legge e delle procedure dell'Associazione, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci e ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria dell'Ente;
- b) adottare comportamenti corretti, nel rispetto delle norme di legge e delle procedure aziendali, per garantire la tutela del patrimonio dell'Associazione, ponendo la massima attenzione ed accuratezza ed acquisendo, elaborando ed illustrando, con diligenza e puntualità, i dati e le informazioni necessari per consentire ai terzi un fondato giudizio sulla situazione patrimoniale, economica e finanziaria dell'Associazione;

- c) osservare rigorosamente la normativa vigente predisposta a tutela dell'integrità ed effettività del patrimonio dell'Ente, agendo nel rispetto delle procedure aziendali che su tale normativa si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- d) assicurare il regolare funzionamento dell'Associazione e degli organi sociali, garantendo ed agevolando ogni forma di controllo sulla gestione sociale previsto dalla legge nonché la libera e corretta formazione della volontà assembleare.

#### **5. Attività a rischio di commissione dei reati previsti nel D.Lgs. 231/01.**

L'analisi dei rischi effettuata in relazione alle aree sensibili individuate nell'ambito delle attività di GOIRC - ha permesso di identificare le seguenti attività a rischio reato (il relativo elenco è soggetto a costante aggiornamento), svolgendo le quali potrebbero configurarsi i reati societari previsti nel D.Lgs.231/01:

- a. tenuta della contabilità e redazione del bilancio di esercizio;
- b. gestione dei rapporti con gli associati e gli organo di controllo;
- c. gestione dei rapporti con Enti Pubblici che svolgono attività regolatorie e di vigilanza.

#### **6. Protocolli di prevenzione.**

I rischi connessi a ciascuna delle attività sensibili individuate e sopra descritte sono presidiati – oltre che mediante l'osservanza del presente Modello 231 e, in particolare, del Sistema generale di prevenzione esposto nella parte generale, del Codice Etico, delle Procedure operative relative ai reati inerenti la P.A. e AVC ed ai reati in materia di riciclaggio - attraverso i seguenti protocolli di prevenzione:

##### **6.1 Tenuta della contabilità e redazione del bilancio di esercizio.**

Le operazioni di formazione del bilancio e degli altri documenti sono effettuate in conformità ai più recenti ed aggiornati Principi Contabili per la chiusura del Bilancio ed alle relative Procedure aziendali.

La tenuta della contabilità e la redazione del bilancio di esercizio vengono effettuate nel rispetto dei principi generali di comportamento del presente Modello 231, dei principi e delle regole del Codice Etico e dei documenti elaborati e diffusi dall'Amministrazione Finanziaria.

##### **6.2 Gestione dei rapporti con soci ed organi di controllo e revisione in genere**

Per le attività relative alla gestione dei rapporti con i soci e gli organi di controllo si osservano le seguenti prescrizioni:

- una volta acquisite, le informazioni richieste vengono trasmesse agli organi di controllo previa verifica della loro completezza, correttezza e pertinenza;
- le richieste e le trasmissioni di dati e informazioni, nonché ogni rilievo, comunicazione o valutazione espressa dagli organi associativi competenti sono istruite e documentate per il relativo formale riscontro;
- i documenti relativi alle operazioni sulle quali gli organi competenti esprimano un parere, sono comunicati e messi a disposizione, con ragionevole anticipo, rispetto alla data della riunione;
- il libero accesso alla contabilità dell'Ente ed alla documentazione richiesta per un corretto svolgimento dell'incarico deve essere garantito ai soci, agli organi di revisione e controllo;

### **6.3 Gestione dei rapporti con la P.A. in occasione di adempimenti in materia fiscale e tributaria e in casi di ispezioni, verifiche ed accertamenti relativi agli adempimenti stessi.**

Le seguenti attività devono ritenersi a rischio reato con specifico riferimento agli adempimenti in materia fiscale:

1. attività di supporto agli organi di controllo fiscali durante la verifica presso l'Ente;
2. produzione di documenti, atti, fatture, bilanci, delibere, in riscontro alle richieste dell'organo di controllo.

La gestione degli adempimenti fiscali e tributari è curata da soggetti specificamente delegati e/o deputati a tali attività.

I suindicati soggetti: gestiscono, in base alla normativa di settore, le attività relative alla predisposizione delle dichiarazioni/comunicazioni necessarie; verificano la completezza e la correttezza di quanto predisposto; sottopongono i documenti alla firma dell'Organo Amministrativo o provvedono a sottoscriverli direttamente ove a ciò autorizzati in base al sistema di procure/deleghe in vigore presso l'Associazione.

Intervenuta la trasmissione all'Ente Pubblico competente, il Responsabile archivia copia della dichiarazione/comunicazione trasmessa, unitamente alla documentazione di supporto o mediante richiamo alla stessa, e ne riferisce all'Organo Amministrativo.

### **7. Controllo Operativo.**

Il controllo operativo degli aspetti relativi ai reati societari è attuato, oltre che mediante i protocolli sopra esposti, attraverso le seguenti attività svolte dagli Organi competenti:

- ispezione e controllo e vigilanza sull'osservanza della legge, dello Statuto e dei principi di corretta amministrazione;
- controllo contabile ed economico di GOIRC e, in particolare, verifica della correttezza delle procedure amministrative, delle registrazioni contabili e della relativa applicazione nonché della correttezza del bilancio e della rispondenza dello stesso alle norme di legge.

### **8. Flusso informativo all'Organismo di Vigilanza**

L'Organo Amministrativo deve inviare all'OdV la copia dei verbali di controllo rilasciati dalle Autorità competenti ovvero le note del Direttore/Dirigente Responsabile in caso di mancata redazione del verbale.

Tale flusso informativo avviene al verificarsi dell'evento.

All'OdV devono altresì pervenire, con cadenza annuale, i seguenti documenti:

- copia del bilancio di esercizio approvato, inviati dall'Organo Amministrativo;
- relazione annuale del Revisore legale dei conti, inviata dal Revisore stesso.

Il flusso informativo sopra esposto costituisce integrazione dei flussi informativi individuati nello Statuto dell'OdV e nelle altre sezioni del Modello 231 afferenti ai flussi informativi dell'OdV.

**PROCEDURA: PRO TRIB**

**REATI TRIBUTARI**

**INDICE**

- 1. Finalità ed ambito di applicazione.**
- 2. Individuazione delle Responsabilità.**
- 3. Individuazione e classificazione delle aree a rischio di commissione del reato.**
- 4. Principi generali di comportamento.**
- 5. Attività a rischio di commissione dei reati ex D.Lgs. 231/01.**
- 6. Protocolli di prevenzione.**
- 7. Controllo Operativo.**
- 8. Flusso informativo all'Organismo di Vigilanza.**

## **PROCEDURA: PRO TRIB REATI TRIBUTARI**

### **1. Finalità ed ambito di applicazione.**

#### **La presente Procedura:**

- disciplina gli aspetti relativi alla gestione ed al controllo delle attività che possono determinare la commissione dei reati tributari indicati nell'art. 25-quinquiesdecies D.Lgs. 231/01;
- costituisce parte integrante del Modello 231 di GOIRC;
- agevola il monitoraggio dell'applicazione del Modello 231 da parte dell'OdV.

#### **Scopo della presente procedura è prevenire la commissione dei seguenti reati:**

- **Art. 2, comma 1, D.Lgs. 74/2000:** dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti che determinano un passivo fittizio uguale o superiore a 100 mila euro;
- **Art. 2, comma 2 bis, D.Lgs. 74/2000:** dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti che determinano un passivo fittizio inferiore a 100 mila euro;
- **Art. 3, D.Lgs. 74/2000:** dichiarazione fraudolenta mediante altri artifici;
- **Art. 8, comma 1, D.Lgs. 74/2000:** emissione di fatture o altri documenti per operazioni inesistenti per importi uguali o superiori a 100 mila euro;
- **Art. 8, comma 2 bis, D.Lgs. 74/2000:** emissione di fatture o altri documenti per operazioni inesistenti per importi inferiori a 100 mila euro;
- **Art. 10D.Lgs. 74/2000:** occultamento o distruzione di documenti contabili;
- **Art. 11D.Lgs. 74/2000:** sottrazione fraudolenta al pagamento di imposte.

### **2. Individuazione delle Responsabilità.**

I reati esaminati e presidiati nella presente Procedura possono configurarsi nello svolgimento delle attività operative poste in essere dai rappresentanti dell'Ente, dai soggetti apicali e dai singoli lavoratori che pongano in essere condotte materiali che determinano reati tributari rilevanti ex D.Lgs. 231/01.

**Sono di seguito evidenziate le singole attività sensibili e le relative fattispecie di reato:**

- A) predisposizione, redazione ed emissione di fatture ed altri documenti contabili e delle dichiarazioni fiscali;
- B) controllo, custodia, gestione e conservazione di documenti contabili;
- C) gestione ed adempimento del pagamento di imposte e tributi.

### **3. Individuazione e Classificazione delle aree a rischio di commissione del reato.**

La sottostante tabella riporta l'esito della classificazione del rischio di commissione del

reato descritta nel Modello 231.

<b><u>Classificazione del rischio Reati</u></b>	<u>Molto basso</u>	<u>Basso</u>	<u>Medio</u>	<u>Alto</u>	<u>Molto alto</u>
<b>Art. 2, comma 1, D.Lgs. 74/20</b>		X			
<b>Art. 2, comma 2 bis, D.Lgs. 74/00</b>			<u>X</u>		
<b>Art. 3 D.Lgs. 74/00</b>			X		
<b>Art. 8, comma 1, D.Lgs. 74/00</b>		<u>X</u>			
<b>Art. 8, comma 2 bis, D.Lgs. 74/2000</b>			X		
<b>Art. 10 D.Lgs. 74/2000</b>		<u>X</u>			
<b>Art. 11 D.Lgs. 74/2000</b>	<u>X</u>				

#### **4. Principi generali di comportamento.**

Al fine di prevenire i reati tributari, i lavoratori, a qualsiasi livello aziendale, e tutti i destinatari del Modello 231, che svolgono attività pertinenti ai reati in esame, devono osservare quanto stabilito nel Codice Etico e nelle Procedure PRO-PA-AVC, PRO-RIC, PRO-SOC e nel Sistema generale di prevenzione nonché nei seguenti principi generali di comportamento:

- GOIRC promuove una cultura aziendale improntata a principi di onestà, correttezza e rispetto della normativa tributaria, assicurandone la completezza e l'affidabilità nonché la conoscibilità a tutti i livelli aziendali;
- GOIRC adotta comportamenti puntuali e rigorosi funzionali al corretto adempimento degli obblighi erariali e tributari, predisponendo, a tal fine, strumenti di prevenzione, verifica e controllo;
- GOIRC e, in particolare, i suoi consulenti e organi apicali, verificano, con attenzione, l'inserimento delle fatture nella contabilità, la veridicità delle fatture stesse, le veridicità e congruità dei relativi costi e la riferibilità degli stessi ad attività e settori operativi dell'Associazione;
- GOIRC attribuisce i ruoli e le responsabilità aziendali nel settore tributario, in modo puntuale e trasparente, a figure con adeguate competenze ed esperienze;
- l'Ente promuove l'adozione ed il rispetto, da parte di tutti i livelli aziendali, di procedure di rilevazione, misurazione, gestione e controllo dei rischi fiscali nonché di verifica e correzione a carenze riscontrate;
- GOIRC osserva, nel settore tributario, compatibilmente alle effettive possibilità di

organico, i principi della separazione delle funzioni, orizzontale, tra operatori che partecipano al medesimo processo, e verticale, tra funzioni operative e funzioni di controllo;

- GOIRC vieta espressamente condotte e scelte in violazione delle norme tributarie, in particolare di quelle di rilievo penale.

