

# MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

*(ai sensi del D.lgs. 231/2001)*

*COME - COMUNICAZIONE,  
EDITORIA & MEDIA S.R.L.*



## Indice degli Argomenti

1. **Parte Generale** (Pagina 3)
  - Premessa
  - Il regime di responsabilità amministrativa dipendente da reato a carico degli Enti
  - L'effetto dell'esenzione dalla responsabilità del MOGC 231/2001
  - Il Sistema Sanzionatorio
  - Reati commessi all'estero
  - Responsabilità da reato nei gruppi di imprese
  - Tentativo
  
2. **Il modello di Governance della Società** (Pagina 08)
  - Premessa
  - Le Linee Guida
  - Definizione del Modello
  - Sistema di controllo interno
  - Rapporti tra MOCG e Codice Etico
  
3. **Diffusione del Modello e Formazione** (Pagina 10)
  - Premesse
  - Diffusione tra le risorse interne alla Società
  - I soggetti terzi destinatari del Modello
  - La Formazione Interna ai soggetti destinatari del Modello
  
4. **Modifiche, Integrazioni e Verifiche Periodiche del Modello** (Pagina 12)
  - Modifiche e integrazioni del Modello
  - Verifica del Modello
  
5. **L'Organismo di Vigilanza** (Pagina 13)
  - Premessa
  - La nomina, composizione e durata dell'Organismo di Vigilanza
  - I requisiti dell'Organismo di Vigilanza
  - Le risorse dell'Organismo di Vigilanza
  - Le Funzioni dell'Organismo di Vigilanza
  - I poteri dell'Organismo di Vigilanza
  - Obblighi di informazione all'Organismo di Vigilanza
  - Obblighi di informative dell'Organismo di Vigilanza nei confronti degli organi sociali

## 6. Whistleblowing (Pagina 21)

- Premessa

## 7. Il Sistema Disciplinare e Sanzionatorio (Pagina 22)

- Premesse
- Definizione e Limiti della Responsabilità Disciplinare
- Destinatari e Loro Doveri
- Principi Generali Relativi alle Sanzioni
- Sanzioni nei Confronti di Dipendenti
- Misure nei Confronti dei Soggetti di cui all'art. 5, 1° comma, lett. a) D.Lgs. 231/01
- Disciplina nei Rapporti con Collaboratori Esterni e Partners

## 8. Parte Speciale (Pagina 25)

- Premessa
- Reati contro la Pubblica Amministrazione (pag. 28)
- Reati societari (pag. 39)
- Reati informatici (pag. 46)
- Reati associati (pag. 55)
- Reati di ricettazione, riciclaggio, impiego di denaro, beni o altre utilità di provenienza illecita e autoriciclaggio (pag. 57)
- Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare (pag. 61)
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (pag. 64)
- Reati contro la personalità individuale: Intermediazione illecita e sfruttamento del lavoro (pag. 65)
- Reati di xenofobia e razzismo (pag. 67)
- Reati di abuso di mercato (pag. 70)
- Delitti in materia di violazione del diritto d'autore (pag. 72)
- Reati tributari (pag. 76)
- Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento dei valori (pag. 82)

# PARTE GENERALE

## Premessa

In riferimento alla normativa sulla responsabilità amministrativa degli Enti, disciplinata dal Decreto Legislativo 231/2001, si rende opportuno adottare un Modello di Organizzazione, Gestione e Controllo (di seguito "Modello" o "MOGC") da parte delle Società e, più in generale, di tutti quegli Enti i cui processi possono esporre le persone e l'Ente medesimo alla commissione di reati ai sensi del su menzionato Decreto.

La società Comunicazione Editoria e Media S.r.l. opera come editore dell'Agenzia Dire, una delle principali agenzie di stampa nazionale, avendo recentemente acquisito in possesso il ramo d'azienda dalla capogruppo COM.E Comunicazioni & Editoria S.r.l., fondata nel 1988 e inizialmente focalizzata sull'analisi delle dinamiche politiche parlamentari e che nel corso del tempo si è affermata come una delle realtà più rilevanti nel panorama informativo italiano.

Questo Modello rappresenta un elemento fondamentale per la gestione aziendale, in quanto garantisce l'efficacia delle regole adottate dall'ente. Per assicurare che il MOGC sia efficace nella prevenzione dei reati e correttamente applicato, è essenziale che vengano formalizzati e documentati principi di comportamento e regole a cui i destinatari del Modello devono attenersi.

