

**FONDAZIONE CARIGE**

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

Edizione/Revisione	Motivo della Edizione/Revisione	Data	Approvazione CDA
Rev. 03	Aggiornamento per modifiche normative	01.10.2024	

**INDICE**

<b>PARTE GENERALE</b> .....	<b>4</b>
<b>1 PREMessa. FINALITÀ DI EMISSIONE DELLA NUOVA RELEASE DEL MOG</b> .....	<b>5</b>
<b>2 IL QUADRO NORMATIVO DI RIFERIMENTO</b> .....	<b>5</b>
2.1 Il regime di responsabilità previsto a carico delle persone giuridiche .....	5
2.2 Autori del reato: soggetti in posizione apicale e soggetti sottoposti all'altrui direzione .....	6
2.3 Reati transnazionali .....	8
2.4 Sistema Sanzionatorio .....	8
2.5 Modelli 231: esimenza, contenuti ed efficace attuazione .....	9
2.6 Codici di comportamento predisposti dalle associazioni rappresentative di categoria (ACRI) .....	10
<b>3 MISSION DI FONDAZIONE CARIGE E ASSETTO ORGANIZZATIVO DELLA SOCIETÀ</b> .....	<b>10</b>
3.1 Premessa: inquadramento delle fondazioni di origine bancaria .....	10
3.2 Mission e Core Business di Fondazione Carige .....	11
3.3 Norme di Governance e Struttura Organizzativa delle FOB.....	11
3.3.1 Norme di Governance e Struttura Organizzativa di Fondazione Carige .....	12
3.3.2 Il Sistema dei Controlli Interni .....	15
3.4 Stakeholders di Fondazione Carige .....	16
<b>4 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI FONDAZIONE CARIGE</b> ....	<b>16</b>
4.1 Destinatari .....	16
4.2 Struttura del Modello e documentazione .....	17
4.2.1 Ulteriori Procedure e Protocolli rilevanti.....	17
4.2.2 Il Sistema di Compliance Integrato .....	18
4.2.3 Il GDPR e il DPO.....	19
4.2.4 Fondazione Carige e gli Obblighi di Trasparenza .....	21
4.2.5 Ulteriori norme di riferimento: Provvedimento Banca d'Italia del 23 luglio 2024 .....	22
<b>5. IL PROCESSO DI REALIZZAZIONE DEL MODELLO</b> .....	<b>24</b>
5.1 Le Soglie Dimensionali di Fondazione Carige.....	24
5.2 la Attività' di Risk Assessment e le Attività Aziendali "Sensibili" .....	24
<b>6 L'ORGANISMO DI VIGILANZA</b> .....	<b>31</b>
6.2 L'organismo di vigilanza di Fondazione Carige.....	31
6.3 Funzioni e poteri dell'Organismo di Vigilanza .....	34
6.4 Obblighi di informazione nei confronti dell'Organismo di Vigilanza – Flussi informativi .....	35
6.5 Reporting dell'Organismo di Vigilanza verso gli organi societari .....	37
<b>7 WHISTLEBLOWING</b> .....	<b>37</b>
7.2 La procedura di "Gestione delle segnalazioni all'Organismo di Vigilanza di violazioni sospette del Modello Organizzativo 231" (whistleblowing).....	40
7.3 Ambito di applicazione della procedura di whistleblowing e canali per le segnalazioni .....	41
7.3.1 Il Canale di Segnalazione Interno: la Piattaforma Whistleblowing .....	42
<b>8 SISTEMA DISCIPLINARE E SANZIONATORIO</b> .....	<b>42</b>
8.2 Funzione del sistema disciplinare .....	42
8.3 Misure nei confronti di lavoratori subordinati non dirigenti.....	42
8.4 Misure nei confronti dei dirigenti.....	44
8.5 Misure nei confronti degli Amministratori e del Collegio Sindacale.....	45
8.6 Misure nei confronti di partner commerciali, consulenti e collaboratori esterni .....	45
8.7 Sanzioni applicabili ai destinatari delle segnalazioni ("Whistleblowing") .....	45
<b>9 FORMAZIONE E COMUNICAZIONE</b> .....	<b>46</b>
9.2 Premessa .....	46
9.3 Dipendenti .....	46
9.4 Partner commerciali, consulenti e collaboratori esterni .....	47
<b>10 AGGIORNAMENTO DEL MODELLO</b> .....	<b>47</b>
<b>11 MATRICE DI RESPONSABILITÀ</b> .....	<b>48</b>

### **Allegati di Parte Speciale**

PARTE SPECIALE 01	REATI CONTRO LA PUBBLICA AMMINISTRAZIONE (ART.24 D.LGS 231/01)
PARTE SPECIALE 02	DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (ART.24bis D.LGS 231/01)
PARTE SPECIALE 03	REATI CONTRO LA PUBBLICA AMMINISTRAZIONE (ART.25 D.LGS 231/01)
PARTE SPECIALE 04	REATI SOCIETARI (ART.25ter D.LGS 231/01)
PARTE SPECIALE 05	REATI COMMESSI IN VIOLAZIONE DEGLI ADEMPIMENTI IN MATERIA DI TUTELA DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO (ART.25 septies)
PARTE SPECIALE 06	REATI DI RICETTAZIONE, RICICLAGGIO ED IMPIEGO DI UTILITÀ ILLECITE, AUTORICICLAGGIO (ART.25 octies)
PARTE SPECIALE 07	INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART.25 decies)
PARTE SPECIALE 08	REATI TRIBUTARI (ART.25 quinquiesdecies)
PARTE SPECIALE 09	DELITTI CONTRO IL PATRIMONIO CULTURALE RICICLAGGIO DI BENI CULTURALI E DEVASTAZIONE E SACCHEGGIO DI BENI CULTURALI E PAESAGGISTICI (ART.25 septiesdecies e duodevicies)

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

**PARTE GENERALE**

## 1 PREMESSA. FINALITÀ DI EMISSIONE DELLA NUOVA RELEASE DEL MOG

Il presente documento illustra il Modello di Organizzazione, gestione e controllo (di seguito il "**Modello**" o "**MOG 231**") adottato da Fondazione Carige ai sensi del Decreto Legislativo 8 giugno 2001 n. 231 (di seguito "**Decreto**") e successive modifiche. Con il presente Modello la Fondazione ha inteso confermare i principi di corretta gestione così come affermati dal Decreto.

Si ricorda come la Fondazione abbia adottato il Modello ex D.Lgs 231/01 sin dal 2014, provvedendo nel corso degli anni alla sua implementazione ed al relativo aggiornamento a seguito:

- (i) di modifiche dell'assetto organizzativo (sotto il profilo dell'Organigramma Aziendale) dell'Ente e
- (ii) degli interventi del Legislatore, il quale man mano ha ampliato il *numerus clausus* delle fattispecie di reato rilevanti. Sotto detto ultimo profilo le competenti funzioni aziendali hanno preso in esame i reati presupposto di nuova introduzione, valutandone via via la configurabilità in astratto e -in ipotesi di esito positivo- introducendo nuove misure di prevenzione. Ad oggi, in conseguenza della stratificazione degli interventi, si è ritenuto opportuno procedere alla ri-emissione di una versione aggiornata del MOG edizione rev.2 del 12.10.2020, il quale compendiasse gli interventi posti in essere.

## 2 IL QUADRO NORMATIVO DI RIFERIMENTO

### 2.1 Il regime di responsabilità previsto a carico delle persone giuridiche

Con il decreto legislativo 8 giugno 2001 n. 231, emanato in attuazione della delega conferita al Governo con l'art. 11 della Legge 29 settembre 2000, n. 300 è stata dettata la disciplina della "*responsabilità degli enti per gli illeciti amministrativi dipendenti da reato*".

Tale disciplina si applica agli enti dotati di personalità giuridica, nonché alle società e associazioni anche prive di personalità giuridica. Nel presente documento si utilizzerà indifferentemente l'espressione "**ente**" o "**società**" per indicare il soggetto giuridico destinatario delle norme di cui al Decreto.

Il D.Lgs. 231/01 trova la sua genesi in alcune convenzioni internazionali e comunitarie ratificate dall'Italia, le quali impongono di prevedere forme di responsabilità degli enti collettivi per talune specifiche fattispecie di reato.

Secondo la disciplina introdotta dal Decreto la società può essere ritenuta "responsabile" per alcuni reati commessi o tentati, nell'interesse o a vantaggio della società stessa.

Per quanto attiene alla nozione di "**interesse**", esso si concretizza ogniqualvolta la condotta illecita sia posta in essere con l'esclusivo intento di fare conseguire un beneficio alla Società, indipendentemente dalla circostanza che tale obiettivo sia stato conseguito.

Del pari la responsabilità incombe sulla Società ogniqualvolta l'autore dell'illecito, pur non avendo agito al fine di beneficiare l'Ente, abbia comunque fatto conseguire un "**vantaggio**" alla persona giuridica, di tipo economico o meno.

Per la sua indubbia rilevanza occorre dare conto di una interpretazione estensiva, operata dalla Giurisprudenza, dei presupposti sopra riportati. A titolo meramente esemplificativo e per facilità di comprensione il vantaggio è stato configurato il vantaggio in ipotesi di risparmio di costi per la sicurezza ovvero nel potenziamento della velocità di esecuzione delle prestazioni o nell'incremento della produttività, sacrificando l'adozione di presidi antinfortunistici (cfr. Cass., sez. IV, n. 3157/2019 e n. 3731/2020). Detta interpretazione estensiva, che sino ad oggi ha trovato applicazione in particolare in ambito SSL e retai ambientali, deve guidare l'interprete nella

valutazione della configurabilità -sotto detto profilo- delle altre fattispecie di reato, potendo i presupposti ricorrere altresì in tale ambito (a titolo esemplificativo ricorrenza di delitti informatici per risparmio sui costi di implementazione di hardware, software e presidi, etc.).

È opportuno evidenziare come la società non risponda, per espressa previsione legislativa (art. 5, comma 2, del D.Lgs. 231/2001), se le persone su indicate hanno agito nell'interesse esclusivo proprio o di terzi. La responsabilità amministrativa delle società è autonoma rispetto alla responsabilità penale della persona fisica che ha commesso il reato e si affianca a quest'ultima.

Il D.Lgs. 231/01 ha, in definitiva, innovato l'ordinamento giuridico italiano in quanto alle società sono ora applicabili, in via diretta ed autonoma, sanzioni di natura sia pecuniaria che interdittiva in relazione a reati ascritti a soggetti funzionalmente legati alla società ai sensi dell'art. 5 del decreto.

## **2.2 Autori del reato: soggetti in posizione apicale e soggetti sottoposti all'altrui direzione**

La società è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- da "persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dell'ente stesso" (cd. soggetti "in posizione apicale" o "apicali"; art. 5, comma 1, lett. a), del D.Lgs. 231/2001);
- da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali (i c.d. soggetti sottoposti all'altrui direzione: art. 5, comma 1, lett. b), del D.Lgs. 231/2001).

Non tutti i reati commessi dai soggetti sopra indicati implicano una responsabilità amministrativa riconducibile alla società, atteso che sono individuate come rilevanti solo specifiche tipologie di reati (*numerus clausus* dei reati presupposti). Le fattispecie di reato oggi suscettibili di configurare la responsabilità amministrativa della società, se commessi nel suo interesse o a suo vantaggio dai soggetti sopra menzionati, sono espressamente richiamate dagli artt. 24, 24-bis, 24-ter, 25, 25-bis, 25-bis.1, 25-ter, 25-quater, 25-quater.1, 25-quinquies, 25-sexies e 25-septies, 25-octies, 25-octies.1, 25-novies, 25-decies, 25-undecies, 25-duodecies, 25-terdecies, 25-quaterdecies, 25-quinquiesdecies e 25-sexiesdecies, 25-septesdecies, 25-duodevices del D.Lgs. 231/01, nonché dalla L. 146/2006 e dall'art. 12, L. n. 9/2013.

Tali fattispecie di reato possono essere comprese nelle seguenti categorie, come di seguito rappresentate (aggiornamento alla data del febbraio 2024).

- **Reati commessi nei rapporti con la Pubblica Amministrazione e delitti contro il patrimonio mediante frode in danno dello Stato o di un altro ente pubblico o dell'Unione europea** (artt. 24 e 25 del Decreto, come da ultimo modificati con il Decreto Legislativo 14 luglio 2020, n. 75, con il Decreto Legge 25 febbraio 2022, n. 13, con il Decreto Legislativo 4 ottobre 2022, n. 156, e infine con il Decreto Legislativo 10 ottobre 2022, n. 150).
- **Reati di falsità in monete, in carte di pubblico credito e in valori di bollo** (art.25-bis del Decreto, introdotto dal decreto legge del 25 settembre 2001, n. 350, in seguito modificato dal d.lgs. 21 giugno 2016, n. 125).
- **Reati societari** (art. 25-ter del Decreto, introdotto dal d.lgs. 11 aprile 2002 n. 61, in seguito modificato con Legge 6 novembre 2012, n. 190 e con Legge 27 maggio 2015, n. 69, e da ultimo con il Decreto Legislativo 15 marzo 2017, n. 38 e con il Decreto Legislativo 2 marzo 2023, n. 19).
- **Delitti con finalità di terrorismo o di eversione dell'ordine democratico** previsti dal codice penale e dalle leggi speciali e delitti posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione Internazionale per la repressione del finanziamento del terrorismo di New York del 9 dicembre 1999 (art. 25-quater del Decreto, introdotto dalla legge n. 7 del 14 gennaio 2003).
- **Pratiche di mutilazione degli organi genitali femminili** (art. 25-quater.1 del Decreto,

introdotto dalla legge n. 7 del 9 gennaio 2006).

- **Delitti contro la personalità individuale** (art. 25-quinquies del Decreto, introdotto dalla legge n. 228 del 11 agosto 2003, e da ultimo modificato con la Legge 29 ottobre 2016, n. 199).
- **Abusi di mercato** (art. 25-sexies del Decreto, introdotto dalla legge n. 62 del 18 aprile 2005 e in seguito modificato dal Decreto Legislativo 10 agosto 2018, n. 107 e dalla Legge 23 dicembre 2021, n. 238).
- **Reati transnazionali** (art. 10 legge n. 146 del 16 marzo 2006).
- **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. 25-septies del Decreto, introdotto con legge del 3 agosto 2007, n. 127).
- **Ricettazione, riciclaggio** e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies del Decreto, introdotto con il decreto legislativo del 21 novembre 2007, n. 231, in seguito modificato con Legge del 15 dicembre 2014, n. 186, e successivamente con il decreto legislativo 8 novembre 2021, n. 195)
- **Delitti informatici e trattamento illecito di dati** (art. 24-bis del Decreto, introdotto con la legge 18 marzo 2008, n. 48, in seguito modificato dai decreti legislativi 15 gennaio 2016, n. 7 e n. 8, e dalla Legge 23 dicembre 2021, n. 238).
- **Delitti di criminalità organizzata** (art. 24-ter del Decreto, introdotto con la legge 15 luglio 2009, n. 94).
- **Delitti contro l'industria e il commercio** (art. 25-bis.1 del Decreto, introdotto con la legge 23 luglio 2009, n. 99).
- **Delitti in materia di violazione del diritto d'autore** (art. 25-novies del Decreto, introdotto con la legge del 23 luglio 2009, n. 99).
- **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** (art. 25-decies del Decreto, introdotto con Legge 3 agosto 2009, n. 116).
- **Reati ambientali** (art. 25-undecies del Decreto, introdotto con il d.lgs. del 7 luglio 2011, n. 121, in seguito modificato con Legge 22 maggio 2015, n. 68, e da ultimo con il d.lgs. 1 marzo 2018, n. 21).
- **Impiego di cittadini di paesi terzi il cui soggiorno è irregolare** (art. 25 duodecies del Decreto, introdotto con il d.lgs. 16 luglio 2012, n. 109, in seguito modificato con il Decreto 7 maggio 2022 del Ministero dell'Interno e con il Decreto Legge 10 marzo 2023, n. 20).
- **Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio** (art. 25 del Decreto, modificato dalla Legge 6 novembre 2012, n. 190 e dal Decreto Legislativo 4 ottobre 2022, n. 156).
- **Corruzione tra privati** e Istigazione alla corruzione tra privati (art. 25-ter lett. s-bis del Decreto, introdotto con Legge n. 190/2012, e da ultimo modificato con il d.lgs. 15 marzo 2017, n. 38).
- **Delitto di «false o omesse dichiarazioni per il rilascio del certificato preliminare»** (art. 25-ter, comma 1, lett. s-ter del Decreto introdotto con il Decreto Legislativo 2 marzo 2023, n. 19).
- **Reati contemplati dalle “Disposizioni contro le immigrazioni clandestine”** (art. 25-duodecies del Decreto, come modificato dalla Legge 17 ottobre 2017, n. 161).
- **Reati in materia di razzismo e xenofobia** (art. 25-terdecies del Decreto, come modificato con d.lgs. 1 marzo 2018, n. 21).
- **Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati** (art. 25- quaterdecies del Decreto introdotto con la Legge 3 maggio 2019, n. 39). Traffico di influenze illecite (art. 25 del Decreto, come modificato dalla Legge 9 gennaio 2019, n. 3).
- **Reati tributari** (art. 25-quinquiesdecies del Decreto, introdotto dal Decreto Legge 26 ottobre 2019, n. 124, convertito, con modificazioni, dalla Legge 19 dicembre 2019 n. 157, e in seguito modificato dal Decreto Legislativo 14 luglio 2020, n. 75, e dal Decreto Legislativo 4 ottobre 2022, n. 156).

- **Reati di contrabbando** (art. 25-sexiesdecies del Decreto, introdotto dal Decreto Legislativo 14 luglio 2020, n. 75, e in seguito modificato dal Decreto Legislativo 4 ottobre 2022, n. 156).
- **Delitti in materia di strumenti di pagamento diversi dai contanti** (art. 25- octies.1 del Decreto, introdotto con il Decreto Legislativo 8 novembre 2021, n. 184).
- **Delitti contro il patrimonio culturale** (art. 25-septiesdecies del Decreto, introdotto con la Legge 9 marzo 2022, n. 22).
- **Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici** (art. 25-duodevicies del Decreto, introdotto con la Legge 9 marzo 2022, n. 22).