#### **5. Attività a rischio di commissione dei reati previsti nel D.Lgs. 231/01.**

L'individuazione delle aree sensibili, effettuata in base all'analisi dei rischi contenuta nel presente Modello 231, consente di identificare, a titolo non esaustivo, le attività di cui alle lettere A), B) e C) del precedente par. 2, come attività a rischio reato svolgendo le quali possono configurarsi reati tributari rilevanti ai sensi del D.Lgs. 231/01.

#### **6. Protocolli di prevenzione.**

**6.1** I rischi connessi a ciascuna delle suindicate attività sensibili sono presidiati, nel presente Modello 231 e, in particolare, nel Sistema generale di prevenzione, con specifico riferimento al paragrafo relativo alla gestione del sistema amministrativo e finanziario, nel Codice Etico, nelle Procedure PRO-PA-AVC, PRO-RIC e, soprattutto, nella PRO-SOC nonché nei seguenti Protocolli di prevenzione:

**6.2** La Funzione/Consulente preposta al controllo fatturazione attive e passive predispone, con cadenza annuale, **una relazione, agli organi di gestione e controllo ed all'OdV**, avente ad oggetto gli adempimenti tributari, le verifiche effettuate in merito alle attività di cui alle lettere A), B) e C) del precedente par. 2 ed i risultati emersi nonché le misure adottate per rimediare a eventuali carenze rilevate e le attività pianificate.

**6.3** La Funzione preposta al controllo fatturazione: cura e verifica interlocuzioni costanti e preventive con l'Agenzia delle entrate, fondate su elementi di fatto veridici nonché la sufficienza e l'adeguatezza della documentazione prodotta e la risposta alle richieste dell'Agenzia nel più breve tempo possibile; comunica, in modo tempestivo ed esauriente, all'organo amministrativo ed agli organi di controllo, l'eventuale sopravvenienza di rischi di natura fiscale; privilegia ed incoraggia, unitamente agli organi di controllo, l'utilizzo degli strumenti preventivi, collaborativi e deflattivi forniti dalla vigente normativa; adotta ed incoraggia comportamenti collaborativi e trasparenti, mediante comunicazioni tempestive ed esaurienti all'Agenzia delle entrate in ordine ad eventuali rischi di natura fiscale e ad eventuali operazioni che possono rientrare nella pianificazione fiscale aggressiva.

**6.4** L'Ente e, in particolare, la Funzione preposta al controllo fatturazione, qualora gli importi delle attività negoziali siano superiori a 100 mila euro, garantisce e verifica l'osservanza, nelle fasi di predisposizione, emissione ed acquisizione delle fatture nonché di predisposizione delle dichiarazioni fiscali, gli adempimenti richiesti dalla normativa tributaria (in particolare, le causali del pagamento ed i documenti contrattuali di riferimento), curandone il flusso informativo verso l'OdV.

**6.5** GOIRC controlla e verifica la qualità dei soggetti con i quali intrattiene rapporti amministrativi, negoziali ed economici, di importo superiore a 100 mila euro, per evitare l'attivazione di relazioni volte, direttamente o indirettamente, alla commissione dei reati tributari di cui al D.Lgs. 231/01.

**6.6** GOIRC, con riferimento ad attività aventi ad oggetto importi superiori a 100 mila euro, avvia il processo di qualifica prima dell'inizio della relazione commerciale al fine di individuare l'identità delle controparti nonché verificare possibili rapporti con soggetti ed attività connessi alla commissione dei reati tributari.

**6.7** GOIRC provvede ad acquisire informazioni di ampiezza e profondità proporzionate all'importo del corrispettivo dovuto e, in ogni caso, provvede ad acquisire dette informazioni ove tale importo sia superiore a 100 mila euro (in caso di importi molto superiori alla citata soglia saranno acquisite informazioni più ampie rispetto a corrispettivi inferiori dovuti ad altre aziende).

**6.8** In particolare, saranno acquisiti ed esaminati i seguenti documenti: visura camerale, ultimi bilanci di esercizio, informazioni sugli organi di stampa e sul web, brochure commerciali, evidenza delle autorizzazioni necessarie per lo svolgimento delle attività, verifica (nei casi previsti) dell'iscrizione nelle white list antimafia.

**6.9** GOIRC verifica, mediante gli apicali a ciò preposti, nella scelta del fornitore e dell'appaltatore, l'adesione al Codice Etico e al presente Modello 231, richiedendo l'espressa accettazione di tali documenti.

## **7. Controllo Operativo**

Il controllo operativo degli aspetti relativi ai reati tributari avviene mediante l'applicazione della presente Procedura, del Sistema generale di prevenzione e delle Procedure PRO-PA-AVC, PRO-RIC, PRO-SOC.

## **8. Flusso informativo relativo all'Organismo di Vigilanza.**

All'OdV devono pervenire, dall'Organo Amministrativo e/o dagli Organi e soggetti sopra indicati

- copia dei verbali di controllo rilasciati dalle Autorità competenti ovvero le note del Direttore/Dirigente o Responsabile in caso di mancata redazione del verbale (al verificarsi di singoli eventi);
- copia del bilancio di esercizio o stralcio dello stesso approvato (con cadenza annuale)
- relazioni annuali inerenti alla gestione dell'Associazione.

## **PROCEDURA: PRO - AMB** **REATI AMBIENTALI**

### **1. Finalità ed ambito di applicazione.**

#### **La presente procedura:**

- disciplina gli aspetti relative alla gestione ed al controllo delle attività che possono determinare la commissione dei reati ambientali previsti dall'art 25 undecies D.lgs 231/01;
- costituisce parte integrante del Modello 231 di GOIRC;
- agevola il monitoraggio dell'applicazione del Modello 231 da parte dell'OdV.

**Scopo della Procedura è prevenire la commissione, da parte dei soggetti indicati nel D.Lgs. 231/01, dei reati di cui all'art. 25 undecies D.Lgs. 231/01, analiticamente elencati e descritti nei successivi par. 2 e 3.**

### **2. Individuazione delle Responsabilità.**

I reati esaminati e presidiati nella presente Procedura possono configurarsi nello svolgimento delle attività operative poste in essere dai singoli lavoratori e da ogni destinatario del Modello 231.

Sono riportate, qui di seguito, in maniera specifica, per ogni singola attività sensibile, le Funzioni aziendali responsabili e le relative fattispecie di reato.

Risultano di seguito correlate le attività aziendali e le relative fattispecie di reato, elencate a titolo non esaustivo:

### **3. Individuazione e classificazione delle aree a rischio di commissione del reato.**

La sottostante tabella riporta l'esito della classificazione del rischio di commissione del reato descritta nel Modello 231 per i soggetti responsabili indicati nel paragrafo precedente.

<b><u>Classificazione del rischio</u></b> <b><u>Reati</u></b>	<b><u>Molto basso</u></b>	<b><u>Basso</u></b>	<b><u>Medio</u></b>	<b><u>Alto</u></b>	<b><u>Molto alto</u></b>
Art. 452 bis c.p., art. 452 quater c.p., art. 452 quinquies			<u>x</u>		
Art.452 sexesies c.p.	<u>x</u>				
Art.256 C.Amb.			<u>x</u>		
Art.257C. Amb. c.n 1 e 2 D.lgs.152/06			<u>x</u>		
Art.258C. Amb.		<u>x</u>			
Art.259 C.Amb.			<u>x</u>		
Art. 260 bis C. Amb.		<u>x</u>			
Art. 279 C. Amb.			<u>x</u>		

### **4. Principi generali di comportamento.**

Al fine di gestire, in modo corretto, le attività operative che possono determinare reati ambientali, occorre osservare i principi generali di comportamento di seguito illustrati.

**I singoli lavoratori e tutti i destinatari del Modello 231 devono contribuire alla corretta esecuzione e gestione delle attività sensibili individuate in sede di analisi dei rischi e descritte nella presente Procedura, rispettando le seguenti prescrizioni:**

- gestire le attività ambientali in conformità a quanto previsto nella vigente normativa;
- provvedere, in particolare, alla gestione dei rifiuti in conformità a quanto previsto nella normativa in materia ambientale, nelle procedure operative e nelle disposizioni del presente Modello 231;
- adempiere a tutte le disposizioni in materia di prevenzione e tutela ambientale ed apportare, se del caso, modifiche organizzative immediate.
- verificare il rispetto dei limiti fissati dalla normativa e dagli atti autorizzativi in merito alle immissioni d'inquinamento nelle diverse matrici ambientali e, in caso di superamento, accertare le cause ed effettuare gli adeguamenti ritenuti necessari;
- verificare, anche attraverso specifiche analisi, l'esistenza ed il rispetto degli atti autorizzativi in materia ambientale ed il rispetto dei limiti di accettabilità previsti dalla normativa in vigore, ed intervenire, immediatamente, ove fossero necessarie manutenzioni, riparazioni, modifiche o ristrutturazioni degli impianti;
- attuare le misure, organizzative e procedurali, idonee a prevenire e ridurre alla fonte gli agenti di rischio ed a limitare i loro effetti sull'ambiente;
- osservare le norme applicabili alle sostanze pericolose, soprattutto in merito all'impatto ambientale dell'uso delle stesse;
- osservare le norme in materia di tutela (dall'inquinamento delle acque, della qualità dell'aria, dall'inquinamento acustico esterno) e ogni altra disposizione connessa;
- provvedere alla corretta gestione dei rifiuti, siano essi pericolosi o non pericolosi, destinati allo smaltimento o al recupero, ai sensi del D.Lgs. n. 152/06 e s.m.i.;
- presenziare, in contraddittorio tecnico, ad eventuali accertamenti o prelievi effettuati dalle Autorità di controllo, chiedendone, ove necessario, la ripetizione e controllare la correttezza delle operazioni di analisi anche in fase di riesame;
- provvedere al più efficace uso delle risorse ai fini del risparmio delle materie prime e dell'energia;
- in caso di pericolo grave per l'ambiente, con potenziali pregiudizi alla salute ed all'integrità fisica delle persone (a causa di sversamenti accidentali, malfunzionamenti di impianti, attrezzature macchinari, ecc.), sospendere, anche solo parzialmente, l'attività lavorativa, dandone immediata comunicazione all'Organo Amministrativo, all'OdV e, in base alla legge, alle autorità competenti;
- effettuare correttamente le registrazioni previste dalla normativa di settore (a titolo solo esemplificativo e, in quanto applicabile: formulario, registro di carico e scarico, divieto di miscelazione, obbligo di conferimento dei rifiuti a soggetti appositamente autorizzati).

#### **5. Attività a rischio di commissione dei reati di cui al D.Lgs. n. 231/01.**

**GOIRC ha individuato le seguenti attività sensibili nell'esercizio delle quali potrebbero commettersi alcuni dei reati ambientali previsti nel D.Lgs. n. 231/01:**

- Attività di trasporto di rifiuti pericolosi o non pericolosi ove la normativa ne prevede il trasporto a fini di legge e di successivo smaltimento;
- Attività logistica per avvio a smaltimento o a recupero dei rifiuti.

## **6. Protocolli di prevenzione.**

Per prevenire la commissione di reati ambientali, i singoli lavoratori e tutti i destinatari del Modello 231 devono osservare, in adempimento della normativa generale e di settore, del D.Lgs. 231/01 e delle Procedure dell'Ente, i seguenti protocolli di prevenzione:

### **Attività di trasporto dei rifiuti.**

L'attività di trasporto dei rifiuti deve essere svolta nel rispetto della normativa e delle relative norme regolamentari e tecniche di attuazione.