Conformemente alle linee guida suggerite dalle associazioni di settore, il MOGC si articola in una Parte Generale e in una Parte Speciale. La Parte Generale descrive l'ente, la sua organizzazione e le attività svolte, oltre a contenere elementi come il sistema disciplinare e il ruolo dell'Organismo di Vigilanza. La Parte Speciale, invece, individua i reati presupposto per l'ente, illustrandone le caratteristiche e delineando le misure di prevenzione del rischio. Queste ultime comprendono sia principi di condotta volti a prevenire la commissione di determinati reati, sia procedure specifiche applicabili alle aree aziendali classificate come "a rischio".

La Parte Speciale non fornisce una descrizione dettagliata delle procedure operative da seguire, ma rimanda alle specifiche Procedure 231 e ad altri documenti aziendali di sistema. Sebbene formalmente esterni al MOGC in senso stretto, questi documenti ne costituiscono parte integrante, evitando duplicazioni inutili e favorendo un'efficace applicazione delle procedure esistenti, le quali risultano più agevolmente fruibili in quanto specifiche per i singoli processi aziendali.

## 1. Il regime di responsabilità amministrativa dipendente da reato a carico degli Enti

L'esigenza di cui in premessa, nasce dall'entrata in vigore del Decreto Legislativo 8 giugno 2001, n. 231 (di seguito "Decreto" o "D.Lgs. 231/2001") il quale ha introdotto nel sistema giuridico italiano la responsabilità amministrativa degli enti per determinati reati commessi nel loro interesse o a loro vantaggio. Questo provvedimento si inserisce in un quadro normativo più ampio volto a contrastare la corruzione e ad allineare l'ordinamento italiano agli standard delle Convenzioni internazionali sottoscritte dal nostro Paese.

Tale responsabilità si aggiunge alla responsabilità personale dell'individuo che ha materialmente commesso il reato. Essa si configura nei casi in cui il reato venga perpetrato da un soggetto legato funzionalmente all'ente e finalizzato a trarne un vantaggio o un interesse diretto.

Gli autori dei reati presupposto possono essere:

- soggetti apicali, ossia coloro che ricoprono ruoli di rappresentanza, amministrazione o direzione all'interno dell'ente o di sue unità organizzative autonome;
- soggetti sottoposti, ovvero individui che operano sotto la direzione o vigilanza dei soggetti apicali.

Al fine di individuare e mitigare i rischi connessi ai reati previsti dal D.Lgs. 231/2001, Comunicazione, Editoria & Media S.r.l. ha condotto un'attenta attività di Risk Assessment con l'ausilio della società Aequa Consulting s.r.l. Questa analisi ha permesso di mappare i processi aziendali e i relativi protocolli, nonché di redigere una Matrice dei rischi lordi e netti.

Attraverso tale processo, sono stati individuati i reati presupposto astrattamente applicabili alla società, suddivisi nelle seguenti categorie:

1. Reati contro la Pubblica Amministrazione;
2. Reati societari;
3. Reati informatici;
4. Reati associativi;
5. Reati di ricettazione, riciclaggio e autoriciclaggio;
6. Impiego di cittadini stranieri in condizioni irregolari;
7. Induzione a rendere dichiarazioni mendaci;
8. Reati contro la personalità individuale, tra cui sfruttamento del lavoro;
9. Reati di xenofobia e razzismo;
10. Reati di abuso di mercato;
11. Violazione del diritto d'autore;
12. Reati tributari;
13. Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento dei valori

Tuttavia, il Modello non prevede specifici schemi di controllo per alcuni reati contemplati dal Decreto, in quanto non pertinenti alle attività di COME S.r.l. Tra questi vi sono reati transnazionali, ambientali, contrabbando, falso nummario, mutilazione degli organi genitali femminili e reati con finalità terroristiche. La remota possibilità che tali reati possano riguardare la società rende sufficiente l'adozione di principi di comportamento stabiliti nel Modello, nel Codice Etico e nelle procedure aziendali esistenti.

### **1.1 L'effetto dell'esenzione dalla responsabilità del MOGC 231/2001**

Ai sensi degli artt. 6 e 7 del D.Lgs. 231/2001, un ente può essere esentato dalla responsabilità amministrativa se dimostra di aver adottato ed efficacemente attuato un Modello idoneo a prevenire i reati della stessa natura di quello verificatosi.

L'esenzione è riconosciuta se:

- il Modello è stato adottato prima della commissione del reato;
- un Organismo di Vigilanza indipendente è stato incaricato di monitorarne l'applicazione;
- il reato è stato commesso eludendo fraudolentemente il Modello;
- non vi è stata negligenza o insufficiente vigilanza da parte dell'OdV.

Il Modello deve includere:

- una mappatura delle attività a rischio;
- protocolli per la formazione e l'attuazione delle decisioni;
- modalità di gestione delle risorse finanziarie atte a prevenire reati;
- un sistema disciplinare per sanzionare le violazioni.