### 2.3 Reati transnazionali

In forza del disposto di cui all'art. 4 del D. Lgs. 231/2001, l'ente può essere chiamato a rispondere in Italia, in relazione a reati contemplati dallo stesso Decreto, ove commessi all'estero.

I presupposti su cui si fonda la responsabilità dell'ente per reati commessi all'estero sono i seguenti:

- il reato deve essere commesso all'estero da un soggetto funzionalmente legato all'ente, ai sensi dell'art. 5, comma 1, del D.Lgs. 231/2001;
- l'ente deve avere la propria sede principale nel territorio dello Stato italiano;
- l'ente può rispondere solo nei casi e alle condizioni previste dagli artt. 7 c.p. "Reati commessi all'estero", 8 c.p. "Delitto politico commesso all'estero", art. 9 c.p. "Delitto comune del cittadino all'estero" e art. 10 c.p. "Delitto comune dello straniero all'estero" (nei casi in cui la legge prevede che il colpevole - persona fisica - sia punito a richiesta del Ministro della Giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti dell'ente stesso);
- lo Stato del luogo in cui è stato commesso il reato non procede nei confronti dell'ente.

Il rinvio agli artt. 7-10 c.p. è da coordinare con le previsioni degli articoli da 24 a 25-octies del D.Lgs. 231/2001, sicché - anche in ossequio al principio di legalità di cui all'art. 2 del D.Lgs. 231/2001 - a fronte della serie di reati menzionati dagli artt. 7-10 c.p., l'Ente potrà rispondere soltanto di quelli per i quali la sua responsabilità sia prevista da una disposizione legislativa *ad hoc*.

### 2.4 Sistema Sanzionatorio

Sono previste le seguenti sanzioni a carico della società qualora se ne ravveda la responsabilità ai sensi del Decreto, in conseguenza della commissione o tentata commissione dei reati sopra menzionati:

- **sanzione pecuniaria**, calcolata tramite un sistema basato su quote, che vengono determinate dal giudice nel numero e nell'ammontare, entro limiti definiti per legge. La sanzione può quindi variare da un minimo di € 25.822,84 a un massimo € 1.549.370,70 (aumentabile fino a 10 volte nel caso di abusi di mercato);
- **sanzioni interdittive** (applicabili anche in via cautelare) di durata non inferiore a tre mesi e non superiore a due anni (con la precisazione che, ai sensi dell'art. 14, comma 1, D.Lgs. 231/01, "Le sanzioni interdittive hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'ente") che, a loro volta, possono consistere in:
  - interdizione dall'esercizio dell'attività;
  - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
  - divieto di contrattare con la Pubblica Amministrazione;

- esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi;
- divieto di pubblicizzare beni o servizi;
- confisca (e sequestro preventivo in sede cautelare);
- pubblicazione della sentenza (in caso di applicazione di una sanzione interdittiva).

## 2.5 Modelli 231: esimenza, contenuti ed efficace attuazione

Aspetto caratteristico del D.Lgs. 231/01 è l'attribuzione di un **valore esimente** ai modelli di organizzazione, gestione e controllo eventualmente adottati della società.

Ai fini dell'accertamento della responsabilità amministrativa occorrerà che il reato si sia configurato per una colpa di organizzazione in quanto ciò che si rimprovera all'ente è il fatto di non aver adottato misure idonee a prevenire il rischio di commissione del reato.

Il criterio di imputazione si differenzia qualora il reato sia stato commesso da soggetti apicali piuttosto che dai sottoposti. L'art. 6 del decreto stabilisce infatti che, in caso di commissione di uno dei reati contemplati dal decreto da parte dei vertici, l'ente non è chiamato a rispondere se dimostra che:

- la Società ha **adottato ed efficacemente attuato** prima della commissione del fatto illecito modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione degli illeciti penali considerati;
- il **compito di vigilare** sul funzionamento e l'osservanza del modello e di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo (Organismo di Vigilanza);
- le persone hanno **commesso il reato eludendo fraudolentemente i modelli** di organizzazione e di gestione;
- **non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo.**

Qualora il reato venga commesso dai soggetti subordinati, l'art. 7 prevede che *"L'ente sarà responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza"* mentre *"è esclusa l'inosservanza degli obblighi di direzione e vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi"*. L'onere probatorio a carico del soggetto collettivo è in tal caso più lieve.

Il D.Lgs. 231/01 delinea il **contenuto dei modelli di organizzazione e di gestione** prevedendo che gli stessi, in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, debbano:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli (o procedure) diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli tramite una idonea procedura di flussi informativi;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

L'art. 7, comma 4, del D.Lgs. 231/01 definisce, inoltre, **i requisiti dell'efficace attuazione** dei modelli organizzativi richiedendo:

- la verifica periodica e l'eventuale modifica del modello qualora siano scoperte significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione e nell'attività;
- l'esistenza di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

La semplice adozione del Modello non è quindi misura sufficiente a determinare l'esonero da responsabilità dell'ente, essendo piuttosto necessario che il Modello sia anche efficace ed effettivo.

## **2.6 Codici di comportamento predisposti dalle associazioni rappresentative di categoria (ACRI)**

L'art. 6, comma 3, del D.Lgs. 231/01 prevede che "(...) i modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui al comma 2, sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati".

L'associazione di categoria a cui la Fondazione aderisce è l'ACRI (Associazione delle Casse di Risparmio Italiane e delle Fondazioni Bancarie). Essa non ha provveduto a elaborare vere e proprie linee guida o codici di comportamento da sottoporre al vaglio e all'approvazione da parte del Ministero della Giustizia e, pertanto, utilizzabili da parte degli enti associati ai sensi del citato comma 3 dell'articolo 6 del Decreto 231, pur avendo prodotto un documento di indirizzo intitolato "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle Fondazioni e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della Legge 29 settembre 2000, n. 300 - decreto legislativo 8 giugno 2001, n. 231 e successive modificazioni e integrazioni*", rilasciato nel maggio 2003. Successivamente, nel marzo 2008, l'ACRI ha diramato alle associate un ulteriore studio in materia, frutto dell'attività di un gruppo di lavoro cui ha collaborato anche KPMG Advisory, società con ampia esperienza nel campo della 231 e conoscitrice della realtà delle fondazioni, intitolato "*Analisi delle tematiche e riflessi operativi per le Fondazioni*". Ai sensi dei citati Documenti ACRI e di quanto previsto in altre linee guida di categoria, dalla dottrina e dalla prassi e dalla metodologia sviluppata nell'esperienza di altri progetti di adeguamento, è possibile affermare come, in base alle *best practice*, le tappe fondamentali nella costruzione di un modello organizzativo siano le medesime sopra delineate.

Il presente Modello è stato redatto tenendo in ogni caso conto delle indicazioni espresse dalle linee guida elaborate da Confindustria, approvate dal Ministero della Giustizia, e da ultimo rimesse nel corso del mese di giugno 2021.

## **3 MISSION DI FONDAZIONE CARIGE E ASSETTO ORGANIZZATIVO GENERALE DELLA SOCIETÀ**

### **3.1 Premessa: inquadramento delle fondazioni di origine bancaria**

Le fondazioni di origine bancaria ("**FOB**"), da un punto di vista giuridico, sono definite come una stabile organizzazione predisposta per la destinazione di un patrimonio privato ad un determinato scopo di natura ideale.

Le FOB dispongono di mezzi patrimoniali vincolati al perseguimento esclusivo di scopi di utilità sociale e di promozione dello sviluppo economico, secondo quanto previsto dalla normativa di riferimento e dai rispettivi statuti. In particolare, lo scopo di tali enti è riconducibile al soddisfacimento, senza finalità lucrative, dei bisogni di determinate categorie di soggetti, diversi da quelli di provenienza delle disponibilità finanziarie.

Da un punto di vista economico aziendale le FOB possono, quindi, essere configurate come insiemi di operazioni economiche coordinate finalizzate alla ricerca, dati i mezzi a disposizione, della miglior soddisfazione dei bisogni della collettività territoriale alla quale fanno riferimento.

Le FOB sono pertanto deputate alla gestione del patrimonio a propria disposizione e, dall'altra, alla gestione dell'attività di erogazione alla collettività di riferimento.

La normativa di riferimento delle FOB, richiede che la gestione del patrimonio:

a) sia condotta nel rispetto dei criteri prudenziali di rischio in modo da conservarne il valore ed ottenerne una redditività adeguata;

b) sia svolta con modalità organizzative idonee ad assicurarne la separazione dalle altre attività.

In ultima analisi il soggetto economico della FOB deve essere in grado di assicurare il collegamento funzionale tra la gestione del patrimonio, improntata alla diversificazione del rischio di investimento al fine di ottenerne un'adeguata redditività, e le finalità istituzionali che fanno riferimento all'azienda di erogazione. Dunque, le politiche di gestione del patrimonio devono essere finalizzate alla massimizzazione dell'utile di esercizio, tenendo conto della diversificazione del rischio di investimento, al fine di consentire all'azienda di erogazione di soddisfare i bisogni presenti e futuri della collettività di riferimento

### **3.2 Mission e Core Business di Fondazione Carige**

Coerentemente con quanto esposto al §3.1 la Fondazione Cassa di Risparmio di Genova e Imperia è un ente non profit privato e autonomo, che continua l'attività di carattere sociale e filantropico esercitata, per oltre cinque secoli, inizialmente dal Monte di Pietà e poi dalla Cassa di Risparmio.

La Fondazione persegue esclusivamente fini di utilità sociale e di promozione dello sviluppo economico. In particolare, la Fondazione interviene direttamente e indirettamente, nei settori dello Sviluppo locale, della Ricerca scientifica e tecnologica, della Salute pubblica, medicina preventiva e riabilitativa, dell'Educazione, istruzione e formazione, dell'Arte, attività e beni culturali, del Volontariato, filantropia e beneficenza.

La Fondazione opera in base alle finalità indicate nel Documento programmatico previsionale annuale sia con propri Programmi Pluriennali di Attività e con Progetti Promossi sia come soggetto erogatore di contributi per iniziative condivise e sostenute solo finanziariamente sia, inoltre, come soggetto catalizzatore di forze sociali miranti al miglioramento della comunità di riferimento.

Nell'amministrare il patrimonio totalmente vincolato al perseguimento degli scopi statutari, la Fondazione deve attenersi a criteri prudenziali in modo da conservare il valore e ottenerne un'adeguata redditività, oltre che in modo coerente con la sua natura di ente senza scopo di lucro che opera secondo i principi di trasparenza e moralità.

### **3.3 Norme di Governance e Struttura Organizzativa delle FOB**

Nell'ambito della corporate governance delle FOB si possono sostanzialmente individuare i seguenti organi statutari, nelle singole fondazioni, variamente denominati:

- a) il Presidente della fondazione bancaria;
- b) il Consiglio generale, quale organo di indirizzo (in Fondazione Carige "**Consiglio di Indirizzo**");
- c) il Consiglio di amministrazione, quale organo amministrativo;
- d) il Collegio Sindacale, quale organo di controllo.

Come già detto precedentemente l'attività di programmazione riveste un ruolo centrale e in questo senso il soggetto economico unico, rappresentato dal Consiglio Generale, deve essere in grado, attraverso il cd. Documento di previsione e programmatico, di definire:

- i programmi, le priorità e gli obiettivi della fondazione;
- le linee generali della gestione patrimoniale e la politica degli investimenti.

Il Consiglio di Indirizzo è il propulsore del ciclo di creazione della ricchezza in quanto, conoscendo i bisogni della collettività di riferimento e quindi il fabbisogno finanziario in capo all'azienda di erogazione, è in grado di definire la gestione del patrimonio.

Una volta definiti i programmi dei due cicli gestionali della FOB spetta al Consiglio di Amministrazione la gestione del patrimonio della FOB, attraverso strutture organizzative dedicate,

al fine di massimizzarne il rendimento nel rispetto dei vincoli individuati dalla norma e dalle scelte programmatiche effettuate dal Consiglio d Indirizzo.

La normativa di riferimento richiede una serie di restrizioni nell'ambito dell'organizzazione delle FOB

e in particolare:

- a) un'organizzazione distinta e specifica per la gestione del patrimonio;
- b) la separazione dei ruoli organizzativi tra indirizzo, amministrazione e controllo;
- c) l'individuazione delle modalità e i criteri che presiedono allo svolgimento dell'attività erogativa.

### **3.3.1 Norme di Governance e Struttura Organizzativa di Fondazione Carige**

In ossequio alla disciplina regolatrice delle FOB ai sensi del vigente Statuto, approvato dal Ministero dell'Economia e della Finanza nel 2015, sono organi della Fondazione:

- a) il Presidente;
- b) il Consiglio di indirizzo;
- e) il Consiglio di amministrazione;
- d) il Collegio sindacale;
- e) il Segretario generale.

Gli Organi statuari cooperano tra loro in un rapporto di leale e reciproca collaborazione, al fine di perseguire in maniera ottimale le finalità statuarie, nel rispetto dei relativi ruoli, competenze e responsabilità, senza ingerenze o sovrapposizioni di attribuzioni. Il Collegio sindacale vigila affinché non si creino confusioni di ruoli e responsabilità.

Il **Presidente della Fondazione** è nominato dal Consiglio di indirizzo. Egli promuove le attività della Fondazione, sovrintende all'esecuzione delle deliberazioni del Consiglio di amministrazione e del Consiglio di indirizzo e al funzionamento generale della struttura organizzativa della Fondazione. Il Presidente ha la rappresentanza legale della Fondazione di fronte ai terzi.

Il **Consiglio di indirizzo**, formato da 13 componenti, ha la esclusiva competenza per quanto attiene le decisioni concernenti:

- a) l'approvazione dello Statuto e delle relative modifiche;
- b) lo scioglimento della Fondazione, secondo quanto previsto all'art. 31 del presente Statuto;
- c) l'approvazione e la modificazione dei regolamenti interni, salvo dove diversamente disposto;
- d) la nomina dei componenti del Consiglio di amministrazione, nel rispetto di quanto previsto dal D.Lgs. 153/1999, art. 4, comma 1, lett f., e la revoca degli stessi per giusta causa, nonché la determinazione dei relativi compensi e il valore della medaglia di presenza;
- e) la dichiarazione di decadenza e sospensione dei componenti del Consiglio di amministrazione nei casi previsti dallo Statuto, ove il Consiglio di amministrazione non vi provveda tempestivamente;
- f) l'esercizio dell'azione di responsabilità nei confronti dei componenti degli Organi di amministrazione e di controllo;
- g) la nomina e la revoca, per giusta causa, dei componenti del Collegio sindacale, la determinazione dei relativi compensi e il valore della medaglia di presenza, la

dichiarazione di decadenza e di sospensione degli stessi nei casi previsti dal presente Statuto;

- h) la nomina di eventuali commissioni consultive o di studio, temporanee o permanenti all'interno del Consiglio di indirizzo, determinandone le funzioni e la composizione;
- i) l'approvazione del bilancio d'esercizio e della relazione sulla gestione, nonché la destinazione dell'avanzo di gestione;
- j) la determinazione, sentito il Consiglio di amministrazione, di programmi pluriennali di attività con riferimento ai bisogni del territorio, individuando i settori, tra quelli previsti dallo Statuto, ai quali destinare le risorse tempo per tempo disponibili definendo in linea di massima gli obiettivi, le linee di operatività e le priorità degli interventi; il Consiglio di indirizzo provvede altresì a monitorare l'attuazione dei programmi pluriennali e dell'attività erogativa disposta dal Consiglio di amministrazione;
- k) la definizione, su proposta del Consiglio di amministrazione, dei settori rilevanti in cui la Fondazione opererà nell'ambito della programmazione pluriennale;
- l) l'approvazione del documento programmatico previsionale annuale recante gli obiettivi, gli ambiti progettuali e gli strumenti di intervento della Fondazione, predisposto dal Consiglio di amministrazione;
- m) la definizione delle linee generali della gestione patrimoniale e della politica degli investimenti;
- n) la costituzione di società strumentali, nonché l'acquisto o la dismissione di partecipazioni in enti o società che abbiano per oggetto esclusivo l'esercizio di imprese strumentali;
- o) l'approvazione delle operazioni di trasformazione, fusione e liquidazione della Fondazione;
- p) la nomina e la revoca del Presidente della Fondazione;
- q) la nomina dei membri del Consiglio di indirizzo nei casi previsti dallo Statuto;
- r) la deliberazione dei compensi e delle medaglie di presenza da corrispondere ai componenti il Consiglio di indirizzo e al Presidente della Fondazione, sentito il Collegio sindacale;
- s) l'affidamento dell'incarico di revisione contabile ad apposita società di revisione e/o allo stesso Collegio sindacale;
- t) la dichiarazione di sospensione o decadenza dei componenti del Consiglio di indirizzo.

Al Consiglio di indirizzo spetta vigilare sull'operato del Consiglio di amministrazione, sulle attività istituzionali della Fondazione, nonché sui risultati dell'attività di investimento, allo scopo di garantire il rispetto dello Statuto, dei regolamenti e degli indirizzi definiti.

Il **Consiglio di amministrazione** è composto da 5 (cinque) Consiglieri, compreso il Presidente che ne fa parte di diritto. Il Presidente della Fondazione ha diritto di voto in seno al Consiglio di amministrazione. Il Consiglio di amministrazione è l'organo responsabile della gestione della Fondazione.

La gestione della Fondazione da parte del Consiglio di amministrazione è basata sulle linee strategiche e sugli obiettivi contenuti nei documenti di programmazione deliberati dal Consiglio di indirizzo.

Competono al Consiglio di amministrazione tutti i poteri di ordinaria e straordinaria amministrazione della Fondazione esclusi quelli espressamente riservati dalla Legge o dallo Statuto ad altri organi della Fondazione.