**Nello svolgimento di tale attività GOIRC è tenuta ad osservare le seguenti prescrizioni:**

- verificare che i rifiuti siano accompagnati, nei casi legge, dai documenti richiesti dalla normativa applicabile;
- garantire l'idoneità tecnica dei mezzi di trasporto all'occorrenza utilizzati sottoposti ad ordinari interventi di manutenzione ordinaria e straordinaria;
- prevenire ed impedire la dispersione del percolato dei rifiuti e la fuoriuscita di esalazioni moleste;
- garantire la protezione dei rifiuti trasportati da agenti atmosferici;
- sottoporre i mezzi a bonifiche prima di essere adibiti ad altri tipi di trasporto e provvedere, comunque, a bonifiche periodiche.

**In particolare, è espressamente vietato:**

- l'utilizzo di mezzi e recipienti che hanno contenuto rifiuti pericolosi per il trasporto di rifiuti non pericolosi;
- il trasporto contemporaneo, su uno stesso veicolo, di rifiuti che tra loro risultino incompatibili ovvero suscettibili di reagire dando luogo alla formazione di prodotti esplosivi, infiammabili o comunque pericolosi.

**- Attività logistica per avvio a smaltimento o recupero.**

- impartire al personale dell'Associazione di monitorare costantemente l'integrità delle impermeabilizzazioni, segnalando per iscritto, ogni eventuale rottura e/o lesione dei contenitori utilizzati, ove ciò dovesse verificarsi;
- disporre la pulizia costante dei contenitori (o piazzali) mediante rimozione dei rifiuti caduti a terra durante le fasi di gestione degli stessi, onerando il personale addetto di procedere alla rimozione immediata dei rifiuti caduti;
- verificare periodicamente la costante pulizia delle aree;
- impartire al personale di effettuare, con la massima cura e diligenza, tutte le operazioni di gestione di rifiuti nelle aree assegnate all'Ente e di evitare qualsiasi accesso nelle stesse a persone estranee e non autorizzate.

**E' espressamente vietato:**

- l'accesso ed il conferimento di rifiuti da parte di soggetti non autorizzati;
- scaricare rifiuti con modalità diverse da quelle prescritte nella normativa;
- depositare rifiuti all'esterno dei previsti contenitori e box di raccolta o comunque dell'area non di

pertinenza;

- ogni forma di commercio o di permuta dei rifiuti.

### **7. Controllo operativo.**

Il controllo operativo relativo alle attività sensibili sopra elencate e descritte si effettua mediante la corretta applicazione: delle procedure operative e dei protocolli adottati dall'Ente, del presente Modello 231 e, in particolare, del Sistema generale di prevenzione e di quanto prescritto nella presente Procedura Operativa.

Segnatamente, il controllo operativo viene effettuato nei differenti siti ove si svolge l'attività associativa, al fine di rispettare la politica ambientale di GOIRC e garantire il rispetto della normativa vigente, delle prescrizioni contrattuali e delle autorizzazioni.

### **8. Flusso informativo all'OdV.**

I responsabili e/o i referenti interni inviano all'OdV:

- una Relazione dettagliata su eventuali anomalie amministrative, quantitative e qualitative nell'attività di gestione dei rifiuti e l'elenco delle difformità nella tenuta della documentazione relativa ai rifiuti (con cadenza semestrale);

- documenti, dati ed informazioni relative ad emergenze ambientali, sversamenti accidentali, difformità, contaminazioni del suolo, delle acque, dell'aria o anche acustiche rispetto ai limiti prefissati o eventuali emissioni soggette ad autorizzazioni e non autorizzate (al verificarsi del singolo evento);

- copia dei verbali di controllo rilasciati dalle Autorità competenti e i rapporti di eventuali audit interni effettuati presso l'Ente nell'ambito della gestione ambientale (con cadenza annuale o al verificarsi di singoli eventi).

**PROCEDURA WHISTLEBLOWING**  
ricezione, accertamento e gestione delle segnalazioni  
ai sensi del Decreto legislativo 10 marzo 2023, n. 24

**GOIRC**

**INDICE**

- 1. FINALITÀ**
- 2. CONTENUTO**
- 3. CONTESTO NORMATIVO E REGOLATORIO**
- 4. AMBITO DI APPLICAZIONE**
  - **4.1 Ambito soggettivo di applicazione**
  - **4.2 Ambito oggettivo di applicazione**
- 5. CARATTERISTICHE DELLE SEGNALAZIONI**
  - **5.1 Segnalazioni anonime**
- 6. CANALI DI SEGNALAZIONE**
- 7. CANALE INTERNO DI SEGNALAZIONE INDIVIDUATO DALL'ENTE**
- 8. GESTIONE DELLA SEGNALAZIONE INTERNA**
  - **8.1 Affidamento della gestione delle segnalazioni**
  - **8.2 Attività di gestione delle segnalazioni**
    - **8.2.1 Ricezione della segnalazione**
    - **8.2.2 Verifica delle condizioni preliminari**
    - **8.2.3 Accertamento ed istruttoria**
    - **8.2.4 Riscontro al segnalante**
    - **8.2.5 Archiviazione e conservazione della documentazione**
- 9. TUTELA DEL SEGNALANTE E DEI SOGGETTI A ESSO ASSIMILATI**
  - **9.1 Riservatezza dell'identità del segnalante**
  - **9.2 Divieto e protezione contro le ritorsioni**
  - **9.3 Limitazioni di responsabilità per il segnalante**
- 10. TRATTAMENTO DEI DATI PERSONALI**
  - **10.1 Natura e caratteristiche del trattamento dei dati personali inerente al WB**
  - **10.2 VIP (Valutazione d'Impatto sulla Protezione dei dati)**
  - **10.3 Esercizio dei diritti degli interessati**
  - **10.4 Registro delle attività di trattamento**
  - **10.5 Soggetti coinvolti nel trattamento**
  - **10.6 Principi applicabili al trattamento dei dati connesso alle segnalazioni**
- 11. ATTIVITÀ DI FORMAZIONE**
- 12. ATTIVITÀ DI INFORMAZIONE**
- 13. SEGNALAZIONE ESTERNA E DIVULGAZIONE PUBBLICA**
  - **13.1 Condizioni per la segnalazione esterna**
  - **13.2 Presentazione e la gestione delle segnalazioni**
  - **13.3 Procedura della divulgazione pubblica**
- 14. SISTEMA SANZIONATORIO**

## 1. FINALITÀ

La presente **Procedura Whistleblowing** (di seguito anche solo: “**Procedura WB**”) definisce le modalità di segnalazione di informazioni relative ad illeciti di diversa natura che possono contribuire a far emergere rischi e/o situazioni potenzialmente pregiudizievoli (c.d. whistleblowing) per.... (di seguito anche solo: “Ente”).

In particolare, **GOIRC** regola, anche attraverso indicazioni operative, il processo di ricezione, accertamento e gestione delle segnalazioni, le forme di tutela della riservatezza dei Segnalanti, dei Segnalati, dei Facilitatori e delle persone menzionate nella segnalazione nonché i ruoli, le attività e le responsabilità dei soggetti coinvolti.

Con la **Procedura WB** viene data attuazione al Decreto legislativo 10 marzo 2023, n. 24 (di seguito anche "Normativa WB" o "Decreto WB"), pubblicato nella Gazzetta Ufficiale del 15 marzo 2023, che ha recepito nell'ordinamento italiano la direttiva UE 2019/1937 riguardante "la protezione delle persone che segnalano violazioni del diritto dell'Unione".

**Il legislatore intende perseguire i seguenti obiettivi:**

- a) garantire un elevato livello di protezione delle persone che segnalano violazioni del diritto dell'Unione, creando canali di comunicazione sicuri, all'interno ed all'esterno delle organizzazioni;
- b) prevenire i fenomeni illeciti nelle organizzazioni pubbliche e private, incentivando l'emersione di condotte pregiudizievoli di cui il Segnalante venga a conoscenza nell'ambito del suo contesto lavorativo in danno dell'ente di appartenenza e, di riflesso, per l'interesse pubblico collettivo.

**GOIRC, al fine di favorire la legalità e la trasparenza all'interno della propria organizzazione, intende, attraverso la presente Procedura WB:**

- rimuovere fattori che possano ostacolare o comunque disincentivare il ricorso alla segnalazione di reati, illeciti o violazioni;
- favorire un ambiente di lavoro virtuoso, garantendo la piena tutela e la massima riservatezza del soggetto Segnalante.

## 2. CONTENUTO

**La presente Procedura riguarda:**

- i soggetti legittimati a presentare le segnalazioni; i soggetti che godono delle misure di protezione previste dalla normativa; l'ambito oggettivo delle segnalazioni ammesse e di quelle estranee all'ambito della disciplina *whistleblowing*; i presupposti per procedere alla segnalazione interna e le relative condizioni di ammissibilità;
- il soggetto esterno, al quale è affidata la gestione delle segnalazioni ed i relativi poteri e gli obblighi;
- le modalità per l'eventuale coinvolgimento da parte del Gestore di altri soggetti, interni all'Ente o esterni, di cui risulti necessario avvalersi per la gestione della segnalazione (l'Ente procede autonomamente e, di volta in volta, alle designazioni privacy);
- le modalità concrete scelte dall'Ente per l'utilizzo del canale di segnalazione interno (piattaforma online e sistema di messaggistica vocale);
- la procedura che il Gestore deve seguire per la gestione delle segnalazioni interne, con indicazione delle varie fasi preliminari e di istruttoria;
- la procedura da seguire nel caso in cui una persona diversa da quella alla quale è affidata la gestione delle segnalazioni riceva una segnalazione identificabile come *whistleblowing*;
- la politica adottata per le ipotesi di segnalazioni anonime o inammissibili;
- le modalità e i termini di conservazione dei dati appropriati e proporzionati ai fini della procedura di *whistleblowing*;
- i necessari adeguamenti prescritti per il trattamento dei dati personali;

- i presupposti per ricorrere alla segnalazione esterna;
- le modalità attraverso cui verranno comunicate ai soggetti potenzialmente interessati le informazioni sull'utilizzo del canale interno e di quello esterno;
- la previsione circa l'attività di formazione sulla disciplina e la procedura stessa;
- la gestione del **conflitto di interessi**, ovvero quando il gestore della segnalazione coincide con il Segnalante, con il segnalato o sia comunque una persona coinvolta o interessata dalla segnalazione.

### 3. CONTESTO NORMATIVO E REGOLATORIO

La normativa prevede un regime di protezione dei soggetti che segnalano condotte illecite poste in essere in violazione di disposizioni europee e nazionali, purché basate su fondati motivi e lesive dell'interesse pubblico o dell'integrità dell'ente, al fine di garantire il recepimento della direttiva senza arretrare nelle tutele già riconosciute nel nostro ordinamento.

Il quadro regolatorio è completato con le Linee Guida ANAC, adottate con delibera del 12 luglio 2023, recanti procedure per la presentazione e gestione delle segnalazioni esterne, nonché indicazioni e principi di cui enti pubblici e privati possono tener conto per i canali interni.

L'Ente tiene conto, quale documento di orientamento nell'applicazione della nuova disciplina, la "Guida operativa per gli enti privati" relativa alla "Nuova disciplina Whistleblowing" pubblicata da Confindustria.