## 1.2 Il Sistema Sanzionatorio

Le sanzioni applicabili a un Ente riconosciuto responsabile di un illecito amministrativo, accertato nell'ambito di un procedimento penale dal Giudice competente, includono:

- Sanzioni pecuniarie;
- Sanzioni interdittive;
- Confisca;
- Pubblicazione della sentenza.

La sanzione pecuniaria si applica in ogni caso di accertata responsabilità dell'Ente. Il suo ammontare viene determinato dal Giudice mediante un sistema di "quote", il cui numero deve essere compreso tra un minimo di 100 e un massimo di 1.000, con un valore unitario variabile tra 258 e 1.549 euro. Nel calcolare l'importo della sanzione, il Giudice valuta:

- Il numero delle quote, tenendo conto della gravità dell'illecito, del grado di responsabilità dell'Ente e delle eventuali misure adottate per mitigare le conseguenze dell'illecito e prevenirne di nuovi;
- L'ammontare della singola quota, sulla base della situazione economica e patrimoniale dell'Ente.

Le sanzioni interdittive, previste dall'art. 9, comma 2, del D.Lgs. 231/2001, possono consistere in:

- Interdizione dall'esercizio dell'attività;
- Sospensione o revoca di autorizzazioni, licenze o concessioni necessarie alla realizzazione dell'illecito;
- Divieto di stipulare contratti con la Pubblica Amministrazione, salvo quelli relativi a servizi pubblici essenziali;
- Esclusione dall'accesso a incentivi, finanziamenti, contributi o sussidi, con eventuale revoca di quelli già concessi;

- Divieto di promuovere beni o servizi.

Queste sanzioni si applicano solo nei casi in cui ciò sia espressamente previsto dalla normativa e quando si verifica almeno una delle seguenti condizioni:

- a) L'Ente ha tratto un vantaggio economico significativo dall'illecito, commesso da persone in posizione apicale o da soggetti subordinati qualora il reato sia stato favorito da gravi carenze organizzative;
- b) L'Ente è recidivo nella commissione di illeciti.

Il Giudice stabilisce il tipo e la durata della sanzione interdittiva, che può variare da un minimo di tre mesi a un massimo di due anni, valutandone l'efficacia nel prevenire reati analoghi. Se necessario, possono essere applicate più misure contemporaneamente (art. 14, commi 1 e 3, D.Lgs. 231/2001). Nei casi più gravi, le sanzioni di interdizione dall'attività, divieto di contrattare con la Pubblica Amministrazione e divieto di pubblicità possono essere imposte in via definitiva.

Esiste inoltre la possibilità che l'attività dell'Ente prosegua sotto la gestione di un commissario nominato dal Giudice, secondo le condizioni previste dall'art. 15 del D.Lgs. 231/2001, in alternativa all'applicazione della sanzione. Le sanzioni interdittive possono essere adottate anche come misure cautelari su richiesta del Pubblico Ministero, qualora sussistano gravi indizi di responsabilità dell'Ente (cd. "fumus boni iuris") e vi sia un concreto rischio di reiterazione di illeciti della stessa natura (cd. "periculum in mora"). In tali circostanze, il Giudice ne dispone l'applicazione tramite ordinanza.

Ai sensi dell'art. 19 del D.Lgs. 231/2001, la sentenza di condanna comporta sempre la confisca – anche per equivalente – del prezzo (somma di denaro o altro vantaggio economico promesso o dato per indurre qualcuno a commettere il reato) o del profitto (beneficio economico immediato derivante dall'illecito). Restano escluse le somme destinate alla restituzione al danneggiato e i diritti dei terzi in buona fede.

Infine, la pubblicazione della sentenza di condanna, per estratto o integralmente, su uno o più quotidiani e mediante affissione nel Comune in cui l'Ente ha la propria sede principale, può essere disposta dal Giudice in presenza di una sanzione interdittiva. L'esecuzione della pubblicazione è a carico della Cancelleria del Giudice e le relative spese sono a carico dell'Ente sanzionato.

### **1.3. Reati commessi all'estero**

Secondo l'articolo 4 del D.Lgs. 231/2001, un Ente può essere ritenuto responsabile anche per reati commessi al di fuori del territorio italiano, a condizione che siano soddisfatti i requisiti di imputazione soggettiva e oggettiva previsti dalla normativa.

In particolare, la responsabilità dell'Ente sussiste solo se:

1. Il reato è stato perpetrato da un soggetto che opera in funzione dell'Ente, secondo quanto stabilito dall'articolo 5, comma 1 del Decreto;
2. L'Ente ha la propria sede principale in Italia;

3. Le autorità del Paese in cui il reato è stato commesso non abbiano già avviato un procedimento nei confronti dell'Ente;
4. Risultino soddisfatte le condizioni previste dagli articoli 7, 8, 9 e 10 del Codice penale.