Il Consiglio provvede, in particolare, a:

- a) verificare la sussistenza in capo ai propri membri dei requisiti di appartenenza all'organo;
- b) dichiarare o sospendere i propri componenti, con l'eccezione del Presidente della Fondazione;

- c) definire i programmi operativi delle attività istituzionali, nell'ambito di quanto stabilito nel documento pluriennale e dei relativi aggiornamenti annuali, nonché esercitare attività di proposta e di impulso ai fini delle decisioni del Consiglio di indirizzo;
- d) nominare, revocare, determinare il compenso, dichiarare la decadenza o la sospensione del Segretario generale;
- e) predisporre il progetto di bilancio di esercizio e la relazione sulla gestione;
- f) predisporre il documento programmatico previsionale annuale;
- g) effettuare la gestione esecutiva delle deliberazioni dell'organo di indirizzo in ordine ai programmi erogativi, ai progetti esecutivi ed a quant'altro inerente l'attività della Fondazione;
- h) definire, su proposta del Segretario generale, il Regolamento interno degli uffici e le norme relative all'organico e al trattamento del personale;
- i) assumere il personale dipendente e gestire tutti gli aspetti del rapporto di lavoro;
- j) promuovere azioni dinanzi agli organi giurisdizionali e resistere nelle stesse, nonché deliberare su con- seguenti arbitrati e transazioni;
- k) formulare proposte al Consiglio di indirizzo in ordine:
  - 1) alle modifiche statutarie
  - 2) all'approvazione e alle modifiche dei regolamenti interni
  - 3) ai programmi di intervento della Fondazione
  - 4) alla definizione delle linee generali della gestione patrimoniale;
  - 5) alla costituzione di società strumentali
  - 6) alla periodica individuazione dei settori rilevanti;
- l) designare e nominare amministratori e sindaci in società ed enti cui la Fondazione è chiamata a provvedere;
- m) con specifico riferimento alla gestione del patrimonio, così come stabilita da specifico Regolamento, spettano al Consiglio di amministrazione:
  - 1) la scelta circa la concreta allocazione del patrimonio nelle diverse tipologie di investimento, nel rispetto delle linee strategiche individuate dall'Organo di indirizzo;
  - 2) l'amministrazione degli investimenti strategici e il relativo esercizio dei diritti economici e amministrativi;
  - 3) l'individuazione, secondo i criteri definiti dall'Organo di indirizzo, degli intermediari abilitati cui affidare la gestione del patrimonio ove ritenuto opportuno;
  - 4) la verifica periodica, in caso di gestione affidata a gestori abilitati, del rispetto delle politiche di investimento e delle regole di bilanciamento dei rischi definite dalla Fondazione;
  - 5) l'assunzione delle decisioni in termini di ribilanciamento strategico dei rischi e delle durate;
  - 6) la valutazione periodica dei gestori.

Il Consiglio di amministrazione può delegare ad uno o più dei suoi componenti o al Segretario generale specifici poteri, determinando i limiti della delega. I titolari di deleghe devono relazionare il Consiglio di amministrazione secondo modalità da questo fissate in merito all'assolvimento del mandato ricevuto.

Il Consiglio di amministrazione può partecipare alle riunioni del Consiglio di indirizzo, senza diritto di voto, al fine di prestare la necessaria collaborazione soprattutto nella definizione dei programmi di attività.

Il **Collegio sindacale**: è l'organo di controllo della Fondazione, composto da tre membri, esercita le funzioni previste dall'articolo 2403, primo comma, del Codice Civile, vigilando sull'osservanza

della legge e dello Statuto, sulla legittimità delle attività e degli atti della Fondazione, sul rispetto dei principi di corretta amministrazione, sull'adeguatezza dell'assetto organizzativo e del sistema amministrativo e contabile della Fondazione e sul loro funzionamento.

Il **Segretario generale** è a capo degli uffici e del personale della Fondazione, dei quali si avvale per lo svolgimento delle sue funzioni.

Ulteriori organi non contemplati in Statuto, ma deputati al controllo del buon andamento della Fondazione e delle aree di rispettiva competenza sono:

- l'Organismo di Vigilanza, per il quale si rimanda al capitolo 4 del presente documento;
- il DPO (Data Protection Officer - in italiano RPD, Responsabile della Protezione dei Dati), figura individuata dalla Fondazione in professionista esterno e che ha la funzione di affiancare titolare, addetti e responsabili del trattamento affinché conservino i dati e gestiscano i rischi seguendo i principi e le indicazioni del Regolamento europeo.

### **3.3.2 Il Sistema dei Controlli Interni**

La Fondazione, in coerenza con le best practice nazionali ed internazionali, ha adottato un sistema di controllo interno e di gestione dei rischi al fine di programmare la formazione e l'attuazione delle decisioni di Fondazione stessa, assicurando il rispetto delle leggi e delle procedure interne.

Costituiscono elementi cardine del sistema di controllo interno e gestione del rischio adottata dalla Fondazione:

- lo Statuto, che definisce i poteri dei principali organi della Fondazione e contempla diverse previsioni finalizzate ad assicurare il corretto svolgimento delle attività;
- l'Organigramma che rappresenta il sistema organizzativo adottato dalla Fondazione, al fine di garantire una corretta attribuzione di ruoli e funzioni;
- il Codice Etico, che definisce i principi etici a cui la Fondazione si ispira;
- il Sistema Sanzionatorio che disciplina le violazioni del Codice Etico, del Modello e delle procedure in vigore;
- il Sistema procedurale, costituito da Procedure e Protocolli, Ordini di servizio, Policy, Regolamenti, Istruzioni operative, Comunicazioni interne e ogni altra documentazione volta a regolamentare i processi rilevanti e a definire le modalità operative e i presidi di controllo per lo svolgimento delle attività;
- le attività di formazione ed informazione.

In aggiunta, la Fondazione ha implementato specifici controlli generali applicabili in tutte le aree ed i processi sensibili. Si tratta, nello specifico, dei seguenti controlli:

- trasparenza: ogni operazione, transazione o azione deve essere giustificabile, verificabile, coerente e congruente;
- segregazione di funzioni e poteri: nessuno può gestire in autonomia un intero processo e può essere dotato di poteri illimitati; i poteri autorizzativi e di firma devono essere definiti in modo coerente con le responsabilità organizzative assegnate;
- adeguatezza delle norme interne: l'insieme delle norme è coerente con l'operatività svolta, il livello di complessità organizzativa ed è tale da garantire i controlli necessari a prevenire la commissione dei reati previsti dal Decreto;
- tracciabilità: ogni operazione, transazione o azione, nonché la relativa attività di verifica e controllo devono essere documentate e la documentazione deve essere adeguatamente archiviata.

### 3.4 Stakeholders di Fondazione Carige

Il modello organizzativo idoneo a prevenire i reati contribuisce alla diffusione della cultura della responsabilità e della prevenzione all'interno delle organizzazioni con un diretto riflesso sull'immagine aziendale e sulla sua percezione da parte dei diversi portatori di interesse (stakeholders) e terzi e crea un circolo virtuoso che comincia dal rispetto di regole e policy di best practice e continua con la promozione di questo presso gli stakeholder dell'Ente.

Stakeholders primari, detti anche stakeholder chiave, sono coloro che hanno il più alto livello di interesse per i risultati dell'azienda e a loro è legata la sua sopravvivenza, tra questi: "azionisti", dipendenti, fornitori, clienti.

- Occorre in primo luogo menzionare gli "stakeholders" che hanno il compito di designare i consiglieri di indirizzo così come previsto dallo statuto:

Regione Liguria

Città metropolitana di Genova

Comune di Genova

Comune di Imperia

Provincia di Imperia

CCIA di Genova

CCIA di Imperia e Savona

Arcidiocesi di Genova, Diocesi di Chiavari, Diocesi di Albenga-Imperia e Diocesi di Ventimiglia e Sanremo Università degli studi di Genova.

- I dipendenti che risultano nel corso dell'anno 2024 pari a 6 unità.
- Tra gli stakeholder primari si ricordano altresì le banche, i fornitori e i beneficiari della procedura di erogazione di contributi, categorie di soggetti con cui la Società intrattiene profittevoli rapporti improntati a trasparenza e puntualità nel rispetto dei reciproci impegni.

Gli stakeholder secondari, sono da individuarsi in quei soggetti in grado di influenzare politiche, processi della Fondazione, e tra questi vanno annoverate associazioni, media, comunità locali. In Fondazione non risultano presenti rappresentanze sindacali di categoria.

## 4 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI FONDAZIONE CARIGE

### 4.1 Destinatari

Le regole e le disposizioni contenute nel MOG si applicano e devono essere rispettate da tutti coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo della Società, dai dipendenti, nonché da coloro i quali, pur non appartenendo alla Società, operano su mandato della medesima.

Sono quindi "Destinatari" del presente Modello:

- i titolari di qualifiche formali riconducibili alla definizione di "soggetti apicali" (componenti del Consiglio di Amministrazione e di Indirizzo);
- il Segretario Generale, il Collegio Sindacale e l'Organismo di Vigilanza;
- i lavoratori subordinati, in forza di qualsiasi tipo di rapporto contrattuale (collaboratori legati da contratti a termine; collaboratori a progetto);
- chiunque agisca in nome e per conto della società sotto la sua direzione e vigilanza a prescindere dal vincolo di subordinazione.

Ai collaboratori, consulenti, fornitori, partner commerciali e altre controparti contrattuali in genere, pur non riconducibili alla definizione di Destinatari del Modello (pertanto non assoggettabili alle sanzioni disciplinari in caso di violazioni al Modello), Fondazione Carige richiede il rispetto delle prescrizioni dettate dal Decreto e dei principi etici adottati dalla Società, tramite la sottoscrizione di specifiche clausole contrattuali che assicurino l'impegno al rispetto delle norme di cui al D.Lgs. 231/01 e dei principi etici adottati dalla Società.

## 4.2 Struttura del Modello e documentazione

Il Modello si compone di:

- 1 Parte Generale, volta ad illustrare i contenuti del D.Lgs. 231/2001, nonché gli elementi fondanti del modello di organizzazione, gestione e controllo adottato dalla Società: la sua definizione e adozione, le caratteristiche, il funzionamento e le funzioni dell'Organismo di Vigilanza, i flussi informativi da e verso l'Organismo, il sistema disciplinare, l'attività di formazione e informazione e i criteri per l'aggiornamento del Modello stesso.
- 2 Parti Speciali predisposte a seguito dell'identificazione dei processi "sensibili", laddove siano stati individuati potenziali profili di rischio associabili alle classi di reato richiamate dal Decreto. Attualmente le Parti Speciali sono:
  - 01 Reati con la Pubblica Amministrazione (Art.24 D.LGS 231/01)
  - 02 Delitti Informatici e Trattamento Illecito di Dati (Art.24bis D.LGS 231/01)
  - 03 Reati contro la Pubblica Amministrazione (Art.25 D.LGS 231/01)
  - 04 Reati Societari (Art.25ter D.LGS 231/01)
  - 05 Reati commessi in violazione degli adempimenti in materia di tutela della salute e sicurezza nei luoghi di lavoro (Art.25 septies)
  - 06 Reati di Ricettazione, Riciclaggio ed impiego di utilità illecite, Autoriciclaggio (Art.25 octies)
  - 07 Induzione a non rendere Dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art.25 decies)
  - 08 Reati tributari (Art. 25 quinquiesdecies)
  - 09 Delitti contro il patrimonio culturale – Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (Art.25 septiesdecies e duodevices).

Le **Parti Speciali hanno ad oggetto la disamina e l'indicazione dei presidi e delle norme di comportamento per le sole categorie di reato che, a seguito della attività di risk assessment, sono state considerate –seppure con graduazione di rischio assai differente tra loro- in astratto configurabili.**

**Le ragioni di non configurabilità tout court o per insufficienza dei presupposti delle altre fattispecie di reato risultano formalizzate nel documento di risk assessment.**

Si evidenzia come dette fattispecie saranno oggetto di monitoraggio e la valutazione operata sarà oggetto di nuova disamina in ipotesi di modifiche normative o dell'ambito delle attività aziendali in concreto esercitate.

Sono **oggetto di pubblicazione sul sito web aziendale:**

- (i) Il Modello Parte Generale;
- (ii) il Codice Etico e di Condotta, da intendersi parte integrante del Modello;
- (iii) la procedura "whistleblowing" e la documentazione ad essa attinente (informativa privacy etc.).

La Parti Speciali, il documento di *risk assessment* ed altra documentazione parte integrante del Modello contengono elementi di sensibilità che ne rendono inopportuna la pubblicazione: la documentazione è in ogni caso divulgata ai destinatari e a disposizione presso la sede della Fondazione.

### 4.2.1 Ulteriori Procedure e Protocolli rilevanti

Pare opportuno ribadire come costituiscano parte integrante del MOG, o in quanto allegati di Parte Speciale o poiché espressamente richiamati nella loro interezza, tra gli altri:

- il documento di *risk assessment* di rilevazione dei rischi di commissione dei reati presupposto (**ALL.A**) nel quale è stata esclusa la configurabilità –financo astratta- di determinate fattispecie e per ogni singolo reato presupposto ritenuto rilevante sulla base di specifica analisi, risultano richiamati appositi protocolli di condotta o procedure atte a prevenire la commissione dei reati stessi;
- tutte le procedure (anche in forza di eventuali certificazioni in essere), nonché le istruzioni operative ivi richiamate;
- il Documento di Valutazione dei rischi e i Duvri;
- il Codice Etico, in cui sono rappresentati i principi generali (trasparenza, correttezza, lealtà) cui si ispira lo svolgimento e la conduzione delle attività;
- tutte le ulteriori procedure e/o le procedure e istruzioni comunque formalmente adottate dalla Società.

In particolare il **Codice Etico** esprime, fra l'altro, linee e principi di comportamento volti a prevenire i reati di cui al D.Lgs. 231/01 e richiama espressamente il Modello come strumento utile per operare nel rispetto delle normative. Il Codice Etico deve quindi essere considerato come parte integrante del presente Modello e strumento fondamentale per il conseguimento degli obiettivi del Modello stesso.

Le **procedure ed i protocolli** ritenuti rilevanti ai fini della prevenzione delle fattispecie di reato 231 si intendono richiamati nella ultima *release* formalmente adottata dalla Società.

#### **4.2.2 Il Sistema di Compliance Integrato**

È ormai dato acquisito che il rischio di *compliance*, ossia di non conformità alle norme, comporta per le imprese il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni reputazionali in conseguenza di violazioni di norme imperative ovvero di autoregolamentazione, molte delle quali rientrano nel novero dei reati di cui al D.Lgs. 231/2001. Ciò posto, la gestione dei numerosi obblighi di *compliance*, secondo un approccio tradizionale, può risultare connotata da una pluralità di processi, informazioni potenzialmente incoerenti, controlli potenzialmente non ottimizzati, con conseguente ridondanza nelle attività.

Il passaggio ad una *compliance* integrata permette invece agli Enti di:

- razionalizzare le attività (in termini di risorse, persone, sistemi, ecc.);
- migliorare l'efficacia ed efficienza delle attività di *compliance*;
- facilitare la condivisione delle informazioni attraverso una visione integrata delle diverse esigenze di *compliance*, anche attraverso l'esecuzione di *risk assessment* congiunti, e la manutenzione periodica dei programmi di *compliance* (ivi incluse le modalità di gestione delle risorse finanziarie, in quanto rilevanti ed idonee ad impedire la commissione di molti dei reati espressamente previsti come fondanti la responsabilità degli enti).

In quest'ottica, un approccio integrato dovrebbe, quindi, contemplare procedure comuni che garantiscano efficienza e snellezza e che non generino sovrapposizione di ruoli (o mancanza di presidi), duplicazioni di verifiche e di azioni correttive, in termini più ampi, di conformità rispetto alla copiosa normativa di riferimento, laddove tali ruoli rispettivamente incidano e insistano sui medesimi processi. Le società tenute al rispetto delle diverse normative dovrebbero valutare l'opportunità di predisporre o integrare tali procedure tenendo conto delle peculiarità sottese a ciascuna di esse, portando a sintesi gli adempimenti, individuando le modalità per intercettare e verificare gli eventi economici e finanziari dell'impresa nell'ottica del corretto agire.

A titolo esemplificativo la legislazione prevenzionistica vigente in materia di salute e sicurezza sul lavoro (art. 2087 c.c., d.lgs. n. 81 del 2008 e successive modifiche) detta principi cogenti e adempimenti organizzativi obbligatori ai fini della gestione dei rischi. In tal caso, quando l'impresa

decide di adottare un modello di organizzazione e gestione, deve assicurare la presenza di un sistema aziendale per l'adempimento delle previsioni del decreto 81 del 2008. In questo modo, l'ente potrà disporre di un sistema di prevenzione e gestione dei rischi in tema di salute e sicurezza sul lavoro complessivamente rispondente alle prescrizioni imposte dal decreto 81/08 (al fine di minimizzare i rischi di malattie professionali e infortuni) e dal decreto 231 (per ridurre ad un livello "accettabile" il rischio di una condotta deviante dalle regole poste dal modello organizzativo). Una simile soluzione può consentire una più efficace attività di prevenzione di rischi, con sensibili vantaggi in termini di razionalizzazione e sostenibilità dei sistemi di prevenzione.

Quanto sopra premesso occorre precisare come l'articolo 30, comma 5, del decreto 81 affermi che i modelli di organizzazione e gestione adottati sulla base di alcuni sistemi di controllo del rispetto delle norme in materia di salute e sicurezza dei lavoratori (Linee guida UNI-INAIL del 2001 o British Standard OH-SAS 18001:2007 o UNI 45001:2018) si presumono conformi ai requisiti di idoneità ai fini dell'efficacia esimente dalla responsabilità da reato dell'ente. Questo non significa che il possesso delle certificazioni indicate dalla norma sia di per sé sufficiente a esonerare l'ente da responsabilità da reato in caso di eventuali infortuni o malattie professionali. L'articolo 6, comma 1, lett. a) del decreto 231, infatti, specifica che il modello idoneo a prevenire reati della specie di quello verificatosi non deve essere solo adottato, ma anche efficacemente attuato. Ebbene, come chiarito dalla giurisprudenza, la presunzione di conformità sancita dall'articolo 30, comma 5, decreto 81 del 2008 può coprire la valutazione di astratta idoneità preventiva del modello, non anche la verifica in ordine alla sua efficace attuazione. Quest'ultima non può prescindere dall'osservazione concreta e reale - da parte del giudice - del modo in cui il modello organizzativo è vissuto nell'assetto imprenditoriale, al fine di verificare se il documento in cui esso consta sia stato effettivamente implementato. Le considerazioni che precedono valgono a maggior ragione per gli altri sistemi di gestione aziendale, per i quali la legislazione non prevede alcuna presunzione di conformità.