Il **Decreto WB** prevede, per i soggetti del settore privato, l'obbligo di istituire un canale interno di segnalazione.

In tale quadro normativo, le aziende, in applicazione della nuova disciplina, hanno l'obbligo di istituire e gestire un canale interno di segnalazione, adottando le soluzioni organizzative più adeguate in base alla propria struttura e governance.

### 4. AMBITO DI APPLICAZIONE

L'Ente, **sentite** le rappresentanze/organizzazioni sindacali, ha definito la **Procedura WB** in un apposito **atto organizzativo**, di competenza dell'organo amministrativo, adottato con apposita delibera.

La presente **Procedura WB** è volta a disciplinare i canali e le modalità per effettuare una segnalazione ai sensi del D.Lgs. n. 24 del 2023 nonché le successive fasi di ricezione e gestione delle segnalazioni.

#### 4.1 AMBITO SOGGETTIVO DI APPLICAZIONE

##### Posizione soggettiva dell'Ente

L'Ente è destinataria della disciplina normativa in tema di *whistleblowing*, avendo impiegato, nell'ultimo anno, la media di almeno 50 lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato ed è **dotata di un Modello organizzativo 231** aggiornato con l'indicazione del canale di segnalazione WB sicché le segnalazioni oggetto della presente Policy possono riguardare violazioni indicate nella Normativa WB ed essere effettuate attraverso canale interno, esterno, divulgazione pubblica o denuncia.

##### Posizione soggettiva dei segnalanti

**I soggetti legittimati a presentare la segnalazione sono:**

- lavoratori dipendenti e autonomi;
- liberi professionisti e consulenti;
- lavoratori autonomi, collaboratori ed agenti;
- volontari e tirocinanti;
- azionisti e persone con funzione di direzione, amministrazione e controllo, vigilanza o rappresentanza.

**Le segnalazioni possono essere effettuate anche** da coloro che hanno instaurato con l'Ente altri tipi di rapporti giuridici diversi da quelli di lavoro in senso stretto (per "azionisti" s'intendono coloro che siano venuti a conoscenza di violazioni oggetto di segnalazione nell'esercizio dei diritti di cui sono titolari in ragione del loro ruolo di azionisti rivestito nell'Ente).

Le segnalazioni possono anche riguardare un rapporto di lavoro poi terminato, se le informazioni sono state acquisite durante il suo svolgimento, nonché qualora il rapporto non sia ancora iniziato e le informazioni sulle violazioni siano state acquisite durante la selezione o in altre fasi precontrattuali o durante il periodo di prova.

In definitiva, a rilevare è l'esistenza di una relazione qualificata tra il Segnalante e l'Ente nel quale il primo opera, relazione che riguarda attività lavorative o professionali presenti o anche passate.

#### **I seguenti soggetti beneficiano di alcune tutele riconosciute ai Segnalanti:**

- facilitatori;
- persone del medesimo contesto lavorativo del Segnalante e che sono legate ad esso da uno stabile legame affettivo o di parentela entro il quarto grado;
- colleghi di lavoro del Segnalante che lavorano nel medesimo contesto lavorativo e che hanno con il Segnalante un rapporto abituale e corrente;
- enti di proprietà del Segnalante o enti per i quali il Segnalante lavora;
- Enti che operano nel medesimo contesto lavorativo del Segnalante.

## **4.2 AMBITO OGGETTIVO DI APPLICAZIONE**

**Le segnalazioni sono le informazioni**, compresi i fondati sospetti, su violazioni già commesse o non ancora commesse (ma che, sulla base di elementi concreti, potrebbero esserlo), nonché su condotte volte ad occultarle (es. occultamento o distruzione di prove).

Con specifico riferimento a **GOIRC**, le segnalazioni possono avere ad oggetto le seguenti tipologie di illecito, elencate a titolo non esaustivo:

- Corruzione
- Violazioni della riservatezza dei dati e delle informazioni
- Comportamenti che possono comportare criticità nella sicurezza informatica
- Violazioni nell'iter di selezione della controparte
- Violazioni contabili, ivi inclusi flussi finanziari e riciclaggio
- Violazione dei diritti umani e comportamenti contrari al Codice Etico
- Manipolazione del mercato e insider trading
- Violazioni in materia di salute e sicurezza sui luoghi di lavoro
- Violazione del diritto d'autore
- Violazioni in materia ambientale
- Furto o utilizzo improprio delle risorse e dei beni Enteli
- Violazione della privacy
- Conflitti di interesse
- Altri illeciti amministrativi, contabili, civili e penali

- Altre condotte illecite rilevanti ex D.Lgs. 231/2001 o violazioni del Modello 231 e/o delle procedure del sistema normativo interno dell'Ente o Gruppo
- Altri illeciti in ambito, ad es. relativi ai settori: appalti pubblici; prevenzione del riciclaggio e del finanziamento del terrorismo; tutela della vita privata; sicurezza delle reti e dei sistemi informatici
- Altri atti od omissioni che ledono gli interessi finanziari dell'Unione
- Altri atti od omissioni riguardanti il mercato interno (compresa: concorrenza, aiuti di Stato e violazioni fiscali)
- Molestie di genere
- Altre violazioni

In generale, le segnalazioni possono riguardare le violazioni della disciplina nazionale, anche con riferimento ai reati 231 nonché le violazioni riguardanti il diritto europeo nelle materie indicate nel Decreto WB e nelle Linee Guida ANAC.

Il Segnalante o il denunciante deve essere venuto a conoscenza di comportamenti, atti od omissioni nel **contesto lavorativo privato**; s'intende, per "contesto lavorativo", un ambito di applicazione ampio e non limitato a chi abbia un rapporto di lavoro "in senso stretto" con l'organizzazione del settore privato.

**Sono escluse dall'ambito di applicazione della Procedura WB:**

- le segnalazioni legate ad un interesse personale del Segnalante, che attengono ai rapporti individuali di lavoro, ovvero inerenti ai rapporti di lavoro con le figure gerarchicamente sovraordinate (es. vertenze di lavoro, discriminazioni, conflitti interpersonali tra colleghi, segnalazioni su trattamenti di dati effettuati nel contesto del rapporto individuale di lavoro in assenza di una lesione dell'interesse pubblico o dell'integrità dell'ente privato o dell'amministrazione pubblica).

Le segnalazioni escluse in quanto legate a un interesse personale del Segnalante non sono, dunque, considerate segnalazioni *whistleblowing* e, quindi, potranno essere trattate come segnalazioni ordinarie, laddove previsto.

**Sono altresì escluse dall'ambito di applicazione della Procedura WB:**

le segnalazioni in materia di sicurezza e difesa nazionale nonché le segnalazioni relative a violazioni già regolamentate in via obbligatoria in alcuni settori speciali, alle quali continua ad applicarsi la disciplina di segnalazione *ad hoc* (servizi finanziari, prevenzione riciclaggio, terrorismo, sicurezza nei trasporti, tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi).

## 5. CARATTERISTICHE DELLE SEGNALAZIONI

La segnalazione dev'essere il più possibile circostanziata e fornire tutti gli elementi utili per consentire al Gestore di comprendere l'oggetto della segnalazione e condurre un'adeguata istruttoria, ai fini di valutarne la ricevibilità e la fondatezza.

**E' opportuno quindi che la segnalazione contenga quantomeno i seguenti elementi:**

- generalità del Segnalante con indicazione della funzione/attività svolta nell'ambito dell'Ente, fatto salve le segnalazioni anonime;
- una chiara e completa descrizione dei fatti precisi e concordanti, oggetto della segnalazione che attengono alle violazioni;

- se conosciute, le circostanze di tempo e di luogo in cui sono stati commessi i fatti oggetto di segnalazione;
- se conosciute, le generalità o altri elementi che consentano di identificare il soggetto e/o i soggetti cui attribuire i fatti segnalati (qualifica ricoperta e/o funzione/attività svolta all'interno dell'Ente);
- indicazione di eventuali altri soggetti che possano riferire sui fatti oggetto di segnalazione;
- indicazione di eventuali documenti che possono confermare la fondatezza dei fatti oggetto di segnalazione;
- ogni altra informazione che possa fornire un riscontro circa la sussistenza dei fatti oggetto di segnalazione ed in genere ogni altra informazione o documento che possa essere utile a comprendere i fatti segnalati.

**Sono considerate irrilevanti le seguenti informazioni:**

- notizie palesemente prive di fondamento;
  - informazioni che sono già totalmente di dominio pubblico;
- informazioni acquisite solo sulla base di indiscrezioni o vociferazioni scarsamente attendibili (c.d. voci di corridoio);
- dati personali non manifestamente utili ai fini del trattamento della stessa.

L'incoraggiamento a segnalare eventuali illeciti o violazioni di cui si abbia avuto conoscenza non significa, né presuppone, in alcun modo che il Segnalante sia tacitamente o implicitamente autorizzato a svolgere azioni di "indagine", soprattutto se improprie o illecite, per raccogliere prove di illeciti nell'ambiente di lavoro.

## 5.1 SEGNALAZIONI ANONIME

Le segnalazioni anonime (cioè le segnalazioni prive di qualsiasi riferimento utile ai fini dell'individuazione del Segnalante), pur non rientrando nella disciplina della Procedura WB, verranno prese in considerazione dall'Ente solo qualora siano adeguatamente circostanziate e purchè ricevute dall'Ente con le modalità previste dalla Procedura.

## 6. CANALI DI SEGNALAZIONE

La **Normativa WB** prevede tre tipologie di canali di segnalazione:

- a) la segnalazione attraverso un **canale interno** all'Ente;
- b) la segnalazione attraverso un **canale esterno** all'Ente istituito e gestito dall'ANAC;
- c) la **divulgazione pubblica**.

Resta ferma la possibilità di effettuare denunce all'autorità giudiziaria e contabile, ove competenti. La **normativa WB** individua le condizioni per accedere sia alla procedura esterna che alla divulgazione pubblica, per incentivare gli enti a dotarsi di sistemi organizzativi efficienti integrati nei propri sistemi di controllo interno e per realizzare un concreto bilanciamento tra la tutela del Segnalante e la salvaguardia della reputazione dell'ente.

## 7. CANALE INTERNO DI SEGNALAZIONE INDIVIDUATO DALL'ENTE

L'Ente, per consentire ed incentivare le segnalazioni, ha garantito la priorità del ricorso al canale interno di segnalazione attraverso piattaforma informatica in quanto ritenuto maggiormente idoneo ad assicurare la riservatezza del Segnalante e della segnalazione.

Il canale di segnalazione interna, prescelto da GOIRC è idoneo ad assicurare la riservatezza dell'identità del Segnalante, delle persone coinvolte (segnalato, facilitatore, eventuali altri terzi), del contenuto della segnalazione e della relativa documentazione.

**Dunque, le segnalazioni WB possono essere effettuate all'Ente:**

- in forma scritta, con **modalità informatica**: l'Ente ha deciso di utilizzare lo strumento della piattaforma on-line;
- in forma orale, attraverso sistemi di **messaggistica vocale** e, su richiesta del Segnalante, attraverso un eventuale **incontro diretto** con il Gestore della segnalazione, fissato entro un tempo ragionevole.

Il Segnalante, dunque, può scegliere la modalità attraverso la quale effettuare la segnalazione tra quella scritta od orale, avendo l'Ente predisposto sia il canale scritto/informatico che quello orale/messaggistica vocale, mettendoli entrambi a disposizione del Segnalante.