#### 1.4. Responsabilità da reato nei gruppi di imprese

Il Decreto non disciplina in modo specifico la responsabilità dell'Ente all'interno di un gruppo societario, nonostante questa configurazione sia piuttosto comune.

Poiché il gruppo di imprese, come entità complessiva, non può essere direttamente considerato responsabile ai sensi del D.Lgs. 231/2001, è necessario valutare come i Modelli organizzativi si applicano ai reati commessi all'interno di strutture aziendali articolate.

Come indicato anche nelle più recenti Linee Guida di Confindustria, la società controllante (holding) potrebbe essere ritenuta responsabile di un reato commesso nell'ambito dell'attività della controllata nei seguenti casi:

- Il reato presupposto è stato commesso nell'interesse o con un vantaggio immediato e diretto non solo per la controllata, ma anche per la controllante;
- Soggetti legati funzionalmente alla società controllante hanno preso parte alla commissione del reato, fornendo un contributo determinante e dimostrabile in modo concreto e specifico.

#### 1.5. Tentativo

Quando i reati presupposto vengono commessi in forma tentata, anziché portati a compimento, le sanzioni pecuniarie (in termini di importo) e quelle interdittive (in termini di durata) subiscono una riduzione compresa tra un terzo e la metà, come stabilito dagli articoli 12 e 26 del D.Lgs. 231/2001.

Tuttavia, l'Ente non è ritenuto responsabile nel caso in cui abbia impedito volontariamente la realizzazione dell'atto o il verificarsi dell'evento dannoso (art. 26 D.Lgs. 231/2001). Questa esclusione di responsabilità deriva dal fatto che, bloccando l'azione illecita, viene interrotto qualsiasi legame di immedesimazione tra l'Ente e i soggetti che agiscono in suo nome o per suo conto.

## 2. Il modello di Governance della Società

### 2.1. Premessa

L'editore COME è governata da un **Amministratore Unico**, dotato di tutti i necessari poteri per la gestione ordinaria e straordinaria della società, al quale spettano la rappresentanza generale dell'Ente e la firma sociale.

Il controllo legale dei conti è demandato al **Sindaco unico**, scelto e nominato tra persone iscritte nel Registro dei Revisori Contabili. Il Sindaco, organo consultivo contabile della Società, vigila sulla gestione finanziaria della stessa, accerta la regolare tenuta delle scritture contabili, esamina le proposte di bilancio preventivo e di conto consuntivo, redigendo apposite relazioni, ed effettua verifiche di cassa. L'adozione del Modello consente all'Ente di migliorare costantemente il proprio

sistema di Governance, promuovendo comportamenti corretti e trasparenti nel rispetto delle normative vigenti e dei valori etico-sociali di riferimento. In linea con il Codice Etico, il Modello ribadisce la condanna di qualsiasi comportamento illecito e garantisce che le attività a rischio siano svolte secondo procedure uniformi e controllate. Inoltre, tutela l'integrità del patrimonio sociale, grazie alla sua efficacia esimente.

## 2.2. Le Linee Guida

Il Modello è stato sviluppato sulla base delle Linee Guida di Confindustria del 7 marzo 2002, aggiornate nel luglio 2014 e nel giugno 2021. Le attività fondamentali previste comprendono:

- Individuazione delle aree a rischio di reato.
- Predisposizione di un sistema di controllo per prevenire i reati mediante protocolli specifici.
- Strutturazione di un sistema di governance per garantire efficienza, affidabilità delle informazioni e conformità normativa.

Pur ispirandosi alle Linee Guida, il Modello è personalizzato sulla realtà dell'Ente e può discostarsi da esse per esigenze specifiche.

## 2.3. Definizione del Modello

L'elaborazione del Modello ha seguito un processo di risk analysis articolato nei seguenti passaggi:

- **Self Risk Assessment** condotto dai Responsabili aziendali tramite questionari.
- **Interviste** ai Responsabili chiave.
- **Mappatura dei processi aziendali** per identificare le aree a rischio.
- **Rilevazione dei controlli interni esistenti** e individuazione di presidi aggiuntivi.
- **Costruzione della Matrice dei Rischi**, distinguendo rischi lordi e netti.
- **Elaborazione del Modello**, aggiornato periodicamente sulla base delle modifiche normative e delle valutazioni di risk assessment.

I rischi sono classificati su una scala da **molto basso (0-1) a alto (3,8-5)**. La mappatura considera processi, procedure, attività sensibili e protocolli preventivi adottati dall'Ente.