#### **4.2.3 Il GDPR e il DPO**

Fermo quanto sopra rilevato, nell'ottica di integrazione dei modelli gestionali adottati, l'insieme di procedure e protocolli adottati dalla Fondazione al fine di conformarsi in ambito privacy al GDPR integrano certamente un presidio anche ai fini 231/01. L'armonizzazione delle due normative (231/01 e GDPR) può essere garantita solo pensando a modelli di organizzazione e gestione integrati con le disposizioni in materia di privacy.

Il GDPR richiede, infatti, l'adesione della compliance aziendale alla normativa in materia di privacy attraverso l'adozione degli strumenti necessari per assicurare il più alto grado di tutela dei dati personali estratti dai database aziendali, tramite l'adeguamento al GDPR dei c.d. MOG 231, ossia i modelli di organizzazione e gestione aziendale previsti dagli artt. 6 e 7 del D. Lgs. n. 231/2001, che contribuiscono a tipizzare il nesso di imputazione soggettiva della responsabilità delle persone giuridiche, articolandolo sulla base di categorie soggettive a cui appartengono gli autori del reato-presupposto e, più precisamente, del legame funzionale di questi con l'ente. modelli organizzativi privacy, tenendo conto dei rischi emergenti dalle attività aziendali che richiedono il trattamento dei dati personali ex art. 4 n. 2) del Regolamento n.679/2016, risultano quindi utili, se non fondamentali, per garantire la prevenzione dell'eventuale responsabilità dell'azienda derivante da reati commessi in suo vantaggio e/o interesse da dipendenti o soggetti in posizioni apicali all'interno della stessa.

L'Art. 25 del GDPR, nel definire la privacy by design al comma 1 (protezione dei dati fin dalla progettazione del sistema) e la privacy by default al comma 2 (protezione dei dati per impostazione predefinita), fa riferimento all'adozione, da parte del titolare del trattamento, di "misure tecniche e

organizzative adeguate, in modo da attuare efficacemente i principi di protezione dei dati e da garantire nel trattamento i requisiti del Regolamento e la tutela dei diritti degli interessati”.

Analogamente, anche se in ambito differente dal data protection, l'Art. 6 comma 2 lett. b) del Dlgs. 231/2001, definendo i modelli di organizzazione e gestione dell'ente, stabilisce che questi devono “prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire”.

Appare oltremodo chiara l'armonia tra le due disposizioni che, pur normando aspetti differenti di compliance, convergono sulla necessità d'adozione di prassi standardizzate al fine di garantire la conformità delle attività aziendali alle normative vigenti e vagliare i rischi sottesi a tali attività, c.d. *risk-based approach* prerequisito per individuare misure tecniche e organizzative adeguate. Ed è proprio questo concetto che permette di introdurre un altro punto di intersezione tra le disposizioni normative esaminate. Infatti, in materia di data protection, esistono comportamenti scorretti ed eventi informatici malevoli che possono integrare fattispecie di reato, le quali, se derivanti da condotte di soggetti interni all'azienda, possono costituire il presupposto per innescare la responsabilità dell'ente stesso.

Si richiamano, a titolo esemplificativo gli artt. 24 e 24 bis del D.Lgs. 231/2001, non a caso rubricati “*Indebita percezione di erogazioni, truffa in danno dello Stato o di ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di ente pubblico*” e “*Delitti informatici e trattamento illecito dei dati*”, che prevedono diverse categorie di cyber crime come reati presupposto all'innescamento della responsabilità d'impresa. L'inserimento di tali reati nel D. Lgs. 231/01, pur non coprendo tutte le fattispecie previste nel GDPR, ha garantito che un solido nucleo di eventi criminosi, legati ai profili della protezione dei dati in ambito aziendale, venissero perseguiti anche in relazione alla responsabilità a carico dell'ente, con conseguente irrogazione di pesanti sanzioni pecuniarie e interdittive di cui all'art. 9 del D.Lgs. 231/01 dal carattere profondamente afflittivo per le imprese. Infatti, al verificarsi di un evento malevolo per la privacy, la normativa 231, insieme con il GDPR, costituirebbero il comune denominatore per la valutazione dell'eventuale responsabilità dell'ente per l'omissione colposa della predisposizione dei MOG funzionali ad evitare la commissione di data breach.

In definitiva, si evidenzia come entrambe le normative spingano sinergicamente verso una sempre crescente responsabilizzazione delle strutture aziendali, in relazione alle attività svolte.

La Fondazione ha pertanto provveduto a conformare la gestione dei dati personali al GDPR (REG UE 2016/679), ponendo in essere la relativa analisi di rischio, redigendo la documentazione a tal fine necessaria (informative etc.), individuando il Titolare del trattamento e nominando il Responsabile della protezione dei dati (indirizzo e-mail di contatto: [privacy@fondazionecarige.it](mailto:privacy@fondazionecarige.it)). A seguito del Reg UE 2016/679 in parola, per quanto qui di interesse, occorre ricordare come d.lgs. 33/2013 (in quota parte applicabile alle Fondazioni Bancarie per quanto esposto *infra* al § 11.) all'art. 7 bis, co. 4, disponga che «*nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione*». Si richiama anche quanto previsto all'art. 6 del d.lgs. 33/2013 rubricato “Qualità delle informazioni” che risponde alla esigenza di assicurare esattezza, completezza, aggiornamento e adeguatezza dei dati pubblicati. Al riguardo, si rinvia alle più specifiche indicazioni fornite dal Garante per la protezione dei dati personali. Si ricorda inoltre che, in ogni caso, ai sensi della normativa europea, il Responsabile della Protezione dei Dati-RPD (vedi *infra* paragrafo successivo) svolge specifici compiti, anche di supporto, per tutta

la realtà aziendale essendo chiamato a informare, fornire consulenza e sorvegliare in relazione al rispetto degli obblighi derivanti della normativa in materia di protezione dei dati personali (art. 39 del RGPD).

#### **4.2.4 Fondazione Carige e gli Obblighi di Trasparenza**

Al fine di enucleare gli obblighi in punto “trasparenza” e pubblicazione sul sito web istituzionale occorre prendere le mosse dai contenuti della Deliberazione Anac 1134/2017, pubblicata in G.U. in data 5.12.2017, la quale detta le “Nuove linee guida per l’attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici”, in sostituzione della previgente Determina n°8/2015.

La questione della applicazione della normativa in materia di prevenzione della Corruzione e per l’integrità e Trasparenza era già stata oggetto di riflessione in seno a Fondazione Carige, anche alla luce di non univoche indicazioni rinvenibili da un lato dalle norme di legge di riferimento e dall’altro dalla interpretazione estensiva di ANAC.

Ancora in Relazione AIR del 14.04.15 l’Autorità affermava quanto di seguito riportato: *«E’ stato osservato (Direttore generale di ACRI) come sia necessario evitare che si possa ingenerare il dubbio che l’attività delle Fondazioni di origine bancaria abbia rilevanza pubblicistica. Ad ogni buon conto viene evidenziato come il tema della trasparenza dell’attività sia per le Fondazioni un principio fondamentale, come testimoniato dalla Carta delle Fondazioni. Alcune delle Fondazioni si sono dotate autonomamente di procedure e protocolli, anche basati sul d.lgs. n. 231 del 2001 in relazione ai reati presupposti che possono, anche in astratto, assumere rilievo per gli enti non profit. Nelle linee guida è stato ribadito come anche per tali enti si ponga, analogamente a quanto avviene per le società partecipate, il problema dell’esposizione al rischio di corruzione che il legislatore ha inteso prevenire con la normativa anticorruzione in relazione alle pubbliche amministrazioni. Gli enti di diritto privato in controllo pubblico e in particolare le Fondazioni in via generale sono, pertanto, tenute ad applicare la normativa sulla prevenzione della corruzione. Per quanto attiene alla trasparenza anche per questi enti, così come per le società in controllo pubblico, la stessa deve essere assicurata sia sull’attività, limitatamente a quella di pubblico interesse disciplinata dal diritto nazionale e dell’Unione europea, sia sull’organizzazione. Per quanto concerne le fondazioni bancarie, le casse di previdenza dei liberi professionisti, le associazioni e le fondazioni derivanti dalla trasformazione per legge di istituzioni pubbliche di assistenza e beneficenza, nonostante l’indubbio rilievo di interesse generale delle funzioni ad esse attribuite, sono state fatte rientrare, anche sulla base della giurisprudenza, ordinaria e costituzionale, nella categoria degli enti di diritto privato solo partecipati da pubbliche amministrazioni. Per esse si applica, dunque, la disciplina prevista per le società partecipate».*

Orbene, nelle nuove Linee Guida al § 3.4.3 rubricato “casi specifici” (pag.40) la Deliberazione si occupa nello specifico della Fondazioni bancarie affermando quanto di seguito, per chiarezza e rilevanza, si riporta: *«Alla luce dei criteri dettati dalle modifiche normative introdotte con il d.lgs. 97/2016, si ritiene che le fondazioni bancarie debbano considerarsi escluse dal novero degli enti di cui al co. 3 dell’art. 2 bis del d.lgs. 33/2013, in quanto la loro attività non appare riconducibile alla definizione di attività di pubblico interesse ivi contenuta. Infatti, ad avviso dell’Autorità e conformemente a quanto finora statuito dalla giurisprudenza maturata sul tema, occorre distinguere le attività “di pubblico interesse” da quelle “di utilità sociale”. Soltanto le prime sono assoggettate alle norme sulla trasparenza (e sulla prevenzione della corruzione). Infatti, l’attività di pubblico interesse deve sempre essere collegata all’espletamento di Funzioni pubbliche.*

*L'attività di utilità sociale rientra, invece, tra le attività svolte in piena autonomia privata da soggetti privati. Si tratta di un'attività che viene riconosciuta e valorizzata da pubbliche amministrazioni, in applicazione dell'articolo 118, ultimo comma, della Costituzione, ma che resta distinta da quelle di esercizio di vere e proprie funzioni pubbliche. La natura pubblica degli interessi non può essere riferita genericamente a tutte le attività che assumano un rilievo sociale di interesse generale in base all'orientamento di scelte rimesse alla discrezionalità privata, come avviene nel caso delle scelte operate dalle fondazioni bancarie. Ciò non esclude, tuttavia, che le fondazioni bancarie possano decidere autonomamente di contribuire all'attuazione della disciplina della trasparenza e della prevenzione della corruzione, pubblicando i dati più rilevanti relativamente alle attività svolte. In particolare, nell'ambito dell'Accordo tra il Ministero dell'economia e delle finanze e l'Associazione di fondazioni e casse di risparmio S.p.A, siglato il 22 aprile 2015, è previsto, all'art. 11 che queste ultime pubblichino i dati sulla propria attività e, tra gli altri, quelli relativi alle procedure attraverso le quali i terzi possono avanzare richieste di sostegno finanziario indicando le condizioni di accesso, i criteri di selezione e il processo attraverso cui ha luogo la selezione delle iniziative proposte nonché gli esiti delle stesse. L'Autorità auspica che ulteriori dati, documenti e informazioni siano individuati, nel quadro del richiamato Accordo o in sede di autonoma decisione delle singole fondazioni, come oggetto di pubblicazione a fini di trasparenza. L'Autorità auspica, poi, che le fondazioni adottino misure di prevenzione della corruzione, secondo il "modello 231", soprattutto per le attività di utilità sociale di maggiore rilevanza».*

Prendendo le mosse dalle indicazioni della Autorità, in riferimento alla pubblicazione dei dati relativi alla gestione delle richieste di sostegno finanziario, si ricorda come la Fondazione abbia adottato per la richiesta di contributi la cd. "Procedura ROL", pubblicata sul sito istituzionale all'indirizzo <https://www.fondazionecarige.it/wp/richiesta-contributi/>. Del pari risultano correttamente pubblicati gli esiti dei bandi, nonché dati ulteriori quali i documenti programmatici, i bilanci, lo statuto, il Modello 231/01, il regolamento delle nomine.

#### **4.2.5 Ulteriori norme di riferimento: Provvedimento della Banca d'Italia del 23 luglio 2024**

Con provvedimento della Banca d'Italia del 23 luglio 2024 BANCA D'ITALIA, COVIP, IVASS E MEF, in considerazione del ruolo ad essi attribuito di "organismi di vigilanza", vista la legge 9 dicembre 2021, n. 220, recante misure per contrastare il finanziamento delle imprese produttrici di mine antipersona, di munizioni e submunizioni a grappolo, hanno provveduto ad emanare istruzioni per l'esercizio di controlli rafforzati sull'operato degli intermediari abilitati per contrastare il finanziamento delle imprese produttrici di mine antipersona, di munizioni e submunizioni a grappolo.

Gli intermediari abilitati si debbono adeguare al contenuto delle istruzioni entro sei mesi (febbraio 2025), decorrenti dalla data della loro entrata in vigore (08.08.2024) e tra essi rientrano altresì le fondazioni italiane di origine bancaria (art.3 Ambito di applicazione).

Le istruzioni emanate prescrivono, in sintesi, che gli intermediari abilitati debbono:

- adottare "idonei presidi procedurali -eventualmente adattando o integrando il sistema esistente di gestione dei rischi -, secondo un approccio risk-based e sulla base del principio di proporzionalità, in ragione della tipologia di attività svolta, dimensione e complessità operativa, opportunamente formalizzati nella regolamentazione interna e volti ad assicurare il rispetto del divieto di finanziamento delle società indicate all'articolo 1, comma 1, della legge. Tali presidi sono definiti in coerenza con le previsioni in materia di sistema di governo, organizzazione e controlli interni contenute nelle normative di settore applicabili a ciascun intermediario abilitato. I presidi

*sono definiti tenendo conto dell'operatività dell'intermediario abilitato e delle società da esso controllate*”;

- adottare misure adeguate ad *“assicurare il rispetto del divieto. Qualora, all'esito delle procedure di controllo effettuate dagli intermediari abilitati, emerga che i potenziali destinatari dei finanziamenti sono coinvolti nelle attività di cui all'articolo 1, comma 1, della legge, gli intermediari abilitati adottano le misure necessarie per assicurare il rispetto del divieto (es. diniego alla concessione del finanziamento) se del caso previo opportuno confronto con i beneficiari interessati”*.

Come anticipato i presidi sono definiti tenendo conto dell'operatività dell'intermediario abilitato. Essi includono almeno:

- l'obbligo di consultare *«elenchi pubblicamente disponibili di società che producono mine antipersona e munizioni e submunizioni a grappolo»* (cfr. articolo 4 della legge) prima di effettuare il finanziamento;

- procedure per valutare il rischio di coinvolgimento del destinatario del finanziamento nelle attività di cui all'articolo 1, comma 1, della legge, alla luce, ad esempio, dell'attività svolta, della sede legale, del luogo di operatività del destinatario.

Si prende atto che il termine finanziamento è da interpretarsi estensivamente, dato che esso ricomprende, ai sensi dell'art.2 della legge *“ogni forma di supporto finanziario effettuato anche attraverso società controllate, aventi sede in Italia o all'estero, tra cui, a titolo esemplificativo e non esaustivo, la concessione di credito sotto qualsiasi forma, il rilascio di garanzie finanziarie, l'assunzione di partecipazioni, l'acquisto o la sottoscrizione di strumenti finanziari emessi dalle società di cui al presente articolo”*.

In considerazione della concreta operatività di Fondazione Carige il rischio di incorrere in condotte che integrino violazione della norma di legge in esame appare, in concreto, del tutto improbabile.

Ed invero Fondazione:

- nell'amministrare il patrimonio totalmente vincolato al perseguimento degli scopi statutari, la Fondazione deve attenersi a criteri prudenziali in modo da conservare il valore e ottenerne un'adeguata redditività, oltre che in modo coerente con la sua natura di ente senza scopo di lucro che opera secondo i principi di trasparenza e moralità: per quanto sopra la Fondazione effettua investimenti unicamente in strumenti finanziari emessi da soggetti istituzionali;

- eroga “finanziamenti”, pur nella interpretazione estensiva sopra ricordata, unicamente tramite la procedura ROL (che già contempla verifiche in punto meritevolezza e liceità delle iniziative oggetto di richiesta di contributo), al fine di intervenire direttamente e indirettamente, nei settori dello Sviluppo locale, della Ricerca scientifica e tecnologica, della Salute pubblica, medicina preventiva e riabilitativa, dell'Educazione, istruzione e formazione, dell'Arte, attività e beni culturali, del Volontariato, filantropia e beneficenza.

La Fondazione ha valutato, per quanto esposto, sufficiente l'adozione dei presidi minimali indicati in Istruzioni e a tal fine ha provveduto a modificare la procedura ROL in vigore, affinché le funzioni competenti provvedano nel corso della istruttoria della pratica ed antecedentemente alla sua liquidazione a verificare per ogni tipologia di finanziamento, erogazione e/o contributo che:

- il beneficiario in forza di consultazione degli elenchi pubblicamente disponibili, non sia ricompreso tra le società che producono mine antipersona e munizioni e submunizioni a grappolo (cfr. articolo 4 della legge;
- non sussista il rischio di coinvolgimento del destinatario del finanziamento nelle attività di cui all'articolo 1, comma 1, della legge, alla luce, ad esempio, dell'attività svolta, della sede legale, del luogo di operatività del destinatario.