## **8. GESTIONE DELLA SEGNALAZIONE INTERNA**

### **8.1 AFFIDAMENTO DELLA GESTIONE DELLE SEGNALAZIONI**

La gestione del canale di segnalazione interno è stata affidata ad un soggetto esterno, dotato di autonomia ed adeguatamente formato alla gestione delle segnalazioni; in tal modo, l'Ente ha garantito il requisito di autonomia del Gestore della segnalazione, assicurando che le segnalazioni vengano gestite in maniera adeguata e conforme alle disposizioni normative.

In particolare, l'Ente ha garantito, nella gestione delle segnalazioni, l'imparzialità (mancanza di condizionamenti e di pregiudizi nei confronti delle parti coinvolte nelle segnalazioni *whistleblowing*) e l'indipendenza (autonomia e libertà da influenze o interferenze da parte del *management*, al fine di garantire un'analisi oggettiva e imparziale della segnalazione).

Dunque, la gestione del canale di segnalazione è stata affidata ad un soggetto esterno, in possesso dei requisiti di autonomia, indipendenza e professionalità necessari nonché delle risorse e conoscenze specialistiche che garantiscano l'adozione di misure tecniche e organizzative idonee ad assicurare la riservatezza, la protezione dei dati e la segretezza.

Si riportano, di seguito, le **"Istruzioni sintetiche per l'invio delle segnalazioni"**:

Il soggetto che intende fare una segnalazione interna può procedere accedendo alla piattaforma informatica dedicata.

La pagina iniziale del portale fornisce una introduzione generale sul funzionamento del sistema, sulla gestione della segnalazione e sulla garanzia dell'anonimato.

Nella pagina iniziale è presente l'informativa privacy per i dipendenti e sono presenti inoltre i pulsanti per inviare la segnalazione

Cliccando sui pulsanti di invio della segnalazione, il Segnalante accede ad un modulo preimpostato che consente di tipizzare il caso ed effettuare la segnalazione in forma completamente anonima o fornendo riferimenti personali sia del segnalante sia degli eventuali soggetti che hanno posto in essere condotte illecite.

Il Segnalante ha facoltà di allegare documenti, immagini (file elettronici) che reputa utili a sorreggere e/o integrare la segnalazione di illecito. Una volta iniziato l'invio:

- al Segnalante viene indicato il codice identificativo e viene raccomandata l'annotazione dello stesso in quanto solo attraverso di esso il Segnalante potrà seguire gli aggiornamenti e gli esiti riguardanti la sua segnalazione sul portale whistleblowing;

- al soggetto formato e deputato alla gestione delle segnalazioni arriva contestualmente una notifica diretta circa la presenza di una nuova segnalazione.

Entro il termine di 7 giorni la segnalazione viene presa in carico ed il segnalante può avere il riscontro di questo attraverso un messaggio di avviso di ricevimento pubblicato all'interno del Portale, accedendo nell'apposita sezione del Portale.

Successivamente, il gestore della segnalazione, attraverso il Portale, può interfacciarsi con il Segnalante attraverso il sistema di messaggistica dedicato se reputa necessari eventuali approfondimenti oppure, se già in possesso di tutti gli elementi necessari, può dare riscontro al Segnalante attraverso il Portale.

In ogni caso, anche qualora la segnalazione non costituisca un illecito e/o risulti infondata o erroneamente presentata (per via dei suoi contenuti) su canale inadeguato, viene fornito un riscontro al Segnalante entro 3 mesi dalla data di avviso di ricevimento, data che il Portale fa coincidere con quella di invio della segnalazione.

Il canale di segnalazione sopra descritto consente di tutelare, anche tramite il ricorso a strumenti di crittografia, la riservatezza del Segnalante, del segnalato e/o della persona comunque menzionata nella segnalazione nonché del contenuto della segnalazione e della relativa documentazione, a prescindere dalla natura anonima della segnalazione.

Si invitano, pertanto, tutti i Segnalanti ad effettuare segnalazioni non anonime.

L'Ente garantisce la possibilità di effettuare le segnalazioni, anche in forma orale, mediante messaggistica vocale ovvero, su richiesta del Segnalante, mediante l'organizzazione di un incontro di persona, fissato entro un termine ragionevole.

## **8.2 ATTIVITÀ DI GESTIONE DELLE SEGNALAZIONI**

L'attività di gestione delle segnalazioni viene distinta in cinque diverse fasi:

### **8.2.1 RICEZIONE DELLA SEGNALAZIONE**

### **8.2.2 VERIFICA DELLE CONDIZIONI PRELIMINARI**

### **8.2.3 ACCERTAMENTO ED ISTRUTTORIA**

### **8.2.4 RISCONTRO AL SEGNALANTE**

### **8.2.5 ARCHIVIAZIONE E CONSERVAZIONE DELLA DOCUMENTAZIONE**

### **8.2.1 RICEZIONE DELLA SEGNALAZIONE**

#### **A) Istituzione dei canali di segnalazione**

L'Ente ha deciso di esternalizzare il servizio di gestione delle segnalazioni a soggetti esterni, implementando, per la ricezione delle stesse, i seguenti canali:

- **canale in forma scritta, mediante utilizzo della piattaforma informatica Valore24 Whistleblowing**, opportunamente configurata in osservanza dei principi privacy by design, privacy by default e minimizzazione;
- **canale in forma orale, attraverso un sistema di messaggistica vocale**, resa disponibile dallo stesso Fornitore della piattaforma online.

L'Ente, nell'ambito dell'istituito canale orale, ha previsto che il Gestore della segnalazione conservi, previo consenso del Segnalante alla registrazione, la segnalazione all'interno di un dispositivo idoneo alla conservazione e all'ascolto.

In caso di mancata registrazione (ad es. per motivi tecnici), la ricezione della segnalazione verrà documentata mediante resoconto dettagliato del messaggio e il contenuto verrà controfirmato dal Segnalante, previa verifica ed eventuale rettifica; infine, del resoconto sottoscritto verrà fornita copia al Segnalante.

Qualora il *whistleblower* (Segnalante) si avvalga della facoltà di richiedere un **incontro diretto** agli uffici o al Gestore della segnalazione, l'incontro diretto si svolgerà entro il termine di 15 giorni, possibilmente in un luogo adatto a garantire la riservatezza del Segnalante (ove il Segnalante ne faccia richiesta, l'incontro potrà effettuarsi in locali diversi da quelli aziendali; ad es., quelli resi disponibili dal Gestore esterno).

Previo consenso del Segnalante, si provvederà alla registrazione dello stesso attraverso dispositivi idonei alla conservazione ed all'ascolto e, ove non si possa procedere alla registrazione (ad esempio, perché il Segnalante non ha dato il consenso o non si è in possesso di strumenti informatici idonei alla registrazione), verrà redatto un verbale, sottoscritto dal Segnalante e dal soggetto che ha ricevuto la dichiarazione (copia del verbale verrà consegnata al Segnalante).

## **B) Ricezione della segnalazione**

Il Gestore della segnalazione rilascia, mediante la citata piattaforma on-line, al Segnalante, l'**avviso di ricevimento** (al fine di informare il Segnalante dell'avvenuta ricezione della stessa) **entro sette giorni** dalla presentazione della segnalazione stessa; l'avviso verrà inoltrato al recapito indicato dal Segnalante nella segnalazione; in mancanza di tale indicazione (e, dunque, della possibilità di interagire con il Segnalante), la segnalazione può essere considerata non gestibile quanto al *whistleblowing* (lasciando traccia di tale motivazione) ed eventualmente trattata, in presenza di altre *policy* aziendali, come segnalazione ordinaria.

Le **segnalazioni anonime**, eventualmente ricevute, qualora risultino puntuali, circostanziate e supportate da idonea documentazione, potranno essere equiparate alle segnalazioni ordinarie ed eventualmente trattate in conformità alle *policy* aziendali, ove implementate.

Le segnalazioni anonime saranno registrate dal Gestore della segnalazione, conservando la relativa documentazione ricevuta, posto che al Segnalante anonimo che venga successivamente identificato e abbia subito ritorsioni, sono garantite le tutele previste per il *whistleblower*.

Ove la segnalazione interna sia presentata a un **soggetto diverso** da quello individuato ed autorizzato dall'Ente e risulti evidente che si tratti di segnalazione *whistleblowing* (ad es. è esplicitata la dicitura "*whistleblowing*" nell'oggetto o nel testo della comunicazione), la stessa verrà trasmessa, entro sette giorni dal suo ricevimento e senza trattenerne copia, al soggetto interno designato per la gestione delle segnalazioni, dando contestuale notizia della trasmissione al Segnalante.

### **8.2.2 VERIFICA DELLE CONDIZIONI PRELIMINARI**

Completata la fase relativa alla trasmissione dell'avviso di ricevimento, il Gestore delle segnalazioni procederà all'**esame preliminare** della segnalazione ricevuta, valutando la **procedibilità e l'ammissibilità** della stessa.

Nell'ambito della verifica preliminare, il Gestore della segnalazione può richiedere al Segnalante ulteriori elementi necessari per effettuare approfondimenti relativi alla segnalazione.

### **Procedibilità della segnalazione**

In primo luogo, il Gestore **verifica la procedibilità della segnalazione** tenendo conto dell'ambito applicativo, **soggettivo e oggettivo**, della "**Normativa WB**".

Il Gestore, tenendo conto di quanto esposto nella presente Procedura, verifica, dunque, la sussistenza dei seguenti presupposti:

- la legittimazione del Segnalante ad effettuare la segnalazione (**presupposto soggettivo**);
- l'effettiva riconducibilità dell'oggetto della segnalazione all'ambito applicativo della disciplina normativa (**presupposto oggettivo**).

### **Ammissibilità della segnalazione**

In secondo luogo, il Gestore **verifica l'ammissibilità della segnalazione** intesa come segnalazione *whistleblowing*, valutando, in particolare:

- le **circostanze di tempo e di luogo** in cui si è verificato il fatto oggetto della segnalazione (la descrizione dei fatti oggetto della segnalazione, con riferimento a notizie precise ed anche le modalità attraverso cui il Segnalante è venuto a conoscenza dei fatti);
- le **generalità o altri elementi** che consentano di identificare il soggetto cui attribuire i fatti segnalati.

Ai fini della valutazione di **ammissibilità**, il Gestore esamina con attenzione il **contenuto** delle segnalazioni le quali devono essere il più possibile **circostanziate**.

Il Gestore verifica, in particolare, che risultino chiari i seguenti elementi essenziali della segnalazione, ai fini del vaglio di **ammissibilità**:

- **i dati identificativi** del Segnalante (nome, cognome, luogo e data di nascita), nonché un recapito a cui comunicare i successivi aggiornamenti;
- le **circostanze di tempo e di luogo** in cui si è verificato il fatto oggetto della segnalazione e, quindi, una descrizione dei fatti che comprenda anche le modalità con cui si è venuto a conoscenza dei fatti oggetto della segnalazione;
- le **generalità o altri elementi** che consentano di identificare il soggetto cui attribuire i fatti segnalati.

**La segnalazione, quindi, sarà ritenuta inammissibile per i seguenti motivi, indicati a titolo esemplificativo e non esaustivo:**

- mancanza dei dati che costituiscono gli elementi essenziali della segnalazione;
- manifesta infondatezza per mancanza degli elementi di fatto riconducibili alle violazioni tipizzate dal legislatore;
- accertato contenuto generico della segnalazione, tale da non consentirne la comprensione dei fatti;
- produzione di sola documentazione senza la segnalazione vera e propria di violazioni ovvero di documentazione non appropriata inconfidente o comunque tale da rendere incomprensibile il contenuto stesso della segnalazione.