Di seguito la tabella relativa alla classificazione dei rischi utilizzata in fase di mappatura:

	<b>Molto basso (0 - 1)</b>
	<b>Basso (1,1 - 1,7)</b>
	<b>Medio (1,8 - 2,6)</b>
	<b>Medio alto (2,7 - 3,7)</b>
	<b>Alto (3,8 - 5)</b>

## 2.4. Sistema di controllo interno

Il Modello si affianca al sistema di controlli interni già adottato, che include:

- Regole di governance e statuto sociale.
- Sistema di procure e attribuzioni interne.
- Organigramma aziendale.
- Procedure, linee guida e istruzioni operative.
- Documento di Valutazione dei Rischi (D.Lgs. 81/2008) e Servizio di Prevenzione e Protezione.
- Sistema informativo per la gestione degli strumenti informatici e conformità alla normativa privacy.
- Manuale per la Qualità.

Il sistema di controllo garantisce la prevenzione dei reati previsti dal D.Lgs. 231/2001, anche per quelli a rischio minimo o insussistente.

## 2.5. Rapporti tra MOCG e Codice Etico

Il Modello è autonomo rispetto al Codice Etico, ma entrambi perseguono l'obiettivo di garantire legalità e correttezza. Il Codice Etico:

- Definisce i valori fondamentali della Società.
- Stabilisce norme di condotta per la prevenzione di comportamenti illeciti.
- Contribuisce alla trasparenza e all'affidabilità della Società.

Vero è che il Codice Etico contiene, invero, l'insieme dei valori che la Società riconosce, rispetta e condivide verso specifiche categorie di portatori di interessi legittimi. Le relative norme di condotta, che ne garantiscono l'attuazione, disciplinano in concreto i principi comportamentali da osservare nello svolgimento delle attività per garantire il buon funzionamento, l'affidabilità e la buona reputazione della Società e costituiscono un efficace strumento di prevenzione di comportamenti illeciti da parte di tutti coloro che si trovano ad agire in nome e per conto della stessa.

Tuttavia, l'adozione combinata di Modello e Codice Etico rafforza l'efficacia dei controlli e della prevenzione dei rischi.

## 3. DIFFUSIONE DEL MODELLO E FORMAZIONE

### 3.1. Premesse

Per garantire l'efficacia del Modello, la Società si impegna a diffondere e rendere pienamente comprensibili le norme di condotta in esso contenute a tutti i membri degli organi sociali, ai

dipendenti, ai collaboratori esterni e ai soggetti terzi con cui COM.E intrattiene relazioni di qualsiasi genere.

Questo obiettivo si estende sia alle risorse già operative all'interno dell'azienda, sia a quelle che vi entreranno in futuro. Il livello di formazione e informazione è calibrato sulla base delle mansioni svolte dai destinatari. La partecipazione alle iniziative formative, organizzate secondo le modalità e i tempi stabiliti dalla Società e in conformità alle indicazioni dell'Organismo di Vigilanza, è obbligatoria. La mancata partecipazione può essere oggetto di provvedimenti disciplinari. Le attività di formazione e informazione verranno erogate secondo le modalità descritte di seguito.

### **3.2. Diffusione tra le risorse interne alla Società**

L'adozione del Modello è comunicata ai destinatari mediante strumenti adeguati, quali la pubblicazione sul sito aziendale, l'affissione in bacheca, la distribuzione di copie cartacee o la trasmissione di informative specifiche. I nuovi assunti, al momento dell'ingresso in azienda, dichiarano formalmente di accettare e rispettare il Codice Etico e il Modello di Organizzazione, Gestione e Controllo D.Lgs. 231/2001, confermandone l'avvenuta ricezione e comprensione.

### **3.3. I soggetti terzi destinatari del Modello**

La comunicazione dei contenuti e dei principi del Modello si estende anche ai soggetti terzi che collaborano con la Società tramite rapporti contrattuali o che la rappresentano senza vincolo di subordinazione, quali partner commerciali, consulenti e collaboratori esterni.

In particolare, fornitori, collaboratori e partner vengono informati dell'esistenza del Modello di Organizzazione, Gestione e Controllo (incluso il Codice Etico) e delle conseguenze derivanti dalla violazione delle sue disposizioni o della normativa vigente sui rapporti contrattuali. A tal fine, nei contratti stipulati con la Società vengono inserite clausole specifiche in cui la controparte dichiara di essere a conoscenza del Modello e si impegna a rispettare le disposizioni del D.Lgs. 231/01 e del MOGC di COM.E. Tali clausole prevedono inoltre la facoltà per la Società di effettuare verifiche sul rispetto del D.Lgs. 231/01 e di applicare sanzioni in caso di inosservanza, quali la risoluzione del contratto o la richiesta di risarcimento danni.