## 5. IL PROCESSO DI REALIZZAZIONE DEL MODELLO

### 5.1 LE SOGLIE DIMENSIONALI DI FONDAZIONE CARIGE

#### 5.2 LA ATTIVITA' DI RISK ASSESSMENT E LE ATTIVITÀ AZIENDALI "SENSIBILI"

L'art. 6 del d.lgs 231/01 indica le caratteristiche essenziali per la costruzione del MOG. In particolare alle lettere a) e b) della disposizione vengono espressamente indicate alcune attività correlate ad un processo di adeguata gestione dei rischi.

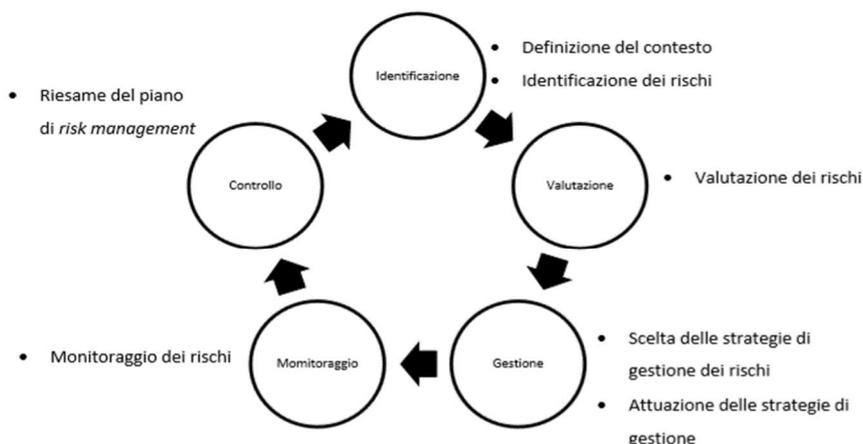
Ferma restando l'esigenza che ogni impresa costruisca e mantenga in efficienza il proprio sistema di gestione dei rischi e di controllo interno in una ottica anche di "compliance integrata" con vari sistemi già presenti, di seguito si indica un approccio coerente con i principali elementi della struttura di riferimento in termini di controllo interno e gestione dei rischi.

Antecedentemente alla emissione della presente release del Modello la Fondazione ha posto in essere un aggiornamento della attività di risk assessment.

Le fasi principali, in cui il sistema di prevenzione dei rischi 231 e il documento di *risk assessment* si è articolato, risultano essere:

- a) la identificazione dei rischi potenziali, ossia l'analisi del contesto aziendale per individuare quali aree o settori di attività e secondo quali modalità si potrebbero astrattamente verificare eventi pregiudizievoli per gli obiettivi indicati nel D.lgs 231. Per "rischio" si intende qualsiasi variabile o fattore che nell'ambito delle attività aziendali, da sola o con altre variabili, possano incidere negativamente sul raggiungimento degli obiettivi del Decreto 231 (es. all'art. 6 comma 1 lettera a); pertanto a seconda della tipologia di reato, gli ambiti di attività a rischio potranno essere più o meno estesi;
- b) la progettazione o implementazione dei sistemi di controllo (i cd. protocolli per la formazione e l'attuazione delle decisioni dell'ente) all'interno della Fondazione per la prevenzione dei reati e dell'eventuale adeguamento dell'assetto, in termini di capacità di efficace contrasto, cioè di ridurre ad un livello accettabile, i rischi identificati. Sotto il profilo concettuale, ridurre un rischio comporta dover intervenire, congiuntamente o disgiuntamente, su due fattori determinanti:
  - la probabilità di accadimento dell'evento;
  - l'impatto dell'evento stesso.

Il *risk management*, attraverso l'applicazione del processo di controllo, protegge e dà valore all'organizzazione e ai suoi stakeholder sostenendo gli obiettivi dell'organizzazione. Il quadro metodologico consente di controllare ogni futura attività e il miglioramento del processo decisionale, secondo lo schema di seguito raffigurato:



E' fondamentale definire il concetto di rischio accettabile. Nella progettazione di sistemi di controllo a tutela dei rischi di business, definire il rischio accettabile è un'operazione relativamente semplice dal punto di vista concettuale. Nel caso della normativa ex D.Lgs 231 la logica ad es. economica dei costi non può, tuttavia, rappresentare un riferimento utilizzabile in via esclusiva.

Riguardo al presente sistema di controllo preventivo costruito in relazione al rischio di commissione delle fattispecie di reato contemplate nel 231, la soglia concettuale di accettabilità, nei casi dolosi, è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non fraudolentemente.

Premesso che i modelli organizzativi devono essere idonei a prevenire i reati sia di origine dolosa che colposa previsti dal decreto 231, primo obiettivo nella nuova ed ulteriore attività di revisione del modello organizzativo (ed ancora prima in quella di redazione della attuale *release* del documento di *risk assessment*) è stato quello di verificare la corretta proceduralizzazione delle attività che comportano un rischio di reato, al fine di evitarne la commissione. L'insieme delle misure che il dipendente aziendale, se vuole delinquere, sarà costretto a "forzare" dovrà essere realizzato in relazione alle specifiche attività dell'ente considerate a rischio e ai singoli reati ipoteticamente collegabili ad essa. Attraverso, quindi, un'attenta analisi della situazione aziendale e della sua dinamica, la Fondazione ha individuato possibili rischi e verificato l'esistenza e l'attuazione di strumenti di controllo atti a prevenire i rischi considerati ovvero ha implementato ed adottato protocolli di condotta aggiuntivi a quelli già esistenti ed attuati.

In collaborazione con il management aziendale e le funzioni competenti (pur in assenza di responsabili di funzioni propriamente detti) è stata effettuata:

- una ricognizione delle aree aziendali a rischio e dei reati rilevanti;
- redatta una mappa documentata delle potenziali modalità attuative degli illeciti nelle aree a rischio;
- documentato il sistema dei controlli preventivi attivato e gli adeguamenti eventualmente necessari.

Come innanzi posto in rilievo, la predisposizione del presente Modello ha preso avvio dall'individuazione delle attività poste in essere dalla Fondazione e dalla conseguente identificazione dei processi e delle attività aziendali "sensibili" per la realizzazione degli illeciti indicati dal Decreto.

In concreto ed in sintesi il *risk assessment* o valutazione del rischio può essere definito come il processo di stima dei fattori di rischio associati a specifiche attività di una organizzazione. Esso comprende le attività di:

- 1) identificazione delle attività/processi;

- 2) individuazione delle minacce e dei fattori di rischio;
- 3) valutazione ed attribuzione del livello di rischio;
- 4) classificazione delle attività in base al rischio potenziale

Nella **fase 1**) debbono essere oggetto di analisi preliminare il contesto aziendale al fine di individuare i processi e le attività per i quali esiste il rischio di incorrere nelle fattispecie di reato previste dal D.Lgs. n. 231/2001.

I principali oggetti di riferimento dell'analisi in questione sono la struttura organizzativa dell'azienda, le procedure esistenti, le eventuali mappature dei processi interni e tutta la documentazione a supporto in grado di fornire informazioni utili ai fini della identificazione delle attività a rischio (politiche aziendali, leggi e regolamenti, sistema di poteri, deleghe e procure, organigramma, policy e procedure vigenti). Si anticipa che, ai fini di una corretta valutazione dei rischi, sono stati esaminati tutti i reati presupposto, indicati negli articoli del D.Lgs. 231/2001.

Nella **fase 2)** si è proceduto all'elencazione di tutti i rischi potenziali, in questo caso quelli di incorrere nelle fattispecie di reato previste dal D.Lgs. n. 231/2001 ed alla loro attribuzione alle singole attività o ai singoli processi, così come rilevati nella prima fase. Nel caso in cui, per il singolo reato presupposto, non siano state rilevate attività sensibili al rischio di commissione del reato stesso, si verificano le seguenti possibilità di valutazione, come esplicitato nella tabella "*Note per la compilazione del Risk Assessment*": PI (Presupposti Insufficienti) o NA (Non Applicabile).

Nel caso in cui, per il singolo reato presupposto, siano state rilevate attività sensibili, si è proceduto all'individuazione delle risorse aziendali coinvolte nonché alla rilevazione dei protocolli di prevenzione (manuali e procedure gestionali e/o organizzative) con una valutazione della probabilità di accadimento dell'evento. Per la valutazione della probabilità di accadimento si è tenuto conto, quindi, dell'efficacia sia dei protocolli di prevenzione sia dei controlli di presidio del rischio di commissione del reato presupposto.

La successiva **fase 3)** del processo di *risk assessment* si è conclusa con la assegnazione di un valore specifico alle categorie di rischio identificate. In particolare si è proceduto alla individuazione di un peso relativo tra le categorie di rischio ed alla valutazione dei singoli fattori di rischio per ciascuna delle attività e processi rilevati.

I criteri utilizzati per la valorizzazione del livello di rischio sono la probabilità di accadimento dell'evento e la gravità e l'impatto/danno in termini conseguenze derivanti dal verificarsi dell'evento a rischio:

(i) ad esempio, è possibile individuare la gravità dell'impatto in termini di danni di immagine all'azienda e economici/ finanziari in caso di accadimento dei fatti illeciti contemplati nel D.Lgs. n. 231/2001: per i diversi reati presupposto il legislatore ha previsto sanzioni pecuniarie (espresse in "quote") e interdittive che possono essere applicate dal Giudice, sulla base dei minimi e massimi edittali, in considerazione della gravità del fatto, del grado di responsabilità dell'ente e dell'attività svolta per eliminare o attenuare le conseguenze del fatto e prevenire la commissione di ulteriori illeciti. L'impatto può pertanto essere quantificato tenendo in conto il danno economico (sanzioni) e di immagine dell'azienda;

(ii) a sua volta la probabilità di accadimento è determinata dall'oggettiva fattispecie dell'attività a rischio, anche in considerazione della:

- frequenza di esecuzione dell'attività;

- *case history* (l'evento si è o meno verificato nel corso di x anni, nel qual caso debbono in ogni caso essere altresì valutati interventi nell'ambito dell'assetto operativo e/o organizzativo, idonei ad elidere la riproponibilità dell'accadimento);

- adeguatezza dei sistemi di controllo in essere: interni (procedure/protocolli) e di organismi indipendenti esterni all'azienda: a tal fine è stata posta in essere una verifica in merito alla corretta attuazione di detti sistemi di controllo.

- efficacia della attività informativa / formativa e di addestramento del personale dipendente: è evidente che la informazione e formazione del personale coinvolto in attività sensibili, laddove ripetuta periodicamente attraverso lo svolgimento di corsi e incontri con verifica di apprendimento, è idonea a ridurre la probabilità di accadimento, quanto meno di talune fattispecie di reato: anche in questo caso in sede di risk assessment è stata richiesta ed estratta a campione documentazione attestante la erogazione di adeguata formazione, in particolare in ambiti sottratti alla formazione obbligatoria. Il documento di risk assesment (all.A) riporta i seguenti contenuti.

<b>REATO PRESUPPOSTO</b>	<b>Articolo</b> , comma, lettera e numero del riferimento legislativo indicato specificatamente nel D.Lgs. 231/2001 i cui articoli rappresentano i reati principali.	
<b>CONTENUTO del REATO PRESUPPOSTO</b>	<b>Sintesi del contenuto</b> relativo al contenuto del reato presupposto per quanto interessa l'applicazione del D.Lgs.231/2001 e s.m.i.	
<b>ATTIVITA' SENSIBILI al REATO PRESUPPOSTO</b>	<p>Individuazione delle <b>attività e/o azioni dei processi</b> che si ritengono <b>sensibili alla commissione</b> delle fattispecie del REATO PRESUPPOSTO.</p> <p>Laddove sia potenzialmente presente il rischio di commissione del reato presupposto ma <u>non vi siano le condizioni nel momento attuale</u>, sarà indicata la presenza dei <b>PI (Presupposti Insufficienti)</b> e si individueranno, quando possibile, gli specifici parametri da tenere sotto controllo.</p> <p>Nel caso in cui <u>non vi siano mai le condizioni</u> per la commissione del reato presupposto ovvero quando il reato presupposto risulta non commissibile nell'ambito delle attività ordinarie e straordinarie dell'azienda, ragionevolmente prevedibili, si indicherà:  <b>NA = Non Applicabile</b></p>	
<b>FUNZIONI AZIENDALI</b>	Formalizzazione delle funzioni aziendali (aree/settori/responsabili) potenzialmente coinvolte nelle attività sensibili alla commissione del reato presupposto	
<b>PROTOCOLLI (MANUALI, PROCEDURE)</b>	Indicazione dei protocolli (Manuali, Procedure gestionali e/o organizzative) di prevenzione che contengono indicazioni operative per annullare o ridurre il rischio di commissione del singolo reato presupposto.	
<b>Tipologia / Responsabilità / Periodicità del Controllo di Presidio del Rischio</b>	Indicazione della <b>tipologia di controllo</b> messa in atto per presidiare il rischio. Formalizzazione della <b>funzione responsabile del controllo</b> ed indicazione della <b>periodicità</b> .	
	<i>TIPOLOGIA</i>	<i>COMPETENZE</i>
	I livello	GESTORE / RESPONSABILE PROCESSO
	II livello	GESTORE CONFORMITA' A NORME E LEGGI
	III livello	ORGANISMI ESTERNI (OdV – Enti Esterni)
<p>Si qualificano controlli di <u>I° Livello</u> quelli insiti nei processi operativi: si tratta di quei controlli, procedurali, informatici, finanziari, comportamentali, svolti sia da chi mette in atto una determinata attività, sia da chi ne ha la diretta responsabilità di supervisione. Tutte le funzioni aziendali eseguono tali controlli diretti nella gestione delle proprie responsabilità.</p> <p>Si qualificano controlli di <u>II° Livello</u> quelli operati da chi presidia il processo di gestione e controllo dei rischi legati all'operatività garantendone la coerenza rispetto agli obiettivi aziendali e rispondendo a criteri di segregazione che consentono un efficace monitoraggio.</p> <p>Si qualificano controlli di <u>III° Livello</u> quelli operati da soggetti terzi, connotati da requisiti di autonomia, professionalità e indipendenza, i quali effettuano attività di monitoraggio e forniscono valutazioni sull'adeguatezza dell'applicazione del sistema di controllo dei processi, in aree rilevanti ai fini della configurabilità di fattispecie di reato ex D.Lgs. 231/2001 e s.m.i..</p>		

### PROBABILITÀ DI ACCADIMENTO DEL REATO (P)

La probabilità di accadimento può essere valutata in forza della applicazione di tre parametri:

- Casi Passati (approccio retrospettivo): n° di volte in cui l'evento si è verificato in passato;
- Previsioni future (approccio prospettico): n° di volte in cui ci si aspetta che l'evento si verificherà in futuro (anche in relazione alla frequenza di esecuzione dell'attività, alla organizzazione aziendale – adozione di procedure, segregazione di compiti e responsabilità etc.-, alla efficacia della attività formativa);
- Stima in termini % della probabilità di accadimento.

Si delineano pertanto 5 livelli di accadimento, che in relazione ai tre parametri sopra citati si distinguono in:

1. **RARO:**
  - l'evento di rischio non si è verificato negli ultimi 3 anni;
  - si prevede che l'evento non si verificherà nei prossimi 3 anni;
  - l'evento di rischio si verifica soltanto in circostanze eccezionali
2. **IMPROBABILE:**
  - l'evento di rischio si è verificato almeno una volta negli ultimi 3 anni;
  - si prevede che l'evento di rischio si verificherà almeno una volta nei prossimi 3 anni;
  - l'evento di rischio è improbabile che si verifichi
3. **MODERATO:**
  - l'evento di rischio si è verificato almeno una volta nell'ultimo anno o più volte negli ultimi 3 anni;
  - si prevede che l'evento di rischio si verificherà almeno una volta nel prossimo anno o più volte nei prossimi 3 anni;
  - l'evento di rischio può verificarsi in un certo numero di casi
4. **POSSIBILE:**
  - l'evento di rischio si è verificato almeno una volta nell'ultimo anno e più volte negli ultimi 3 anni;
  - si prevede che l'evento di rischio si verificherà almeno una volta nel prossimo anno e più volte nei prossimi 3 anni;
  - l'evento di rischio può verificarsi in un numero rilevante di casi
5. **PROBABILE:**
  - l'evento di rischio si è verificato molto frequentemente nell'ultimo anno e nei prossimi tre anni;
  - si prevede che l'evento di rischio si verificherà molto frequentemente nel prossimo anno e nei prossimi tre anni;
  - l'evento di rischio si verifica nella maggior parte dei casi

### MAGNITUDO (P)

La magnitudo, o gravità delle conseguenze della commissione del reato, è determinata alla luce delle sanzioni connesse al reato commissibile nello svolgimento dell'attività oggetto di analisi. La magnitudo si classifica in:

1. **BASSA (M=1) = confisca del profitto** per riparazione delle conseguenze del reato;

2. SIGNIFICATIVA (M=2) = **sanzione pecuniaria** che va da 100 a 300 quote per la commissione del reato singolo (per la pluralità di illeciti la sanzione dell'illecito più grave è aumentata fino al triplo);
3. RILEVANTE (M=3) = **sanzione pecuniaria** che va da 301 a 500 quote con eventuali moltiplicazioni previste dal D.Lgs. 231/01 (per la pluralità di illeciti la sanzione dell'illecito più grave è aumentata fino al triplo);
4. MOLTO RILEVANTE (M=4) = **sanzione pecuniaria** che va da 501 a 1000 quote con eventuali moltiplicazioni previste dal D.Lgs. 231/01 (per la pluralità di illeciti la sanzione dell'illecito più grave è aumentata fino al triplo)
5. ESTREMA (M=5) = **Sanzione di tipo interdittivo**: Art. 9 co.2 lett. b, c, d, e; (b=sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c=divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d=esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e=divieto di pubblicizzare beni o servizi) / **interdizione dell'attività**: sospensione temporanea (da 3 a 24 mesi) dell'attività; commissariamento o sospensione definitiva.