Qualora la segnalazione risulti **improcedibile o inammissibile**, il Gestore della segnalazione può procedere all'**archiviazione**, garantendo comunque la tracciabilità delle motivazioni a supporto.

### **8.2.3 ACCERTAMENTO ED ISTRUTTORIA**

Verificata la procedibilità e l'ammissibilità della segnalazione, il Gestore avvia l'istruttoria interna sui fatti segnalati per valutarne la fondatezza.

Nello svolgimento dell'istruttoria, il Gestore garantisce tempestività e rispetto dei principi di obiettività, competenza e diligenza professionale.

In caso di **conflitto di interessi**, ovvero quando il gestore della segnalazione coincide con il Segnalante, con il segnalato o sia comunque una persona coinvolta o interessata dalla segnalazione, la segnalazione può essere indirizzata all'OdV, al vertice dell'Ente oppure a un altro soggetto/ufficio che possa garantirne la gestione efficace, indipendente e autonoma, sempre nel rispetto dell'obbligo di riservatezza previsto dalla disciplina.

Nella fase di accertamento, si valuta la fondatezza o meno dei fatti segnalati, anche al fine di attivare eventuali procedure correttive sui processi interessati nell'ottica di rafforzare il sistema di controllo interno.

**Le verifiche** si svolgeranno secondo discrezionalità del Gestore, nei **seguenti modi indicati a titolo esemplificativo**:

- acquisendo gli elementi informativi necessari alle valutazioni attraverso l'analisi dei dati e documenti ricevuti;
- attraverso il coinvolgimento di strutture o di soggetti specializzati esterni in ragione delle specifiche competenze tecniche e professionali richieste;
- mediante audizione di eventuali soggetti interni/esterni.

Il Gestore mantiene le interlocuzioni con il Segnalante e richiede eventualmente a quest'ultimo le integrazioni ritenute necessarie, dando diligente seguito alle Segnalazioni.

L'attività di istruttoria e di accertamento spetta esclusivamente al Gestore delle segnalazioni.

Il Gestore richiede, se opportuno ed utile ai fini della gestione, documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.

Ove risulti necessario avvalersi dell'assistenza tecnica di professionisti terzi, verranno oscurati i dati che possano rendere identificabile il Segnalante o altre persone coinvolte (il "facilitatore" o altre persone menzionate nella segnalazione).

Ove risulti necessario avvalersi di soggetti interni diversi dal Gestore (altre funzioni aziendali), ad essi andranno estesi gli obblighi di riservatezza e confidenzialità applicabili al caso di specie.

Ove i dati oggetto di segnalazione siano necessari all'indagine condotta da soggetti esterni (eventualmente coinvolti dal Gestore), sarà necessario estendere i doveri di riservatezza e confidenzialità anche a tali soggetti esterni.

Gli obblighi di riservatezza e confidenzialità verranno applicati mediante specifiche clausole contrattuali da inserire negli accordi stipulati con i soggetti esterni ovvero attraverso atti di nomina/avvertenza sottoscritti dai soggetti interni; in entrambi i casi, andranno assicurate le necessarie designazioni privacy.

Tutte le fasi dell'attività di accertamento sono tracciate e archiviate al fine di dimostrare la corretta diligenza tenuta nel dare seguito alla segnalazione.

Durante le fasi di istruttoria e di accertamento della segnalazione, è necessario sia tutelata la riservatezza dell'identità del Segnalante, del segnalato e di tutte le persone coinvolte e/o menzionate nella segnalazione.

#### **8.2.4 RISCONTRO AL SEGNALANTE**

Il Gestore della segnalazione fornisce un **riscontro** al Segnalante, entro tre mesi dalla data di avviso di ricevimento o - in mancanza di tale avviso - entro tre mesi dalla data di scadenza del termine di sette giorni per tale avviso.

Il riscontro, alla scadenza del termine indicato, può essere definitivo se l'istruttoria è terminata oppure interlocutorio sull'avanzamento dell'istruttoria, ancora non ultimata.

Alla scadenza dei tre mesi, il Gestore della segnalazione comunica al Segnalante:

- **l'avvenuta archiviazione** della segnalazione, motivandone le ragioni;
- l'avvenuto **accertamento della fondatezza della segnalazione** e la sua trasmissione agli organi interni competenti;
- **l'attività svolta fino a questo momento e/o l'attività che intende svolgere.**

#### **8.2.5 ARCHIVIAZIONE E CONSERVAZIONE DELLA DOCUMENTAZIONE.**

**Una volta completata l'attività di accertamento, il Gestore della segnalazione può:**

- archiviare la segnalazione perché infondata, motivandone le ragioni;
- dichiarare fondata la segnalazione e rivolgersi agli organi/funzioni interne competenti per i relativi seguiti (es. il *management* aziendale, ufficio legale o risorse umane); infatti, al Gestore della segnalazione non compete alcuna valutazione in ordine alle responsabilità individuali ed agli eventuali successivi provvedimenti o procedimenti conseguenti (rimessi agli apicali e funzioni Enteli competenti, rispettando il MOG 231 adottato ed il flusso dei dati verso l'OdV).

I dati contenuti nelle segnalazioni e nella relativa documentazione sono conservati per il tempo necessario alla gestione della segnalazione e, comunque, non oltre **5 anni** a decorrere dalla data della comunicazione dell'esito finale della segnalazione.

Ove pervengano segnalazioni fuori ambito o semplici lamentele (ad esempio, contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale del Segnalante, comunicazioni o reclami relativi ad attività di natura commerciale), le stesse saranno immediatamente cancellate ovvero, sussistendone i presupposti, saranno conservate per un periodo non superiore a **5 mesi** dall'archiviazione della segnalazione.

In generale, i dati contenuti nelle segnalazioni e nella relativa documentazione potranno essere conservati per un periodo ulteriore rispetto ai 5 anni a decorrere dalla data della comunicazione dell'esito finale della segnalazione ove sussista la necessità di adempiere agli obblighi di legge nel rispetto della vigente normativa in tema di protezione dei dati personali.

Nel caso in cui sia avviata un'azione giudiziaria e/o disciplinare nei confronti del segnalato, ovvero del Segnalante che avesse reso dichiarazioni in malafede, false o diffamatorie, i dati personali potranno essere conservati fino a conclusione definitiva del procedimento giudiziario e/o disciplinare.

I dati personali, se già trattati nell'ambito del rapporto di lavoro in corso con il Titolare datore di lavoro, saranno conservati nei termini indicati nell'informativa generale dei dipendenti.

### **9. TUTELA DEL SEGNALANTE E DEI SOGGETTI A ESSO ASSIMILATI**

Uno dei principali cardini della disciplina del whistleblowing è rappresentato dalle tutele riconosciute al Segnalante per le segnalazioni effettuate nel rispetto della disciplina.

**L'Ente, nel rispetto della normativa WB, protegge il Segnalante**, adempiendo l'obbligo di riservatezza della sua identità e rispettando il divieto di atti ritorsivi nei suoi confronti.

L'Ente è consapevole della limitazione di responsabilità del Segnalante per la rilevazione o diffusione di alcune tipologie di informazioni protette.

Applica le misure di protezione al soggetto Segnalante ed ai soggetti ad esso assimilati che potrebbero essere destinatari di ritorsioni, in ragione del ruolo assunto o della particolare vicinanza o rapporto con il Segnalante:

- **facilitatore**: la persona fisica che assiste il Segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata (il facilitatore potrebbe essere il collega dell'ufficio del Segnalante o di un altro ufficio che lo assiste in via riservata nel processo di segnalazione); il facilitatore potrebbe essere un collega che riveste anche la qualifica di sindacalista se assiste il Segnalante in suo nome, senza spendere la sigla sindacale; se, invece, assiste il Segnalante utilizzando la sigla sindacale, lo stesso non riveste il ruolo di facilitatore;
- persone del **medesimo contesto lavorativo** del Segnalante e che sono legate a esso da uno stabile legame affettivo o di parentela entro il quarto grado (coloro che hanno un rapporto di convivenza con il Segnalante; non solo come convivenza in senso stretto, bensì anche come rapporto di natura affettiva caratterizzato da una certa stabilità);
- **colleghi di lavoro** del Segnalante che lavorano **nel medesimo contesto lavorativo** dello stesso e che hanno con detta persona un **rapporto abituale e corrente** (rapporti non meramente sporadici, occasionali, episodici ed eccezionali ma attuali, protratti nel tempo, connotati da una certa continuità tali da determinare un rapporto di "comunanza", di amicizia);
- **enti di proprietà**, in via esclusiva o in compartecipazione maggioritaria di terzi, del Segnalante o del denunciante;
- **enti presso** i quali il Segnalante, denunciante o chi effettua una divulgazione pubblica **lavorano**.

Per la corretta individuazione di tali soggetti, il Gestore della segnalazione, nell'ambito del processo di istruttoria della segnalazione, richiede al Segnalante di indicare esplicitamente l'esistenza di tali soggetti, dimostrando la sussistenza dei relativi presupposti.

## 9.1 RISERVATEZZA DELL'IDENTITÀ DEL SEGNALANTE

**GOIRC garantisce la riservatezza** dell'identità del Segnalante delle persone coinvolte e/o menzionate nella segnalazione, nonché ai facilitatori, in considerazione del rischio di ritorsioni; garantisce altresì la riservatezza di ogni altra informazione, inclusa l'eventuale documentazione allegata, dalla quale si possa direttamente o indirettamente risalire all'identità del whistleblower.

La riservatezza deve essere garantita per ogni modalità di segnalazione, quindi, anche quando avvenga in forma orale (messaggistica vocale).

L'Ente, pertanto, nel rispetto delle previsioni in materia di protezione dei dati personali, nell'istituzione e regolamentazione del canale interno, predispone adeguate misure volte a mantenere riservata l'identità del Segnalante, il contenuto della segnalazione e la relativa documentazione.

Nell'ambito del procedimento disciplinare attivato dall'Ente contro il presunto autore della condotta segnalata, l'identità del Segnalante non viene rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa.

Qualora invece la contestazione sia fondata, in tutto o in parte, sulla segnalazione e l'identità del Segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare o della persona comunque coinvolta nella segnalazione, quest'ultima sarà utilizzabile ai fini del procedimento disciplinare solo previo consenso espresso del Segnalante alla rivelazione della propria identità.

In tali casi, è dato preventivo avviso al Segnalante, mediante comunicazione scritta, delle ragioni che

rendono necessaria la rivelazione dei dati riservati.

Qualora il Segnalante neghi il proprio consenso, la segnalazione non potrà essere utilizzata nel procedimento disciplinare che, quindi, non potrà essere avviato o proseguito in assenza di elementi ulteriori sui quali fondare la contestazione.

Resta ferma in ogni caso, sussistendone i presupposti, la facoltà dell'Ente di procedere con la denuncia all'Autorità giudiziaria.

## 9.2 DIVIETO E PROTEZIONE CONTRO LE RITORSIONI

L'Ente rispetta il divieto di atti ritorsivi nei confronti del Segnalante, intesi come qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, che si verifichi nel contesto lavorativo e che determini, in via diretta o indiretta, un danno ingiusto ai soggetti tutelati.

È consapevole della nullità degli atti ritorsivi adottati in violazione di tale divieto e del possibile intervento dell'ANAC, quale autorità preposta a ricevere dal Segnalante e gestire le comunicazioni su presunte ritorsioni dallo stesso subite.

Applica la stessa tutela nei confronti dei facilitatori e degli altri soggetti assimilati al Segnalante.