### **3.4. La Formazione Interna ai soggetti destinatari del Modello**

il piano formativo si articola in due tipologie: una formazione di carattere generale, rivolta a tutto il personale aziendale, e una formazione specifica, destinata ai destinatari del Modello che ricoprono ruoli operativi di rilievo nelle aree a rischio, ovvero quelle in cui potrebbero verificarsi i reati previsti dal D.Lgs. 231/01.

Esso è finalizzato a diffondere la conoscenza della normativa prevista dal D.Lgs. 231/01 ed è strutturato in modo differenziato nei contenuti e nelle modalità di erogazione, tenendo conto della

qualifica dei destinatari, del livello di rischio dell'area in cui operano e dell'eventuale esercizio di funzioni di rappresentanza della Società.

In particolare, la formazione generale ha l'obiettivo di fornire una comprensione approfondita dei requisiti relativi alla responsabilità amministrativa degli enti, nonché delle caratteristiche principali del Modello Organizzativo e del ruolo dell'Organismo di Vigilanza.

La formazione specifica, invece, mira a informare i destinatari sui rischi specifici legati all'area in cui operano, fornendo indicazioni sui principi di condotta e sulle procedure aziendali da seguire nello svolgimento delle loro attività.

La pianificazione dei corsi di formazione, comprese le tempistiche, le modalità di attuazione e i contenuti dei programmi, è di competenza dell'Organo gestorio, che ne informa l'Organismo di Vigilanza. Quest'ultimo, qualora non si occupi direttamente della formazione, è incaricato di verificarne l'effettivo svolgimento.

## **4. MODIFICHE, INTEGRAZIONI E VERIFICHE PERIODICHE DEL MODELLO**

### **4.1. Modifiche e integrazioni del Modello**

La responsabilità dell'adozione e della corretta applicazione del Modello ricade, per esplicita previsione normativa, sull'Organo amministrativo. Poiché il presente documento rappresenta un "atto emanato dall'organo dirigente" (in conformità con l'art. 6, comma 1, lettera a del Decreto), qualsiasi modifica o integrazione, sia di natura sostanziale che non, rientra esclusivamente nelle competenze dell'Organo amministrativo di COM.E.

### **4.2. Verifica del Modello**

Il Modello sarà sottoposto a due tipologie di verifica:

- **Controllo delle procedure:**  
L'OdV, secondo una propria programmazione, verificherà che le procedure adottate siano sempre coerenti con i requisiti di efficacia ed effettività del Modello.
- **Esame degli atti:**  
Qualora emergano situazioni di potenziale criticità, l'OdV analizzerà gli atti dell'ente e i contratti stipulati nelle aree a rischio per valutare se le variazioni intervenute rendano opportuna una revisione, anche parziale, del Modello.

I risultati delle verifiche saranno sintetizzati dall'OdV in un apposito libro verbali e comunicati all'organo gestorio attraverso i consueti canali informativi. Nel caso in cui le verifiche riguardino processi particolarmente rilevanti o vengano riscontrate criticità significative, l'OdV potrà redigere un report specifico, oltre alla verbalizzazione standard, da sottoporre all'Organo amministrativo di COM.E, evidenziando le problematiche rilevate e le eventuali azioni correttive consigliate.

## 5. L'ORGANISMO DI VIGILANZA

### 5.1. Premessa

In linea generale, l'OdV è incaricato di verificare l'adeguatezza e l'efficacia del Modello, proporre l'aggiornamento in caso di modifiche normative, violazioni o esiti negativi delle verifiche, nonché a seguito di variazioni nella struttura organizzativa dell'Ente. Deve inoltre vigilare sulla corretta applicazione del Modello, effettuare analisi periodiche sulle sue componenti, garantire un flusso informativo efficace da e verso l'Organismo e segnalare eventuali violazioni riscontrate.

L'effettivo svolgimento di tali compiti da parte dell'OdV rappresenta un elemento fondamentale affinché l'Ente possa beneficiare dell'esimente prevista dalla normativa.

Orbene, ai sensi del D.Lgs. 231/01, l'articolo 6, comma 1, lettera b) stabilisce che, con riferimento all'operato dei soggetti apicali, *"il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento"* deve essere affidato *"a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo"*.