<b>R = P x M</b>	<b>RISCHIO RESIDUO (R)</b>					
<b>RISCHIO RESIDUO</b>	<p><b>R = P x M =</b> Valore di esposizione al rischio di commissione dei reati presupposto Per il calcolo del rischio residuo, il valutatore ha a disposizione la sola variabile Probabilità (P). La Magnitudo / Impatto (M) è definita sulla base delle sanzioni massime applicabili previste dal legislatore.</p>					
La matrice del rischio residuo nasce dal prodotto <b>R = P x M</b> e risulta avere dimensione 5x5.						
<b>MAGNITUDO</b>	Estrema (5)	5	10	15	20	25
	Molto Rilevante (4)	4	8	12	16	20
	Rilevante (3)	3	6	9	12	15
	Significativa (2)	2	4	6	8	10
	Bassa (1)	1	2	3	4	5
		(1)	(2)	(3)	(4)	(5)
		Raro	Improbabile	Moderato	Possibile	Probabile
		<b>PROBABILITA'</b>				
<b>MATRICE DEL RISCHIO RESIDUO</b>	<b>0 – 5</b>					
	<b>6 – 10</b>					
	<b>11 – 16</b>					
	<b>17-25</b>					

La soglia concettuale di accettabilità del rischio di commissione di reati dolosi è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non fraudolentemente.

La soglia concettuale di accettabilità va diversamente modulata in relazione al rischio di commissione di reati colposi ed è rappresentata dalla realizzazione di una condotta in violazione del modello organizzativo di prevenzione, nonostante l'efficace implementazione di un sistema preventivo, vale a dire la puntuale applicazione delle procedure idonee alla prevenzione delle fattispecie di reato e l'osservanza degli obblighi di vigilanza previsti dal D.Lgs. 231/2001.

In ragione della decisione assunta dal management aziendale sulla base dell'attività di *risk assessment*, la Società ha ritenuto applicabili, seppure con diversa graduazione del rischio, le categorie di reato presupposto 231 esaminate negli allegati di Parte Speciale.

Per le categorie di reato presupposto 231 indicate in documento di risk assesment come “non applicabili” (NA) alla Società o con presenza di presupposti insufficienti (PI), è stato ritenuto, in fase di autovalutazione dei rischi 231, che la specifica attività svolta dalla Fondazione non presenti profili di rischio tali da rendere ragionevolmente fondata la possibilità della loro commissione nell'interesse o a vantaggio dell'Ente.

In merito alla “non applicabilità” delle categorie di reato sopra riportate, si precisa che il presente Modello è stato elaborato a seguito di un'approfondita attività di *risk self assessment* che ha portato alla identificazione delle principali aree di rischio da parte del management aziendale.

Infatti il *risk self assessment* ha evidenziato l'opportunità di escludere la commissione di tali reati nell'ottica di predisporre un modello personalizzato sulle specificità della Fondazione.

Dal punto di vista normativo e metodologico, si precisano nel seguito alcune considerazioni di carattere generale relative all'approccio seguito nella autovalutazione dei rischi 231 e dell'applicabilità delle categorie di reati alla Fondazione.

Le disposizioni contenute nelle lettere a) e b) dell'art. 6, comma 2 del Decreto definiscono le esigenze cui devono rispondere i Modelli aziendali di organizzazione e gestione idonei alla prevenzione dei reati elencati in decreto. Le stesse richiedono, in particolare, che l'ente abbia a tal fine:

- individuato le aree nel cui ambito possono essere commessi i reati e, per l'effetto,
- previsto specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire.

Come indicato dalle Linee Guida di Confindustria, riferimento riconosciuto in materia, “L'art. 6, comma 2, del decreto 231 indica le caratteristiche essenziali per la costruzione di un modello di organizzazione, gestione e controllo. In particolare, le lettere a) e b) della disposizione si riferiscono espressamente ad alcune attività correlate ad un processo di sana e prudente gestione dei rischi. Ferma restando l'esigenza che ogni impresa costruisca e mantenga in efficienza il proprio sistema di gestione dei rischi e di controllo interno, anche in ottica di “compliance integrata”, le stesse propongono un approccio coerente con i principali framework di riferimento in tema di controllo interno e di gestione dei rischi”.

In tale contesto, l'Ente ha inteso elaborare il proprio MOG in linea con le Linee Guida di Confindustria, come espressamente riportato al §1.7 “Codici di comportamento predisposti dalle associazioni rappresentative di categoria”, e quindi svolgere un'attività di *risk self assessment* che ha visto il coinvolgimento di tutti i responsabili di funzione individuati in incontri nei quali è

stata auto valutata dal management e dalle rilevanti funzioni la rischiosità delle diverse categorie di reato alle specifiche attività di business in essere.

In aggiunta si rileva come la Relazione di Accompagnamento al Decreto legislativo 231/2001 evidenzia in maniera inequivoca che, ai fini della esclusione della responsabilità, all'ente viene richiesta l'adozione di **Modelli comportamentali specificamente calibrati sul rischio reato, e cioè volti ad impedire, attraverso la fissazione di regole di condotta, la commissione di determinati reati elencati nel medesimo Decreto.**

Si evidenzia pertanto come l'efficacia esimente del Modello 231 sia strettamente correlata alla personalizzazione dello stesso sulla specifica realtà aziendale, e pertanto la presenza nel Modello 231 della Società delle esclusioni di alcuni reati rappresenta la volontà e l'impegno della Società di adottare un **Modello 231 non generico ma derivante da un'analisi puntuale della realtà aziendale e dei reali rischi connessi in ambito 231.**

Per quanto attiene alla individuazione dei rischi di commissione dei reati nei singoli macro-processi e processi e alle funzioni coinvolte in ogni attività sensibile si rinvia all'allegato documento di "Risk Assessment".

Inoltre, al fine di semplificare la leggibilità del presente Modello rispetto all'Allegato precitato, si precisa che le attività sensibili sono state riportate in modo sintetico nel presente documento, lasciando un maggiore dettaglio negli allegati di parte speciale nell'Allegato A, a cui si rimanda.

## 6 L'ORGANISMO DI VIGILANZA

### 6.2 L'organismo di vigilanza di Fondazione Carige

In base alle previsioni del D.Lgs. 231/01 – art. 6, comma 1, lett. b), l'ente può essere esonerato dalla responsabilità conseguente alla commissione di reati da parte dei soggetti qualificati ex art. 5 del D.Lgs. 231/01, se l'organo dirigente ha, fra l'altro, affidato il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

L'affidamento dei suddetti compiti ad un organismo dotato di autonomi poteri di iniziativa e controllo, unitamente al corretto ed efficace svolgimento degli stessi rappresentano, quindi, presupposti indispensabili per l'esonero dalla responsabilità prevista dal D.Lgs. 231/01.

I requisiti principali dell'Organismo di Vigilanza (di seguito anche "OdV"), così come proposti dalle Linee guida per la predisposizione dei Modelli di Organizzazione e Gestione emanate da Confindustria e fatti propri anche dagli organi giudicanti nelle diverse pronunce giurisprudenziali pubblicate, possono essere così identificati:

- autonomia ed indipendenza;
- professionalità;
- continuità di azione.

L'autonomia e l'indipendenza dell'OdV si traducono nell'autonomia dell'iniziativa di controllo rispetto ad ogni forma d'interferenza o di condizionamento da parte di qualunque esponente della persona giuridica e, in particolare, dell'organo amministrativo.

Al fine di assicurare tali requisiti, l'OdV riporta esclusivamente al Presidente del Consiglio di Amministrazione e a quest'ultimo nel suo complesso. L'OdV deve altresì godere di garanzie tali

da impedire che lo stesso o alcuno dei suoi componenti possano essere rimossi o penalizzati in conseguenza dell'espletamento dei loro compiti.

Il requisito della professionalità si traduce nella capacità dell'OdV di assolvere alle proprie funzioni, rispetto all'effettiva applicazione del Modello, nonché nelle necessarie qualità per garantire la dinamicità del Modello medesimo, attraverso proposte di aggiornamento da indirizzare al vertice aziendale.

Con riferimento, infine, alla continuità di azione, l'OdV dovrà vigilare costantemente sul rispetto del Modello, verificare l'effettività e l'efficacia dello stesso, promuoverne il continuo aggiornamento e rappresentare un referente costante per ogni soggetto che presti attività lavorativa per la Società.

Il D.Lgs. 231/01 non fornisce indicazioni specifiche circa la composizione dell'organismo di vigilanza. In assenza di tali indicazioni, la Società deve optare per una soluzione che, tenuto conto delle finalità perseguite dalla legge e dagli indirizzi ricavabili dalla giurisprudenza espressasi sul tema, sia in grado di assicurare, in relazione alle proprie dimensioni ed alla propria complessità organizzativa, l'effettività dei controlli cui l'organismo di vigilanza è preposto. In considerazione di quanto sopra Fondazione Carige ha optato per una struttura collegiale del proprio Organismo di Vigilanza.

#### Principi generali in tema di istituzione, nomina e sostituzione dell'Organismo di Vigilanza

L'Organismo di Vigilanza della Società è istituito con delibera del Consiglio di Amministrazione e resta in carica per un periodo definito in sede di nomina da parte del Consiglio di Amministrazione. Il componente è rieleggibile. L'Organismo di Vigilanza cessa per scadenza del termine del periodo stabilito in sede di nomina, pur continuando a svolgere *ad interim* senza soluzione di continuità le proprie funzioni fino a nuova nomina. La nuova nomina è effettuata dal Consiglio di Amministrazione tempestivamente.

Il compenso per la qualifica di componente dell'Organismo di Vigilanza è stabilito, per tutta la durata del mandato, dal Consiglio di Amministrazione.

La nomina quale componente dell'Organismo di Vigilanza è condizionata alla presenza di requisiti soggettivi di eleggibilità.

In particolare, all'atto del conferimento dell'incarico, il soggetto designato a ricoprire la carica di componente dell'Organismo di Vigilanza attesta, anche per il tramite della accettazione dell'incarico, l'assenza di motivi di ineleggibilità quali:

- titolarità, diretta o indiretta, di partecipazioni al capitale sociale della Società di entità tale da permettere di esercitare una notevole influenza sulla Società;
- funzioni di amministrazione – nei tre esercizi precedenti alla nomina quale membro dell'Organismo di Vigilanza ovvero all'instaurazione del rapporto di consulenza/collaborazione con lo stesso Organismo – di imprese sottoposte a fallimento, liquidazione coatta amministrativa o altre procedure concorsuali;
- sentenza di condanna anche non passata in giudicato ed anche ai sensi dell'art. 444 c.p.p., in Italia o all'estero, per i delitti richiamati dal D.Lgs. 231/01 o delitti comunque incidenti sulla moralità professionale;
- stato di interdizione temporanea o di sospensione dagli uffici direttivi delle persone giuridiche e delle imprese;

- esistenza di una delle condizioni di ineleggibilità o decadenza previste dall'art. 2382 del codice civile;
- misure di prevenzione ai sensi della legge 27 dicembre 1956, n. 1423 o della legge 31 maggio 1965, n. 575 e successive modificazioni e integrazioni, salvi gli effetti della riabilitazione;
- condanna, ancorché con sentenza non ancora passata in giudicato e anche se con pena condizionalmente sospesa, nonché una sentenza di applicazione della pena su richiesta delle parti ai sensi dell'art. 444 c.p.p. (cosiddetto "patteggiamento"), salvi gli effetti della riabilitazione:
  - a pena detentiva per un tempo non inferiore ad un anno per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267;
  - a pena detentiva per un tempo non inferiore ad un anno per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;
  - a pena detentiva per un tempo non inferiore ad un anno per un reato contro la pubblica amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, per un delitto in materia tributaria;
  - per un qualunque delitto non colposo alla pena della reclusione per un tempo non inferiore ad un anno.

Laddove alcuno dei sopra richiamati motivi di ineleggibilità dovesse configurarsi a carico del soggetto nominato, questi decadrà automaticamente dalla carica.

L'Organismo di Vigilanza potrà giovare inoltre, sotto la sua diretta sorveglianza e responsabilità, della collaborazione di tutte le funzioni e strutture della Società ovvero di consulenti esterni, avvalendosi delle rispettive competenze e professionalità. Tale facoltà consente all'Organismo di Vigilanza di assicurare un elevato livello di professionalità e la necessaria continuità di azione.

A tal fine il Consiglio di Amministrazione assegna, ogni anno, un idoneo e autonomo fondo di dotazione all'Organismo di Vigilanza, su sua richiesta. L'assegnazione del fondo di dotazione permette all'Organismo di Vigilanza di operare in autonomia e con gli strumenti opportuni per un efficace espletamento del compito assegnatogli dal presente Modello, secondo quanto previsto dal D.Lgs. 231/01.

Il Fondo di dotazione si intende *rolling*, vale a dire che si ricostituisce automaticamente alla soglia indicata a seguito di ogni concreto utilizzo da parte dell'Organismo di Vigilanza, che verrà comunicato formalmente al Consiglio di Amministrazione.

In caso di necessità, l'Organismo di Vigilanza potrà richiedere al Consiglio di Amministrazione di disporre anche di cifre superiori, dandone adeguata rendicontazione successiva.

In caso di urgenza o di necessità connessa all'esercizio dei propri compiti, l'Organismo di Vigilanza potrà in ogni caso attivarsi autonomamente.

Al fine di garantire la necessaria stabilità all'Organismo di Vigilanza, la revoca dei poteri propri dell'Organismo di Vigilanza e l'attribuzione di tali poteri ad altro soggetto potrà avvenire soltanto per giusta causa, mediante un'apposita delibera del Consiglio di Amministrazione.

A tale proposito, per "giusta causa" di revoca dei poteri connessi con l'incarico di membro dell'Organismo di Vigilanza potrà intendersi, a titolo meramente esemplificativo:

- una grave negligenza nell'assolvimento dei compiti connessi con l'incarico;
- l'"omessa o insufficiente vigilanza" da parte dell'Organismo di Vigilanza, allo stesso addebitabile – secondo quanto previsto dall'art. 6, comma 1, lett. d), D.Lgs. 231/01 – risultante da una sentenza di condanna passata in giudicato, emessa nei confronti della Società ai sensi del D.Lgs. 231/01 ovvero da provvedimento che comunque ne accerti la responsabilità;
- la violazione della riservatezza del segnalante con riferimento alle disposizioni normative in materia di whistleblowing e alla procedura applicativa (si veda paragrafo 7);
- l'attribuzione di funzioni e responsabilità operative all'interno dell'organizzazione aziendale incompatibili con i requisiti di "autonomia e indipendenza" e "continuità di azione" propri dell'Organismo di Vigilanza.

In casi di particolare gravità, il Consiglio di Amministrazione potrà comunque disporre la sospensione dei poteri dell'Organismo di Vigilanza e la nomina di un Organismo *ad interim* oppure, disporre senza indugio, la revoca e la nomina di un nuovo Organismo di Vigilanza.

### **6.3 Funzioni e poteri dell'Organismo di Vigilanza**

Le attività poste in essere dall'Organismo di Vigilanza non possono essere sindacate da alcun altro organismo o struttura della Società, fermo restando che l'Organo Gestorio è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza dell'operato dell'OdV, in quanto lo stesso ha la responsabilità ultima del funzionamento e dell'efficacia del Modello.

All'Organismo di Vigilanza sono conferiti i poteri di iniziativa e controllo necessari per assicurare un'effettiva ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello secondo quanto stabilito dall'art. 6 del D.Lgs. 231/01.

Pertanto, a tale Organismo è affidato il compito di vigilare in generale:

- sulla reale efficacia del Modello rispetto all'esigenza di prevenire la commissione dei reati per cui trova applicazione il D.Lgs. 231/01;
- sull'osservanza delle prescrizioni del Modello da parte dei destinatari;
- sull'aggiornamento del Modello nel caso in cui si riscontrassero esigenze di adeguamento in relazione alle mutate condizioni aziendali o normative. A tale proposito si precisa che fra i compiti dell'Organismo vi è quello di suggerire eventuali proposte di adeguamento agli organi aziendali in grado di dare loro concreta attuazione e di seguirne il follow-up, al fine di verificare l'implementazione e l'effettiva funzionalità delle soluzioni proposte.

In particolare, all'Organismo di Vigilanza sono affidati, per l'espletamento e l'esercizio delle proprie funzioni, i seguenti compiti e poteri:

- convocare i responsabili delle funzioni aziendali che non potranno esimersi dal presentarsi, salvo giustificato motivo, per riferire su fatti ritenuti rilevanti;
- effettuare, direttamente o indirettamente, verifiche mirate su specifiche attività a rischio;
- promuovere l'aggiornamento della mappatura dei rischi in caso di significative variazioni organizzative o di estensione della tipologia di reati presi in considerazione dal D.Lgs. 231/01;

- verificare con le funzioni aziendali di riferimento l'adeguatezza della regolamentazione interna adottata e definire eventuali proposte di adeguamento e miglioramento (regole interne, procedure, modalità operative e di controllo) accertandone, successivamente, l'attuazione;
- monitorare le iniziative di informazione/formazione finalizzate alla diffusione della conoscenza e della comprensione del Modello in ambito aziendale;
- raccogliere e gestire le informazioni necessarie a fornire un quadro costantemente aggiornato circa l'attuazione del Modello;
- supervisionare il sistema di comunicazione interna per consentire la trasmissione di notizie rilevanti ai fini del D.Lgs. 231/01 garantendo la tutela e riservatezza del segnalante;
- esprimere, sulla base delle risultanze emerse dalle attività di verifica e di controllo, una valutazione periodica sul funzionamento e l'osservanza del Modello;
- segnalare, qualora opportuno, al CdA eventuali violazioni di protocolli e/o procedure o le carenze rilevate in occasione delle verifiche svolte, affinché questo possa adottare i necessari interventi di adeguamento coinvolgendo, ove necessario, il Consiglio di Amministrazione;
- proporre l'applicazione coerente delle sanzioni previste dalle normative interne nei casi di violazione del Modello, ferma restando la competenza dell'organo dirigente per l'applicazione dei provvedimenti sanzionatori;
- rilevare gli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni.

L'Organismo di Vigilanza è tenuto al vincolo di riservatezza rispetto a tutte le informazioni di cui viene a conoscenza a causa dello svolgimento dell'incarico. La divulgazione di tali informazioni potrà essere effettuata solo ai soggetti e con le modalità previste dal presente Modello.