Questo implica, da parte del Segnalante, un'attenta diligenza nella valutazione delle informazioni che non è sufficiente si fondino su semplici supposizioni, "voci di corridoio" o notizie di pubblico dominio.

**Di seguito sono elencate, in modo non esaustivo, le possibile fattispecie ritorsive:**

- a) licenziamento, sospensione o misure equivalenti;
- b) retrocessione di grado o mancata promozione;
- c) mutamento di funzioni, cambiamento del luogo di lavoro, riduzione dello stipendio, modifica dell'orario di lavoro;
- d) sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- e) note di merito negative o referenze negative;
- f) adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- g) coercizione, intimidazione, molestie o ostracismo;
- h) discriminazione o comunque trattamento sfavorevole;
- i) mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- j) mancato rinnovo o risoluzione anticipata di un contratto di lavoro a termine;
- k) annullamento di una licenza o di un permesso;
- l) richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Sia le funzioni aziendali maggiormente coinvolte che il Gestore delle segnalazioni prenderanno in seria considerazione, nell'espletamento delle proprie attività, il potenziale carattere ritorsivo di alcuni atti, comportamenti od omissioni posti in essere nei confronti dei lavoratori.

## 9.3 LIMITAZIONI DI RESPONSABILITÀ PER IL SEGNALANTE

La **normativa WB** limita la responsabilità del Segnalante rispetto alla rivelazione e alla diffusione di alcune categorie di informazioni, che altrimenti lo esporrebbero a responsabilità penali, civili e amministrative.

**Non è imputabile al Segnalante una responsabilità penale, civile o amministrativa in merito a:**

- rivelazione e utilizzazione del segreto d'ufficio (art. 326 c.p.);
- rivelazione del segreto professionale (art. 622 c.p.);
- rivelazione dei segreti scientifici e industriali (art. 623 c.p.);
- violazione del dovere di fedeltà e di lealtà (art. 2105 c.c.);
- violazione delle disposizioni relative alla tutela del diritto d'autore;
- violazione delle disposizioni relative alla protezione dei dati personali;
- rivelazione o diffusione di informazioni sulle violazioni che offendono la reputazione della persona

coinvolta.

**Affinché operino le suddette limitazioni di responsabilità occorrono, tuttavia, le seguenti condizioni:**

- a) al momento della rivelazione o della diffusione vi siano fondati motivi per ritenere che le informazioni siano necessarie per svelare la violazione oggetto di segnalazione;
- b) la segnalazione sia effettuata nel rispetto delle condizioni previste dalla **Normativa WB** per beneficiare della tutela contro le ritorsioni (fondati motivi per ritenere veritieri i fatti segnalati, la violazione sia tra quelle segnalabili e siano rispettate le modalità e le condizioni di accesso alla segnalazione).

La limitazione di responsabilità a favore del Segnalante opera se le ragioni alla base della rivelazione o diffusione non sono fondate su semplici illazioni, gossip, fini vendicativi, opportunistici o scandalistici.

In ogni caso, non è esclusa la responsabilità per condotte che:

- non siano collegate alla segnalazione;
- non siano strettamente necessarie a rivelare la violazione;
- configurino un'acquisizione di informazioni o l'accesso a documenti in modo illecito.

## **10. TRATTAMENTO DEI DATI PERSONALI**

Considerato che la ricezione e la gestione delle segnalazioni interne determinano un trattamento dei dati personali delle persone a vario titolo coinvolte nei fatti segnalati, **l'Ente presta particolare attenzione al rispetto della disciplina sulla privacy.**

### **10.1 NATURA E CARATTERISTICHE DEL TRATTAMENTO DEI DATI PERSONALI INERENTE AL WB**

**Il trattamento dei dati personali consistente nella ricezione e gestione delle segnalazioni:**

- riguarda dati di natura comune, di natura particolare (ex "dati sensibili") e giudiziari (condanne penali e reati), eventualmente contenuti nella segnalazione e nei documenti allegati, relativi a tutte le persone fisiche - identificate o identificabili - a vario titolo coinvolte nelle vicende segnalate (Segnalante, segnalato, facilitatore, eventuali altri terzi), c.d. interessati;
- è necessario per dare attuazione agli obblighi di legge previsti dalla disciplina whistleblowing la cui osservanza è condizione di liceità del trattamento ex art. 6, par. 1, lett. c) e par. 2 e 3, art. 9, par. 2, lett. b) e artt. 10 e 88 del GDPR;
- è realizzato al solo fine di gestire le segnalazioni.

### **10.2 VIP (VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI)**

Il trattamento dei dati personali inerente al WB, in ragione della particolare delicatezza delle informazioni potenzialmente trattate, della vulnerabilità degli interessati nel contesto lavorativo, nonché dello specifico regime di riservatezza dell'identità del Segnalante previsto dalla legge, **presenta rischi specifici per i diritti e le libertà degli interessati** e, pertanto, viene preceduto da una **valutazione d'impatto sulla protezione dei dati, c.d. VIP o DPIA** (art. 13, co. 6 della normativa WB e artt. 35 e 36 del GDPR) effettuata dall'Ente prima dell'inizio del trattamento dei dati.

### **10.3 ESERCIZIO DEI DIRITTI DEGLI INTERESSATI**

L'esercizio dei diritti degli interessati (es. accesso, rettifica, aggiornamento, cancellazione, limitazione del trattamento, portabilità, opposizione) può essere limitato qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del Segnalante (art. 13, co. 3 del Decreto n. 24/2023 e art. 2-undecies del Codice privacy).

### **10.4 REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO**

Il trattamento dei dati personali relativo alla ricezione ed alla gestione delle segnalazioni verrà censito nel **registro delle attività di trattamento (RAT)** in conformità all'art. 30 del GDPR, procedendo al relativo aggiornamento.

### **10.5 SOGGETTI COINVOLTI NEL TRATTAMENTO**

L'Ente, attivando il canale interno, effettua i trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni in qualità di **Titolare del trattamento**.

I soggetti esterni a cui l'Ente affida la gestione del canale di segnalazione trattano i dati in qualità di **Responsabili del trattamento** ai sensi dell'art. 28 del GDPR, con conseguente conclusione del relativo accordo di nomina del Responsabile esterno.

Le persone fisiche preposte alla ricezione e/o alla gestione della segnalazione trattano i dati in qualità di **soggetti Autorizzati al trattamento**, espressamente autorizzati e previamente istruiti in tal senso dal titolare ovvero dal responsabile ai sensi dell'art. 29, dell'art. 32, par. 4 del GDPR e dell'art. 2-*quaterdecies* del Codice privacy ovvero in qualità di Responsabili del trattamento.

Ove possibile, lo svolgimento delle attività degli autorizzati è tracciato al fine di evitare l'uso improprio di dati relativi alla segnalazione ed assicurare le garanzie a tutela del Segnalante.

In ogni caso, è escluso il tracciamento di qualunque informazione che possa ricondurre all'identità ovvero all'attività del Segnalante.

### **10.6 PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI CONNESSO ALLE SEGNALAZIONI**

**GOIRC** effettua il trattamento dei dati personali, osservando i seguenti principi:

- **Trasparenza** (art. 5, par. 1, lett. a) del GDPR), rendendo ex ante ai possibili interessati **un'ideonea informativa sul trattamento dei dati personali**, recante, tra le altre, le informazioni su: il titolare del trattamento e i relativi dati di contatto; la finalità del trattamento; la base giuridica del trattamento; le modalità del trattamento; l'ambito del trattamento ed i soggetti cui sono comunicati i dati (es. responsabili, autorizzati del trattamento); il periodo di conservazione dei dati personali.

Tale informativa (fornita in allegato alla procedura *whistleblowing*) viene pubblicata sul sito web e in un'apposita sezione dell'applicativo informatico utilizzato per la gestione delle segnalazioni.

Nella fase di ricezione della segnalazione non vengono fornite informative specifiche a soggetti diversi dal Segnalante per evitare che l'attivazione di flussi informativi dai quali è possibile dedurre il coinvolgimento della persona in una segnalazione possa vanificare le tutele per la riservatezza previste dalla legge.

- **Limitazione delle finalità** (art. 5, par. 1, lett. b) del GDPR): le segnalazioni non possano essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.

- **Minimizzazione dei dati** (art. 5, par. 1, lett. c) del GDPR): i dati manifestamente non utili alla trattazione di una specifica segnalazione non sono raccolti o, in caso di raccolta accidentale, sono prontamente cancellati; il principio di minimizzazione viene dall'Ente interpretato in modo restrittivo ai soli casi in cui sia palese la assoluta irrilevanza di parti della segnalazione che contengono dati personali rispetto alla vicenda segnalata.

- **Limitazione della conservazione** (art. 5, par. 1, lett. e) del GDPR): le segnalazioni e la relativa documentazione sono conservate per il tempo necessario alla trattazione della segnalazione e, comunque, non oltre 5 anni dalla comunicazione dell'esito finale della procedura.

- **Integrità e riservatezza** (art. 5, par. 1, lett. f) del GDPR), prevedendo l'individuazione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi del trattamento e promuovendo il ricorso a strumenti di crittografia.

- **Privacy by design e by default** (art. 25 del GDPR), considerando le garanzie di protezione dei dati personali sin dalla progettazione del canale di segnalazione (*privacy by design*) ed assicurando che per impostazione predefinita (*privacy by default*) siano trattati solo i dati personali strettamente necessari in relazione alla specifica segnalazione.

- **Riservatezza**, garantendo il divieto di tracciamento dei canali di segnalazione e la non tracciabilità del Segnalante nel momento in cui viene stabilita la connessione a tali canali.

## 11. ATTIVITÀ DI FORMAZIONE

GOIRC, al fine di garantire una gestione consapevole, accurata e professionale delle segnalazioni intende sensibilizzare, anche attraverso attività di formazione e informazione, i soggetti interni ed esterni coinvolti nell'ambito del whistleblowing in merito alle implicazioni etiche, legali e di riservatezza connesse alle procedure di segnalazione.

**A tal fine, predispone il seguente piano formativo:**

a) gli uffici o le persone cui è demandata la gestione del canale di segnalazione devono ricevere una specifica formazione relativa alla gestione del canale;

b) gli uffici o le persone cui è demandata la gestione del canale di segnalazione mettono a disposizione del Segnalante informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne od esterne.

c) l'attività di formazione avrà ad oggetto le seguenti tematiche:

- aspetti normativi: principi e disposizioni del Decreto n. 24/2023; disciplina sul trattamento dei dati personali, ecc.;

- procedure e presupposti: policies, procedure e modalità operative adottate per la gestione del canale di segnalazione;

- principi generali di comportamento: confidenzialità e riservatezza (applicazione delle misure tecniche e organizzative da parte del personale cui è affidata la gestione delle segnalazioni); etica ed integrità (promozione di un ambiente etico e integro all'interno dell'Ente, azioni improntate all'onestà, trasparenza e responsabilità nella gestione delle segnalazioni);

- ascolto attivo, competenze comunicative e collaborazione (sensibilizzazione del personale cui è affidata la gestione delle segnalazioni circa l'ascolto attivo e la comunicazione empatica, con particolare riguardo alle interlocuzioni con la persona Segnalante);

d) la formazione viene erogata con cadenza periodica (quantomeno annuale) per garantirne l'efficacia;

e) viene garantito un adeguato coinvolgimento delle risorse coinvolte, mediante sessioni formative in aula, *workshop* e formazione in modalità *e-learning*.