Sebbene non vi sia una disposizione legislativa specifica in merito ai soggetti subordinati, l'articolo 7, comma 4, lettera a) prevede che, ai fini dell'efficace attuazione del Modello adottato, sia necessaria una verifica periodica con eventuali modifiche, qualora emergano violazioni significative delle prescrizioni o intervengano cambiamenti nell'organizzazione o nelle attività. Tale compito rientra tipicamente tra le funzioni dell'Organismo di Vigilanza. Confindustria ha fornito ulteriori indicazioni sulle attribuzioni dell'OdV nelle linee guida emanate a marzo 2002 e successivamente aggiornate a maggio 2004, marzo 2014 e giugno 2021.

### 5.2. La nomina, composizione e durata dell'Organismo di Vigilanza

Tenuto conto delle dimensioni aziendali, della specificità delle funzioni dell'OdV e delle raccomandazioni dell'associazione di categoria, la Società ha scelto di adottare un organismo monocratico.

Il ruolo di componente dell'OdV viene assegnato a un soggetto esterno indipendente, selezionato in base alle competenze richieste per l'incarico. Tale figura deve possedere adeguate conoscenze in ambito giuridico, controllo e gestione dei rischi aziendali, oltre a una conoscenza approfondita delle dinamiche aziendali.

Questa scelta, conforme alle linee guida di Confindustria, è finalizzata a garantire l'autonomia e l'indipendenza dell'Organismo di Vigilanza.

La nomina dell'OdV avviene tramite determina dell'Amministratore Unico, che ne stabilisce anche il compenso, oltre ad approvare l'adozione iniziale del MOGC e le sue eventuali successive modifiche.

La composizione, i compiti e i poteri dell'OdV sono resi noti all'interno dell'Ente mediante pubblicazione del presente documento sulla rete intranet aziendale e/o mediante affissione in un'area accessibile a tutti nei locali aziendali.

La durata dell'incarico dell'Organismo di Vigilanza è pari a tre anni, salvo diversa determinazione dell'Organo Amministrativo.

La cessazione dell'incarico può avvenire per una delle seguenti cause:

- scadenza dell'incarico;
- revoca dell'OdV da parte dell'organo amministrativo;
- rinuncia formalizzata mediante apposita comunicazione scritta, inviata all'organo amministrativo;
- qualora sopraggiunga una delle cause di ineleggibilità e/o decadenza.

La revoca dell'organismo di vigilanza può avvenire solo per giusta causa, ove per giusta causa possono intendersi, in via esemplificativa ma non esaustiva:

- una grave negligenza nell'espletamento dei compiti connessi all'incarico;
- il possibile coinvolgimento dell'Ente in un procedimento, penale o civile, che sia connesso ad una omessa o insufficiente vigilanza, anche colposa.

La revoca per giusta causa è disposta con determinazione dell'Organo amministrativo, previo parere dell'Organo di controllo dal quale il primo può dissentire solo con adeguata motivazione.

In caso di revoca o rinuncia, l'Amministratore Unico nomina, senza indugio, il nuovo OdV.

### **5.3. I requisiti dell'Organismo di Vigilanza**

Considerata la natura delle responsabilità attribuite all'OdV, le disposizioni normative e le indicazioni fornite nelle Linee Guida di Confindustria, la selezione dell'Organismo è stata effettuata in modo da assicurare il rispetto dei requisiti di autonomia, indipendenza, professionalità e continuità d'azione richiesti per questa delicata funzione.

In particolare, sulla base delle suddette Linee Guida, tali requisiti si possono così delineare:

#### **a) Autonomia**

L'OdV gode di autonomia decisionale.

Esso opera in maniera indipendente rispetto all'Ente e deve essere in grado di svolgere il proprio ruolo senza alcuna influenza, diretta o indiretta. Le attività svolte dall'Organismo di Vigilanza non possono essere soggette a controllo o valutazione da parte di altri organi o strutture aziendali.

L'OdV è altresì autonomo sotto il profilo regolamentare, avendo la facoltà di definire in autonomia le proprie regole comportamentali e procedurali, nei limiti dei poteri conferiti dall'organo amministrativo. Inoltre, ha piena libertà nella determinazione delle modalità e della frequenza delle proprie riunioni.

#### **b) Indipendenza**

Il componente dell'Organismo di Vigilanza non deve trovarsi in alcuna situazione, nemmeno potenziale, di conflitto di interessi con l'Ente né ricoprire funzioni esecutive al suo interno.

#### **c) Professionalità**

L'OdV deve possedere adeguate competenze professionali e garantire affidabilità nello svolgimento delle proprie funzioni.

È dunque necessario che disponga di conoscenze tecniche e professionali adeguate ai suoi compiti, con competenze in ambito giuridico, contabile, aziendale e organizzativo.

In particolare, devono essere presenti capacità specifiche nell'ambito ispettivo e consulenziale, incluse competenze nelle tecniche di analisi e valutazione dei rischi, nelle metodologie di intervista e nella predisposizione di questionari, nonché nelle strategie per l'individuazione di frodi.