#### **6.4 Obblighi di informazione nei confronti dell'Organismo di Vigilanza – Flussi informativi**

L'OdV deve essere tempestivamente informato, in merito ad atti, comportamenti od eventi che possano determinare una violazione del Modello o che, più in generale, siano rilevanti ai fini del D.Lgs. 231/01.

Le informazioni che debbono essere inviate da e in favore di OdV sono espressamente disciplinate da apposita Procedura Flussi Informativi.

Si ritiene in ogni caso puntualizzare anche nella presente Parte Generale del Modello quanto di seguito.

Ciascun Destinatario del presente Modello è tenuto a segnalare eventuali violazioni o sospetti di violazione del Codice Etico o dei principi di controllo previsti nel Modello stesso (c.d. "segnalazioni").

Oltre alle segnalazioni di cui sopra, devono essere obbligatoriamente trasmesse all'Organismo di Vigilanza le informazioni concernenti (c.d. "informazioni"):

##### **Salute e Sicurezza sul Lavoro**

- resoconto della formazione dei lavoratori in relazione alla normativa in materia di igiene e sicurezza sul lavoro;

- le nomine effettuate in ambito Salute e Sicurezza sul Lavoro;
- resoconto dell'attività di monitoraggio;
- resoconto delle eventuali prescrizioni e sanzioni impartite dagli organi ispettivi in materia di sicurezza;
- le attività di sorveglianza sanitaria e le eventuali richieste provenienti dall'INAIL in merito alle denunce di malattie professionali;
- il programma e il resoconto delle attività di Vigilanza Antinfortunistica;
- copia dei verbali delle riunioni periodiche di cui all'art. 35 del D.Lgs. 81/08;
- le segnalazioni di infortuni gravi occorsi a chiunque acceda nei luoghi di lavoro della Società e le segnalazioni di anomalie e criticità riscontrate;

#### *Ambiente*

- resoconto della formazione dei lavoratori in materia ambientale;
- le nomine effettuate nell'ambito del Sistema di Gestione Ambientale;
- resoconto delle eventuali prescrizioni e sanzioni impartite dagli organi ispettivi in materia di tutela dell'ambiente;
- le segnalazioni di incidenti e quasi-incidenti ambientali ed eventuali anomalie o criticità riscontrate nello svolgimento delle attività sensibili con riferimento all'Ambiente;

#### *Legale e Societario*

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal D.Lgs. 231/2001 e che possano coinvolgere la Società;
- riepilogo delle modifiche al sistema di deleghe e procure adottato dalla Società;

#### *Audit*

- resoconto dei rapporti di audit inerenti aree e/o processi sensibili ai sensi del Decreto;

#### *Amministrazione e Finanza*

- riepilogo delle richieste, l'eventuale erogazione ed utilizzo di finanziamenti pubblici.

#### *Comunicazione*

- resoconto delle donazioni e sponsorizzazioni erogate;

#### *Risorse umane*

- riepilogo delle modifiche organizzative e societarie;
- riepilogo delle notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate ovvero ai provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, con particolare riferimento ai reati ex D.Lgs. 231/01;
- resoconto della formazione in materia 231 erogata.

Restano salvi i flussi informativi "ad evento", che vanno tempestivamente segnalati all'Organismo di Vigilanza, a prescindere dalla periodicità programmata, al verificarsi di circostanze che possano

avere rilevanza ai fini della efficace attuazione del Modello organizzativo e delle misure di prevenzione in esso previste.

Il Consiglio di Amministrazione dovrà informare l'Organismo di Vigilanza in merito ad eventuali delibere aventi ad oggetto situazioni rilevanti ai sensi del D.Lgs. 231/01.

#### Raccolta e conservazione delle informazioni

Ogni informazione, segnalazione, *report*, relazione previsti nel Modello sono conservati dall'Organismo di Vigilanza in un apposito archivio riservato (informatico o cartaceo) per un periodo di dieci anni.

L'accesso ai dati è consentito esclusivamente all'Organismo di Vigilanza ed a persone da questi delegate e autorizzate.

### **6.5 Reporting dell'Organismo di Vigilanza verso gli organi societari**

L'Organismo di Vigilanza riferisce in merito all'osservanza del Modello, all'emersione di eventuali aspetti critici e alla necessità di aggiornamento. A tal fine, l'Organismo di Vigilanza predispone:

- con cadenza annuale, una relazione informativa, relativa all'attività svolta da presentare al Consiglio di Amministrazione; in alternativa può partecipare direttamente alla seduta di CDA al fine di relazionare l'organo gestorio in merito allo stato di attuazione del MOG ed alle attività svolte;
- al verificarsi di violazioni accertate del Modello, con presunta commissione di reati, una comunicazione da presentare al Presidente del Consiglio di Amministrazione.

L'Organismo di Vigilanza ha comunque la facoltà di richiedere la propria audizione al Consiglio di Amministrazione, qualora ne ravvisi la necessità.

Allo stesso modo, il Consiglio di Amministrazione ha facoltà di convocare l'Organismo di Vigilanza qualora lo ritenga opportuno.

Nell'ambito del *reporting* annuale vengono affrontati i seguenti aspetti:

- controlli e verifiche svolti dall'Organismo di Vigilanza ed esito degli stessi;
- stato di avanzamento di eventuali progetti di implementazione/revisione di processi sensibili;
- eventuali innovazioni legislative o modifiche organizzative che richiedano aggiornamenti nell'identificazione dei rischi o variazioni del Modello;
- eventuali sanzioni disciplinari irrogate dagli organi competenti a seguito di violazioni del Modello;
- eventuali segnalazioni ricevute da soggetti interni ed esterni nel corso del periodo in ordine a presunte violazioni al Modello o al Codice Etico;
- altre informazioni ritenute significative;
- valutazione di sintesi sull'aggiornamento ed effettiva applicazione del Modello.

## **7 WHISTLEBLOWING**

In data 29 dicembre 2017 è entrata in vigore la Legge 30 novembre 2017, n. 179 recante le "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a

conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" che è intervenuta sull'art. 54-bis del D. Lgs. n. 165/2001 e sull'art. 6 del D. Lgs. n. 231/2001.

Il Legislatore, nel tentativo di armonizzare le disposizioni previste per il settore pubblico con la richiamata Legge, ha introdotto specifiche previsioni per gli enti destinatari del D. Lgs. n. 231/2001 ed ha inserito all'interno dell'art. 6 del D. Lgs. n. 231/2001 tre nuovi commi, ovvero il comma 2-bis, 2-ter e 2-quater.

In particolare l'art. 6 dispone:

- al comma 2-bis che i Modelli di Organizzazione, Gestione e Controllo devono prevedere:
  - uno o più canali che consentano ai soggetti indicati nell'art. 5, comma 1, lettere a) e b)<sup>1</sup>, di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del Decreto e fondate su elementi di fatto precisi e concordanti, ovvero di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;
  - almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
  - il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
  - nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate;
- al comma 2-ter prevede che l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2-bis può essere denunciata all'Ispettorato del Lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo;
- al comma 2-quater è disciplinato il licenziamento ritorsivo o discriminatorio del soggetto segnalante, che viene espressamente qualificato come "nullo". Sono altresì indicati come nulli il mutamento di mansioni ai sensi dell'art. 2103 c.c., nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante.

Il predetto articolo, inoltre, prevede che in caso di controversie legate all'erogazione di sanzioni disciplinari, demansionamenti, licenziamenti, trasferimenti ovvero sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi sulle condizioni di lavoro, spetta al datore di lavoro provare che tali misure siano state adottate sulla base di ragioni estranee alla segnalazione.

La Legge sul *whistleblowing* introduce nell'ordinamento giuridico italiano un apparato di norme volto a migliorare l'efficacia degli strumenti di contrasto ai fenomeni corruttivi, nonché a tutelare con maggiore intensità gli autori delle segnalazioni incentivando il ricorso allo strumento della denuncia di condotte illecite o di violazioni dei modelli di organizzazione, gestione e controllo

---

<sup>1</sup> Art. 5, D. Lgs. n. 231/2001: (...) a) persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

gravando il datore di lavoro dell'onere di dimostrare - in occasione di controversie legate all'irrogazione di sanzioni disciplinari, demansionamenti, licenziamenti, trasferimenti o alla sottoposizione del segnalante ad altra misura organizzativa successiva alla presentazione della segnalazione avente effetti negativi, diretti o indiretti, sulla condizione di lavoro - che tali misure risultino fondate su ragioni estranee alla segnalazione stessa (c.d. "*inversione dell'onere della prova a favore del segnalante*").

Da ultimo il D. Lgs. 10 marzo 2023 n. 24 (pubblicato sulla Gazzetta Ufficiale del 14 marzo 2023 n. 63), d'ora in poi, per brevità, anche solamente "**Decreto**", integra il provvedimento con cui l'Italia ha recepito in via definitiva la Direttiva UE n. 1937/2019 (c.d. "**Direttiva Whistleblowing**").

Il Decreto ha abrogato e modificato la normativa previgente, disciplinando in un unico provvedimento, valido in Italia sia per il settore pubblico che per il settore privato, il regime di protezione dei soggetti che segnalano condotte illecite, le quali integrino violazione di disposizioni europee e nazionali.

Le principali novità introdotte dal Decreto attengono:

- (i) all'ambito soggettivo di applicazione, con ampliamento dei soggetti legittimati ad effettuare le segnalazioni e assoggettati alle tutele ivi sancite;
- (ii) all'ambito oggettivo di applicazione. La normativa definisce "**Violazioni**" tutti quei comportamenti, atti od omissioni che siano idonei a ledere l'interesse pubblico o l'integrità della Società, di cui i *whistleblowers* siano venuti a conoscenza nell'ambito del contesto lavorativo riferito alle Società del Gruppo nel perimetro della presente Procedura, e che consistono in:
  - illeciti amministrativi, contabili, civili o penali;
  - condotte illecite rilevanti ai sensi del D.Lgs 231/2001 o violazioni dei Modelli Organizzativi;
  - illeciti richiamati e indicati nel D.Lgs. 24/2023, a titolo esemplificativo e non esaustivo riguardanti i seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei 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;
  - atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'articolo 325 del Trattato sul funzionamento dell'Unione europea specificati nel diritto derivato pertinente dell'Unione europea;
  - atti od omissioni riguardanti il mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;
  - atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori sopra richiamati.

Fondazione Carige ha, conseguentemente, provveduto ad adottare una piattaforma informatica la Procedura Whistleblowing, pubblicata sul sito web aziendale, con cui vengono esplicitate:

- le modalità di utilizzo di canali informativi che consentono di presentare, a tutela dell'integrità della Società, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del Decreto e fondate su elementi di fatto precisi e concordanti, ovvero di violazioni del Modello stesso, di cui i segnalanti siano venuti a conoscenza in ragione delle funzioni svolte. Tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;
- l'individuazione di un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
- le modalità di gestione delle segnalazioni ricevute, in termini di protocollazione, analisi preliminare, accertamento, comunicazione degli esiti, archiviazione, etc;
- le modalità di gestione delle segnalazioni, che pervengono dall'Organismo di Vigilanza, da parte di Organi o Strutture aziendali laddove si presentino eventi con possibili implicazioni di natura disciplinare.

## **7.2 La procedura di “Gestione delle segnalazioni all’Organismo di Vigilanza di violazioni sospette del Modello Organizzativo 231” (whistleblowing)**

Come anticipato le modalità per effettuare le segnalazioni e le modalità di gestione debbono essere conformi alle indicazioni di cui al Decreto 24/2023 e le successive Linee Guida Anac 311/2023, distinguendo fasi e responsabilità, eventualmente con una procedura *ad hoc*.

Per quanto riguarda i profili più operativi, la legge prevede che i canali destinati a veicolare le segnalazioni garantiscano la riservatezza dell'identità del denunciante nelle diverse fasi di gestione della denuncia e che, almeno uno di essi, provveda a tali garanzie con modalità informatiche.

In merito alla riservatezza dell'identità del segnalante, si evidenzia che occorre distinguere questo profilo da quello dell'anonimato: infatti per garantire al denunciante una tutela adeguata, anche in termini di riservatezza dell'identità, è necessario che esso sia riconoscibile. Ciò non esclude che i modelli organizzativi possano contemplare anche canali per effettuare segnalazioni in forma anonima. Tale ipotesi, in linea di principio, sembra rendere più complessa la verifica della fondatezza della denuncia, con il rischio di alimentare denunce infondate e mere doglianze che si discostano dall'obiettivo di tutelare l'integrità dell'ente. In ogni caso, per contenere questo rischio si può valutare l'adozione di specifiche misure per l'ipotesi di segnalazioni anonime: per rafforzarne il fondamento, ad esempio, si può prevedere che esse siano documentate adeguatamente ovvero rese con dovizia di particolari e “*in grado di far emergere fatti e situazioni relazionandoli a contesti determinati*” (come precisato altresì dall'Autorità Nazionale Anticorruzione: v. Determinazione ANAC n. 6 del 28 aprile 2015 – “*Linee Guida in materia di tutela del dipendente pubblico che segnala illeciti*”). Nell'ambito delle Linee Guida adottate nel 2015 sul whistleblowing nel settore pubblico, l'ANAC ha formulato anche alcuni principi di carattere generale che possono essere utilmente consultati anche dal settore privato, nei limiti della compatibilità con la specifica disciplina prevista dalla legge n. 179/2017. In particolare, si fa riferimento alle misure per la tutela della riservatezza dell'identità del segnalante e agli aspetti più operativi, attinenti ai requisiti che i sistemi informatici dovrebbero avere per attuare il complessivo sistema di gestione delle segnalazioni, garantendo la sicurezza delle informazioni. In quest'ottica, le Linee Guida dell'ANAC raccomandano anche di svolgere in via preliminare l'analisi dei rischi nella gestione delle informazioni e dei dati che potrebbero essere trattati nel corso della procedura, con l'obiettivo di individuare misure di sicurezza adeguate a garantirne la riservatezza,

l'integrità e la disponibilità. Le misure raccomandate dall'ANAC sono i protocolli standard per il trasporto dei dati e gli strumenti di crittografia end-to-end per i contenuti delle segnalazioni e dei documenti allegati. Allo stesso modo, sarà utile riferirsi anche alle nuove Linee Guida sulle procedure per la presentazione e la gestione delle segnalazioni che l'ANAC è tenuta ad adottare in attuazione della legge n. 179/17 (art. 1, co. 5), che *“prevedono l'utilizzo di modalità anche informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e per il contenuto delle segnalazioni e della relativa documentazione”*. Sotto il profilo dei possibili canali attivabili, uno di essi deve *“garantire, con modalità informatiche, la riservatezza dell'identità del segnalante”*: tali modalità possono essere realizzate, ad esempio, attraverso l'utilizzo di piattaforme informatiche anche gestite da terze parti indipendenti e specializzate, oltre che con l'attivazione di caselle di posta elettronica dedicate. L'altro canale può consistere, sempre in via esemplificativa, nel servizio postale ordinario ovvero nel deposito fisico presso cassette *ad hoc*. È quindi fondamentale che la definizione della policy in materia di *whistleblowing* proceda di pari passo con la predisposizione degli strumenti informatici di supporto.

Inoltre, l'attuazione delle misure prescritte dalla nuova normativa *whistleblowing* nei modelli organizzativi 231 dovrà tenere conto delle implicazioni a livello di privacy, anche alla luce dell'entrata in vigore del Regolamento (UE) 2016/679, c.d. GDPR.

In linea con lo spirito della nuova disciplina, si prevede che il modello organizzativo stabilisca il divieto di atti discriminatori nei confronti dei *whistleblowers*. Inoltre, il sistema disciplinare deve indicare le misure sanzionatorie da applicare ai casi sia di violazione degli obblighi di riservatezza e del divieto degli atti ritorsivi o discriminatori appena richiamati, sia di segnalazioni infondate effettuate con dolo o colpa grave. Questa impostazione adottata in via definitiva con la legge n. 179/17 rafforza l'efficacia deterrente del sistema disciplinare che risultava, invece, depotenziata nella precedente formulazione del provvedimento, focalizzata soltanto sulle sanzioni a tutela dei soggetti segnalanti. In parallelo, la legge n. 179/17 integra l'articolo 6 del decreto 231 con due ulteriori disposizioni. Il comma 2-ter prevede che il segnalante e l'organizzazione sindacale di riferimento possono denunciare all'Ispettorato Nazionale del Lavoro le misure discriminatorie eventualmente adottate dall'ente. Il comma 2-quater, come sopra anticipato, sancisce in via espressa la nullità delle misure ritorsive o discriminatorie, inclusi il licenziamento e il mutamento di mansioni, assunte nei confronti del soggetto segnalante.

### **7.3 Ambito di applicazione della procedura di whistleblowing e canali per le segnalazioni**

La procedura adottata da Fondazione Carige è volta a regolamentare, incentivare e proteggere, chi, nello svolgimento delle proprie mansioni lavorative, venendo a conoscenza di una “violazione” (come definita) provvede alla sua denuncia.

Non saranno meritevoli di segnalazione, invece, questioni di carattere personale del segnalante, rivendicazioni o istanze attinenti alla disciplina del rapporto di lavoro o rapporti con il superiore gerarchico o con i colleghi.

Le segnalazioni devono fornire elementi utili a consentire ai soggetti preposti di procedere alle dovute e appropriate verifiche ed accertamenti.

Le caratteristiche di segnalazione sono le seguenti:

- la segnalazione può essere fatta dai dipendenti di Fondazione Carige e dai dipendenti e collaboratori delle imprese fornitrici della stessa;
- il segnalante non può essere sanzionato, demansionato, licenziato, trasferito o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro

determinata dalla segnalazione di condotte illecite di cui è venuto a conoscenza in ragione del proprio rapporto di lavoro;

- le tutele del segnalante non sono garantite nei casi in cui sia accertata la responsabilità penale del segnalante per i reati di calunnia o diffamazione;
- la segnalazione viene fatta attraverso la piattaforma informatica, adottata dalla Fondazione, e può essere inviata in forma anonima. Se anonima, sarà presa in carico solo se adeguatamente circostanziata.
- la segnalazione viene ricevuta OdV e gestita mantenendo il dovere di confidenzialità nei confronti del segnalante.
- la segnalazione può essere fatta da qualsiasi dispositivo digitale (pc, tablet, smartphone) sia dall'interno della Società che dal suo esterno. La tutela dell'anonimato è garantita in ogni circostanza.