## 12. ATTIVITÀ DI INFORMAZIONE

L'Ente mette a disposizione del Segnalante informazioni chiare circa il canale, le procedure ed i presupposti per effettuare le segnalazioni, interne o esterne.

A tal fine, garantisce un'adeguata informativa in ordine all'utilizzo del canale interno e di quello esterno gestito da ANAC, con particolare riguardo ai presupposti per effettuare le segnalazioni attraverso tali canali, ai soggetti competenti cui è affidata la gestione delle segnalazioni interne, nonché alle procedure adottate.

Tali informazioni saranno esposte nei luoghi di lavoro in un punto visibile, accessibile a tutte le persone.

Detta esposizione consente la visibilità anche ai soggetti che, pur non essendo presenti fisicamente nei luoghi di lavoro, sono legittimati ad effettuare segnalazioni di whistleblowing.

Inoltre, tali informazioni saranno esposte in una sezione apposita del sito web istituzionale dell'Ente e della piattaforma informatica.

**GOIRC fornisce le seguenti informazioni, indicate a titolo esemplificativo e non esaustivo:**

- soggetti legittimati a effettuare le segnalazioni;

- soggetti che godono delle misure di protezione riconosciute dalla legge;

- violazioni che possono essere segnalate;

- presupposti per effettuare la segnalazione interna o esterna;

- indicazioni sul canale di segnalazione interno e su quello esterno gestito da ANAC;

- procedure che il Segnalante deve seguire per effettuare in maniera corretta una segnalazione (a

- titolo esemplificativo, gli elementi che la segnalazione deve contenere);
- soggetti competenti cui è affidata la gestione delle segnalazioni interne;
  - attività che, una volta correttamente effettuata la segnalazione, devono essere svolte dal soggetto che ha ricevuto e che gestisce la segnalazione;
  - tutele riconosciute dalla legge al Segnalante e agli altri soggetti che godono di protezione;
  - condizioni al verificarsi delle quali è esclusa la responsabilità del Segnalante;
  - sistema sanzionatorio applicabile in caso di violazione delle disposizioni della normativa.

### **13. SEGNALAZIONE ESTERNA E DIVULGAZIONE PUBBLICA**

La **normativa WB** attribuisce all'ANAC il compito di istituire un canale di segnalazione, accessibile anche ai soggetti appartenenti al settore privato, idoneo ad assicurare la riservatezza dell'identità del Segnalante e di coloro che sono coinvolti nella segnalazione, del contenuto della segnalazione stessa e della relativa documentazione.

Il Decreto n. 24/2023 introduce, inoltre, una nuova forma di segnalazione attraverso la divulgazione pubblica.

L'Ente intende scongiurare il rischio di ricorso a tali canali in assenza dei relativi presupposti e, per questo motivo, predispone il citato programma di formazione dei dipendenti e pubblica sul suo sito idonee informazioni circa le caratteristiche dei diversi canali, le condizioni per il loro utilizzo e le conseguenze di un uso improprio degli stessi.

#### **13.1 CONDIZIONI PER LA SEGNALAZIONE ESTERNA**

**Il Segnalante può ricorrere alla “procedura esterna” soltanto se sussiste una delle seguenti condizioni:**

- nel suo contesto lavorativo non è prevista l'attivazione del canale interno come obbligatoria o, se prevista, non è stata attivata;
- la segnalazione non ha avuto seguito (tale circostanza si verifica quando il soggetto cui è affidata la gestione del canale non abbia intrapreso entro i termini previsti dalla normativa alcuna attività circa l'ammissibilità della segnalazione, la verifica della sussistenza dei fatti segnalati o la comunicazione dell'esito dell'istruttoria svolta);
- ha fondati motivi di ritenere che se effettuasse la segnalazione interna questa non avrebbe seguito (ad esempio, per il rischio che le prove di condotte illecite possano essere occultate o distrutte o vi sia il timore di un accordo tra chi riceve la segnalazione e la persona coinvolta nella segnalazione, o ancora all'ipotesi in cui il gestore della segnalazione sia in conflitto di interessi);
- ha fondati motivi di ritenere che se effettuasse la segnalazione interna andrebbe incontro a ritorsioni (ad esempio quando si siano già verificate situazioni ed eventi analoghi nell'Ente);
- ha fondati motivi di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

In ogni caso, i fondati motivi devono essere basati su circostanze concrete che devono essere allegate alla segnalazione e su informazioni effettivamente acquisibili.

#### **13.2 PRESENTAZIONE E GESTIONE DELLE SEGNALAZIONI**

L'ANAC ha disciplinato le modalità di presentazione e gestione delle segnalazioni esterne, prevedendo che le stesse possono essere effettuate soltanto dalle persone fisiche legittimate ai sensi della normativa (non potranno, invece, essere effettuate, ad esempio, segnalazioni da parte di rappresentanti di organizzazioni sindacali).

**Con riguardo alle modalità di presentazione, le segnalazioni possono essere effettuate:**

- tramite piattaforma informatica, delineata come canale prioritario di segnalazione in quanto ritenuto maggiormente idoneo a garantire la riservatezza del Segnalante e della segnalazione (i dati della segnalazione sono crittografati e i dati del Segnalante sono oscurati e segregati in apposita sezione della piattaforma, in modo da renderli inaccessibili anche all'ufficio istruttore di ANAC);
- oralmente, attraverso un servizio telefonico con operatore (un componente dell'Ufficio ANAC competente, che acquisisce la segnalazione telefonica e la inserisce sulla piattaforma ANAC

unitamente al file audio della registrazione);

- tramite incontri diretti fissati entro un termine ragionevole, cui consegue l'inserimento della segnalazione nella piattaforma da parte dell'operatore (per ricorrere all'incontro diretto è necessaria una richiesta motivata).

**Per essere ammissibile, nella segnalazione devono essere indicati:** la denominazione e i recapiti del *whistleblower*; i fatti oggetto di segnalazione e l'Amministrazione o Ente in cui essi sono avvenuti; l'Amministrazione o l'Ente nel cui contesto lavorativo il *whistleblower* opera e il profilo professionale da quest'ultimo rivestito.

**La segnalazione esterna è considerata, inoltre, inammissibile per i seguenti motivi:** manifesta infondatezza per l'assenza di elementi di fatto riconducibili alle violazioni tipizzate nell'art. 2, co. 1, lett. a), della normativa; manifesta insussistenza dei presupposti di legge per l'esercizio dei poteri di vigilanza dell'Autorità; manifesta incompetenza dell'Autorità sulle questioni segnalate; accertato contenuto generico della segnalazione esterna, tale cioè da non consentire la comprensione dei fatti, ovvero segnalazione esterna corredata da documentazione non appropriata, inconferente o comunque tale da rendere incomprensibile il contenuto stesso della segnalazione; produzione di sola documentazione in assenza della segnalazione esterna; mancanza dei dati che costituiscono elementi essenziali della segnalazione esterna; sussistenza di violazioni di lieve entità.

Qualora la segnalazione non sia dichiarata inammissibile, l'Ufficio può trasmettere la segnalazione e la documentazione allegata agli uffici di vigilanza dell'Autorità competenti per materia, l'Ufficio istruttore deve provvedere a inviare la relativa segnalazione all'autorità amministrativa competente oppure all'autorità giudiziaria (in caso di illeciti penali o erariali) e di tale trasmissione deve essere informato il Segnalante.

In ogni caso, l'Ufficio comunica al Segnalante: l'archiviazione predisposta o che intende predisporre; la trasmissione all'Autorità competente già effettuata o che intende effettuare; l'attività già svolta dall'Ufficio di vigilanza competente.

### **13.3 PROCEDURA DELLA DIVULGAZIONE PUBBLICA**

La normativa introduce anche la possibilità per il Segnalante di effettuare una divulgazione pubblica beneficiando della protezione e ciò determina potenzialità lesive per l'Ente di una denuncia effettuata in assenza di giustificati motivi o di fondati elementi di prova (la divulgazione può essere effettuata attraverso la stampa o anche social network e nuovi canali di comunicazione; ad es. Facebook, Twitter, ecc.).

Ciò rende di estrema importanza circoscrivere il più possibile il ricorso a tale istituto e costruire in modo efficace i canali interni di segnalazione.

**Per ricorrere a tale procedura deve sussistere almeno una delle seguenti condizioni:**

- che si sia previamente utilizzato il canale interno e/o esterno, ma non vi sia stato riscontro o non vi sia stato dato seguito entro i termini previsti dalla normativa;

- che il Segnalante ritenga sussistere fondati motivi di un "pericolo imminente e palese per il pubblico interesse", considerato come una situazione di emergenza o di rischio di danno irreversibile, anche all'incolumità fisica di una o più persone, che richieda che la violazione sia tempestivamente svelata con ampia risonanza per impedirne gli effetti;

- che il Segnalante ritenga sussistere fondati motivi per ritenere che la segnalazione esterna possa comportare un rischio di ritorsione oppure non avere efficace seguito (ad esempio potrebbe ricorrere un pericolo di distruzione delle prove o di collusione tra l'autorità preposta a ricevere la segnalazione e l'autore della violazione).

Dovrebbe, in altri termini, trattarsi di situazioni particolarmente gravi di negligenza o comportamenti dolosi all'interno dell'Ente.

Anche in tali casi, inoltre, i fondati motivi che legittimano il ricorso alla segnalazione esterna devono essere fondati sulla base di circostanze concrete che devono essere allegate alla segnalazione e su informazioni effettivamente acquisibili.

#### **14. SISTEMA SANZIONATORIO**

**In merito al regime sanzionatorio, la normativa, come specificata nelle Linee Guida ANAC, prevede quanto segue:**

- nelle ipotesi di mancata istituzione del canale, di mancata adozione delle procedure o di adozione di procedure non conformi, il responsabile è individuato nell'organo di indirizzo;
- nelle ipotesi in cui non sia stata svolta l'attività di verifica e analisi delle segnalazioni ricevute, nonché quando sia stato violato l'obbligo di riservatezza, il responsabile è il gestore delle segnalazioni.

**Nel dettaglio, le sanzioni amministrative pecuniarie sono le seguenti:**

- a) da 10.000 a 50.000 euro quando accerta che la persona fisica individuata come responsabile abbia commesso ritorsioni;
- b) da 10.000 a 50.000 euro quando accerta che la persona fisica individuata come responsabile abbia ostacolato la segnalazione o abbia tentato di ostacolarla;
- c) da 10.000 a 50.000 euro quando accerta che la persona fisica individuata come responsabile abbia violato l'obbligo di riservatezza di cui all'art. 12 del d.lgs. n. 24/2023. Restano salve le sanzioni applicabili dal Garante per la protezione dei dati personali per i profili di competenza in base alla disciplina in materia di dati personali 146;
- d) da 10.000 a 50.000 euro quando accerta che non sono stati istituiti canali di segnalazione; in tal caso responsabile è considerato l'organo di indirizzo sia negli enti del settore pubblico che in quello privato;
- e) da 10.000 a 50.000 euro quando accerta che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero che l'adozione di tali procedure non è conforme a quanto previsto dal decreto; in tal caso responsabile è considerato l'organo di indirizzo sia negli enti del settore pubblico che in quello privato;
- f) da 10.000 a 50.000 euro quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute; in tal caso responsabile è considerato il gestore delle segnalazioni;
- g) da 500 a 2.500 euro, quando è accertata, anche con sentenza di primo grado, la responsabilità civile della persona segnalante per diffamazione o calunnia nei casi di dolo o colpa grave, salvo che la medesima sia stata già condannata, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia dell'autorità giudiziaria.