### **7.3.1 Il Canali di Segnalazione Interno: la Piattaforma Whistleblowing**

Si rinvia per ogni approfondimento in merito ai canali di segnalazione, all'ambito soggettivo ed oggettivo di applicazione ed alle tutele garantite in capo al Segnalante ed ai Facilitatori alla Procedura Whistleblowing in vigore.

Il link per effettuare la segnalazione è pubblicato sul sito web aziendale.

## **8 SISTEMA DISCIPLINARE E SANZIONATORIO**

### **8.2 Funzione del sistema disciplinare**

L'art. 6, comma 2, lett. e) e l'art. 7, comma 4, lett. b) del D.Lgs. 231/01 indicano, quale condizione per un'efficace attuazione del modello di organizzazione, gestione e controllo, l'introduzione di un sistema idoneo a sanzionare il mancato rispetto delle misure indicate nel modello stesso.

Pertanto, la definizione di un adeguato sistema disciplinare e sanzionatorio, con sanzioni proporzionate alla gravità della violazione rispetto alle infrazioni delle regole di cui al presente Modello da parte dei Destinatari, costituisce un presupposto essenziale per l'efficacia del modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/01.

Le sanzioni previste saranno applicate ad ogni violazione delle disposizioni contenute nel Modello, a prescindere dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria, nel caso in cui il comportamento da censurare integri gli estremi di una fattispecie di reato rilevante ai sensi del D.Lgs. 231/01.

In ogni caso, la sanzione prescinde dalla commissione del reato e si attesta come reazione della Società al mancato rispetto di procedure o regole comportamentali richiamate dal Modello.

### **8.3 Misure nei confronti di lavoratori subordinati non dirigenti**

L'osservanza delle disposizioni e delle regole comportamentali previste dal Modello costituisce adempimento da parte dei dipendenti della Società degli obblighi previsti dall'art. 2104, comma 2 c.c. e dalla normativa di cui al CCNL di riferimento; obblighi dei quali il contenuto del medesimo Modello rappresenta parte sostanziale ed integrante.

Ne consegue che la violazione delle singole disposizioni e regole comportamentali previste dal Modello da parte dei dipendenti della Società costituisce sempre illecito disciplinare.

La predeterminazione delle norme sostanziali e procedurali, ossia dei fatti disciplinari rilevanti, delle sanzioni corrispondenti a tali fatti e delle procedure di contestazione delle sanzioni irrogate è affidata al Contratto collettivo di lavoro applicato nella Società e vigenti alla data della violazione.

I provvedimenti disciplinari e sanzionatori sono irrogabili nei confronti dei lavoratori dipendenti in conformità a quanto previsto dall'art. 7 della legge 20 maggio 1970, n. 300 (c.d. "Statuto dei Lavoratori"), dal CCNL di riferimento ed eventuali normative speciali applicabili.

Per i dipendenti di livello non dirigenziale, tali provvedimenti sono quelli previsti dalle norme disciplinari di cui al rispettivo CCNL e dai codici disciplinari applicati.

Costituisce pertanto illecito disciplinare ogni violazione delle regole previste dal Modello o da questo richiamate e, in ogni caso, la commissione (anche sotto forma di tentativo) di qualsiasi illecito penale per cui è applicabile il D.Lgs. 231/01.

In particolare si applicano i seguenti provvedimenti.

Incorre nei provvedimenti di rimprovero, multa, sospensione o trasferimento (ove previsto), il dipendente che violi le procedure interne previste o richiamate dal presente Modello - ad esempio non osserva le procedure prescritte, omette di dare comunicazione all'Organismo di Vigilanza delle informazioni prescritte, omette di svolgere controlli - o adotti, nell'espletamento di attività sensibili, un comportamento non conforme alle prescrizioni del Modello stesso. La sanzione sarà commisurata alla gravità dell'infrazione e alla reiterazione della stessa (della recidiva si terrà conto anche ai fini della commisurazione di una eventuale sanzione espulsiva).

Costituiscono comunque grave trasgressione, ove non si configuri un comportamento sanzionabile con uno dei provvedimenti di cui ai punti successivi, i seguenti comportamenti:

- l'inadempimento degli obblighi di "segnalazione" e di "informazione" nei confronti dell'Organismo di Vigilanza previsti dal paragrafo 6.4;
- la non giustificata o sistematica mancata partecipazione alle iniziative di formazione in tema 231, promosse dalla Società;
- il mancato rispetto delle regole generali di comportamento;
- il mancato rispetto dei protocolli specifici di controllo previsti per le attività sensibili nella parte speciale del presente Modello ed i relativi flussi informativi;
- la messa in atto di azioni o comportamenti non conformi a quanto previsto dalla Legge sul *whistleblowing*.

Incorre nel provvedimento di licenziamento con preavviso, il dipendente che adotti nell'espletamento delle attività sensibili un comportamento non conforme alle prescrizioni del Modello e diretto in modo univoco al compimento di un reato sanzionato dal D.Lgs. 231/2001.

Incorre nel provvedimento di licenziamento senza preavviso il dipendente che adotti, nell'espletamento delle Attività sensibili un comportamento palesemente in violazione delle prescrizioni del Modello, tale da determinare la concreta applicazione a carico dell'Ente di misure previste dal D.Lgs. 231/2001.

Ad ogni notizia di violazione del Modello, verrà promossa un'azione disciplinare finalizzata all'accertamento della violazione stessa. In particolare, nella fase di accertamento verrà previamente contestato al dipendente l'addebito e gli sarà, altresì, garantito un congruo termine di replica in ordine alla sua difesa. Una volta accertata la violazione, sarà comminata all'autore

una sanzione disciplinare proporzionata alla gravità della violazione commessa ed all'eventuale recidiva.

Resta inteso che saranno in ogni caso rispettate le procedure, le disposizioni e le garanzie previste dall'art. 7 dello Statuto dei Lavoratori e dalla normativa pattizia in materia di provvedimenti disciplinari.

Per quanto concerne l'accertamento delle infrazioni concernenti il presente Modello, i procedimenti disciplinari e la comminazione delle sanzioni restano validi i poteri già conferiti, nei limiti delle rispettive deleghe e competenze.

Le sanzioni e l'eventuale risarcimento del danno sono commisurate al livello di responsabilità e autonomia del dipendente, all'eventuale esistenza di precedenti disciplinari a carico dello stesso, all'intenzionalità o al grado di colpa riferibile al suo comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui l'azienda può ragionevolmente ritenersi esposta – ai sensi e per gli effetti del D.Lgs. 231/2001 – a seguito della condotta censurata.

Il sistema disciplinare viene continuamente monitorato dalla funzione "Personale" con il supporto, qualora necessario, dell'Organismo di Vigilanza.

Ai dipendenti verrà data immediata e diffusa informazione circa l'introduzione delle nuove disposizioni.

Ogni atto relativo al procedimento disciplinare dovrà essere comunicato all'Organismo di Vigilanza per le valutazioni ed il monitoraggio di sua competenza.

#### **8.4 Misure nei confronti dei dirigenti**

In caso di violazione del Modello organizzativo da parte del dirigente (figura allo stato non presente in Fondazione), l'Ente provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dalla vigente normativa e dal CCNL applicabile.

A titolo esemplificativo, costituiscono infrazioni:

- la commissione (anche sotto forma di tentativo) di qualsiasi illecito penale per cui è applicabile il D.Lgs. 231/01;
- l'inosservanza delle regole prescritte dal Modello;
- la mancata vigilanza sui sottoposti circa il rispetto del Modello e delle regole da esso richiamate;
- l'inadempimento degli obblighi di "segnalazione" e di "informazione" nei confronti dell'Organismo di Vigilanza;
- la tolleranza od omessa segnalazione di irregolarità commessa da altri prestatori di lavoro o partner della Società;
- la messa in atto di azioni o comportamenti non conformi a quanto previsto dalla Legge sul *whistleblowing* e della *procedura applicativa*.

In ogni caso, se la violazione del Modello fa venire meno il rapporto di fiducia, la sanzione è individuata nella risoluzione del rapporto di lavoro.

Ogni atto relativo al procedimento sanzionatorio dovrà essere comunicato all'Organismo di Vigilanza per le valutazioni ed il monitoraggio di sua competenza.

### **8.5 Misure nei confronti degli Amministratori e del Collegio Sindacale**

L'Organismo di Vigilanza, raccolta una notizia di violazione delle disposizioni e delle regole di comportamento del Modello da parte di membri del Consiglio di Amministrazione, dovrà tempestivamente informare dell'accaduto il Presidente del Consiglio di Amministrazione. I soggetti destinatari dell'informativa dell'Organismo di Vigilanza, valutata la fondatezza della segnalazione ed effettuati i necessari accertamenti, potranno assumere, secondo quanto previsto dallo Statuto, gli opportuni provvedimenti tra cui, se del caso, la convocazione del Consiglio di Indirizzo, al fine di adottare le misure più idonee previste dalla legge.

Si specifica, a titolo esemplificativo, che costituisce violazione dei doveri degli amministratori:

- la commissione, anche sotto forma di tentativo, di un reato per cui è applicabile il D.Lgs. 231/01 nell'espletamento delle proprie funzioni;
- l'inosservanza delle regole prescritte dal Modello;
- la mancata vigilanza sui prestatori di lavoro o partner della Società circa il rispetto del Modello e delle regole da esso richiamate;
- l'inadempimento degli obblighi di "segnalazione" nei confronti dell'Organismo di Vigilanza;
- la messa in atto di azioni o comportamenti non conformi a quanto previsto dalla Legge sul *whistleblowing* e della *procedura applicativa*;
- tolleranza di irregolarità commessa da prestatori di lavoro o partner della Società.

Ogni atto relativo al procedimento sanzionatorio dovrà essere comunicato all'Organismo di Vigilanza per le valutazioni ed il monitoraggio di sua competenza.

L'Organismo di Vigilanza, raccolta una notizia di violazione delle disposizioni e delle regole di comportamento del Modello da parte del Collegio Sindacale dovrà tempestivamente informare dell'accaduto il Presidente del Consiglio di Amministrazione. Il destinatario dell'informativa dell'Organismo di Vigilanza, valutata la fondatezza della segnalazione ed effettuati i necessari accertamenti, potrà assumere, secondo quanto previsto dallo Statuto e dalla Legge, gli opportuni provvedimenti tra cui, ad esempio, la convocazione del CdA, al fine di adottare le misure più idonee previste dalla legge.

### **8.6 Misure nei confronti di partner commerciali, consulenti e collaboratori esterni**

L'adozione - da parte di *partner* commerciali, fornitori, consulenti e collaboratori esterni, comunque denominati, o altri soggetti aventi rapporti contrattuali con la Società - di comportamenti in contrasto con i principi ed i valori contenuti nel Codice Etico sarà sanzionata secondo quanto previsto nelle specifiche clausole contrattuali che saranno inserite nei relativi contratti.

La violazione grave o reiterata dei principi contenuti nel Codice Etico sarà considerato inadempimento degli obblighi contrattuali e potrà dar luogo alla risoluzione del contratto da parte della Società.

### **8.7 Sanzioni applicabili ai destinatari delle segnalazioni ("Whistleblowing")**

La Società, in caso di violazione delle disposizioni normative in materia di *whistleblowing* al fine di tutelare l'identità del segnalante e lo stesso da eventuali atti di ritorsione o discriminazione,

potrà applicare le seguenti sanzioni nei confronti dell'OdV: nell'ipotesi in cui l'OdV dovesse violare la riservatezza dell'identità del segnalante, il CDA potrà procedere con la revoca dell'incarico.

## 9 FORMAZIONE E COMUNICAZIONE

### 9.2 Premessa

La Società, al fine di dare efficace attuazione al Modello, assicura una corretta divulgazione dei contenuti e dei principi dello stesso, oltre che di quelli del Codice Etico, all'interno ed all'esterno della propria organizzazione.

L'attività di comunicazione e formazione è diversificata a seconda dei destinatari cui essa si rivolge, ma deve essere, in ogni caso, erogata a tutti i dipendenti, improntata a principi di completezza, chiarezza, accessibilità e continuità al fine di consentire ai diversi destinatari la piena consapevolezza di quelle disposizioni aziendali che sono tenuti a rispettare e delle norme etiche che devono ispirare i loro comportamenti. In particolare, l'attività di formazione è finalizzata a promuovere la conoscenza della normativa di cui al D. Lgs. n. 231/01 nonché della disciplina concernente il whistleblowing anche al fine di sviluppare una corretta cultura aziendale.

L'attività di comunicazione e formazione (ivi compreso il piano di formazione) è supervisionata dall'Organismo di Vigilanza che potrà proporre eventuali integrazioni ritenute utili.

In particolare l'approvazione da parte del Consiglio di Amministrazione delle versioni aggiornate del Modello viene comunicata a tutto il personale mediante emissione di specifici Ordini di Servizio all'interno dei quali i dipendenti vengono invitati alla consultazione del documento e viene loro ricordata la responsabilità dell'attuazione del Modello stesso, nell'ambito delle attività di propria competenza.

### 9.3 Dipendenti

Ogni dipendente è tenuto a acquisire consapevolezza dei contenuti del Modello messi a sua disposizione.

Deve essere garantita ai dipendenti la possibilità di accedere e consultare, anche sulla Intranet aziendale, la documentazione costituente il Modello ed i protocolli di controllo e le procedure aziendali ad esso riferibili. Inoltre, al fine di agevolare la comprensione del Modello, i dipendenti, con modalità diversificate secondo il loro grado di coinvolgimento nelle attività individuate come sensibili ai sensi del D.Lgs. 231/01, sono tenuti a partecipare alle specifiche attività formative che saranno promosse dalle competenti funzioni.

La Società garantisce l'organizzazione delle attività formative specifiche rivolte a tutti i dipendenti coinvolti nelle attività sensibili, con frequenza e contenuti idonei a garantire la conoscenza del Decreto e la diffusione del Modello. Le attività formative hanno carattere di obbligatorietà e devono essere documentate. Sono inoltre previsti controlli di frequenza e verifiche dell'apprendimento.

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

#### **9.4 Partner commerciali, consulenti e collaboratori esterni**

I partner commerciali, i fornitori, i consulenti e i collaboratori esterni sono rispettivamente informati dell'adozione, da parte della Società, del Codice Etico e dell'esigenza che il loro comportamento sia conforme ai principi etici e alle linee di condotta adottati da Fondazione Carige. La violazione del MOG può dare luogo alla risoluzione del contratto.

### **10 AGGIORNAMENTO DEL MODELLO**

Il Consiglio di Amministrazione delibera in merito all'aggiornamento del Modello ed al suo adeguamento in relazione a modifiche e/o integrazioni che si dovessero rendere necessarie in conseguenza di:

- modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa;
- cambiamenti delle aree di business;
- modifiche normative;
- risultanze dei controlli;
- significative violazioni delle prescrizioni del Modello.

Nel caso in cui si rendano necessarie modifiche di natura esclusivamente formale, quali chiarimenti o precisazioni del testo, l'amministratore delegato può provvedervi in maniera autonoma, dopo aver sentito il parere dell'OdV, riferendone senza indugio al Consiglio di Amministrazione.

In ogni caso, eventuali accadimenti riscontrati dall'OdV che rendano necessaria la modifica o l'aggiornamento del Modello devono essere segnalati dallo stesso al Consiglio di Amministrazione, affinché possa assumere le delibere di propria competenza.

Le modifiche delle procedure aziendali necessarie per l'attuazione del Modello avvengono ad opera delle funzioni interessate. L'OdV è costantemente informato dai responsabili delle funzioni aziendali in merito all'introduzione o agli aggiornamenti più significativi delle procedure operative.

Al fine della verifica e del monitoraggio in merito alla efficace attuazione delle procedure attuative del Modello 231 Fondazione Carige ha approntato il sistema di controlli già descritto nel presente modello ai fini della quantificazione del rischio residuo per le singole fattispecie di reato nel documento di *Risk Assessment*.

## 11 MATRICE DI RESPONSABILITA'

Nella matrice di seguito riportata vengono individuati, per immediata comprensione, i compiti e i comportamenti che la Società si aspetta dal proprio Organo Gestorio, dai dipendenti, dall'OdV e dalle terze parti.

TASKS PRINCIPALI	CdA	OdV	Resp. Funzione	Dipendenti	Terze parti
Adozione del MOG	<input type="checkbox"/>				
Vigilanza MOG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Accettazione MOG	<input type="checkbox"/>				
Nomina ODV	<input type="checkbox"/>				
Accettazione e messa in atto regole, adempimenti previsti nel rispetto delle <i>policies</i> e delle procedure di controllo	<input type="checkbox"/>				
Comunicazione e diffusione MOG		<input type="checkbox"/>	<input type="checkbox"/>		
Valutazione modifiche e adeguamento MOG		<input type="checkbox"/>	<input type="checkbox"/>		
Impulso a realizzazione nuove procedure finalizzate al rispetto dei contenuti del Decreto		<input type="checkbox"/>	<input type="checkbox"/>		
Approvazione modifiche MOG	<input type="checkbox"/>				
Segnalazione atto o attività che configuri un rischio reato	<input type="checkbox"/>				
Aggiornamento e formazione		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Occorre ribadire come, in una ottica di diffusione della "cultura 231", tutte le funzioni aziendali, coinvolte sin dalle attività propedeutiche alla emissione della revisione del Modello, sono costantemente chiamate e fornire il proprio supporto allo scopo di individuare processi e attività operative e di supporto, nel cui ambito possono realizzarsi le condotte illecite di natura finale e strumentale rispetto ai reati richiamati dal d.lgs. 231/01, nonché formulare suggerimenti per il miglioramento e l'implementazione delle procedure, con finalità di prevenzione della configurabilità delle fattispecie di reato.