L'unione di queste caratteristiche, insieme al requisito dell'indipendenza, assicura l'obiettività di giudizio dell'OdV.

#### **d) Continuità d'azione**

Per garantire l'efficace e costante applicazione del Modello, l'OdV opera senza interruzioni.

L'Organismo di Vigilanza adotta soluzioni operative che assicurano un impegno costante nell'adempimento delle proprie funzioni con efficienza ed efficacia.

Per svolgere adeguatamente i propri compiti, l'OdV è dotato di risorse economiche e operative adeguate, inclusi budget specifici per l'espletamento della propria attività.

### **5.4. I requisiti**

Il componente dell'Organismo di Vigilanza deve possedere requisiti di indipendenza, onorabilità e moralità. Non è eleggibile e/o decade dall'incarico chi, a titolo esemplificativo e non esaustivo:

- sia stato dichiarato interdetto, inabilitato o fallito;
- abbia riportato una condanna con sentenza irrevocabile ai sensi dell'art. 648 c.p.p.:
  - a) per fatti inerenti lo svolgimento delle sue funzioni;
  - b) per reati che incidano in maniera rilevante sulla sua integrità morale e professionale;
  - c) per violazioni che comportino l'interdizione dai Pubblici Uffici, dagli organi direttivi di imprese e persone giuridiche, dall'esercizio di una professione o di un'arte, nonché l'incapacità di contrattare con la Pubblica Amministrazione;
  - d) in ogni caso, per aver commesso uno dei reati previsti dal D.Lgs. 231/2001.

### **5.5. Le risorse dell'Organismo di Vigilanza**

All'OdV sono assegnate le risorse umane e finanziarie necessarie per lo svolgimento delle proprie funzioni.

Per quanto riguarda le risorse umane, l'organo dirigente, su indicazione dell'OdV, può destinare specifiche risorse in numero adeguato alle dimensioni dell'ente e ai compiti dell'Organismo. Le risorse assegnate, pur continuando a rispondere al proprio referente gerarchico, operano funzionalmente sotto l'OdV per le attività svolte in suo nome.

In merito alle risorse finanziarie, l'OdV dispone di un budget annuale assegnato su sua proposta, necessario per l'adempimento delle proprie funzioni. Se nel corso del mandato dovesse emergere la necessità di ulteriori risorse, l'OdV può richiederle all'Organo amministrativo attraverso una comunicazione motivata scritta.

L'OdV può inoltre avvalersi, sotto la propria diretta supervisione e responsabilità, del supporto di consulenti esterni, il cui compenso è sostenuto tramite le risorse finanziarie assegnate.

### 5.5. Le Funzioni dell'Organismo di Vigilanza

Ai sensi dell'art. 6, comma 1, del Decreto, l'OdV ha il compito di "vigilare sul funzionamento e sull'osservanza del modello e di curarne l'aggiornamento".

Nello specifico, le funzioni dell'OdV comprendono:

1. **Verifica e vigilanza sul modello**, ovvero:
  - accertare l'adeguatezza del modello, valutando la sua capacità di prevenire comportamenti illeciti e di individuare eventuali violazioni;
  - verificare l'effettiva applicazione del modello, monitorando la coerenza tra i comportamenti aziendali e le previsioni formali;
  - effettuare verifiche periodiche e straordinarie sul sistema di prevenzione adottato dall'Ente.
2. **Aggiornamento del modello**, proponendone le necessarie modifiche per migliorarne l'efficacia e l'adeguatezza, considerando:
  - eventuali interventi normativi sopraggiunti;
  - cambiamenti nella struttura organizzativa o nelle attività aziendali;
  - violazioni significative del modello.
3. **Informazione e formazione sul modello**, attraverso:
  - la promozione di iniziative volte a diffondere la conoscenza del modello tra i destinatari;
  - l'organizzazione di corsi e comunicazioni per garantire un'adeguata formazione in merito;
  - la risposta tempestiva a richieste di chiarimento e consulenza da parte di funzioni aziendali o organi amministrativi e di controllo.
4. **Gestione dei flussi informativi**, che include:
  - l'esame e la valutazione di segnalazioni e informazioni relative al rispetto del modello;
  - la comunicazione periodica agli organi sociali sulle attività svolte e sui risultati ottenuti;
  - la segnalazione agli organi istituzionali di eventuali violazioni del modello e dei soggetti responsabili, con aggiornamenti sull'esito delle segnalazioni;

- il supporto informativo agli organi ispettivi in caso di controlli da parte di enti istituzionali, inclusa la Pubblica Autorità.

L'OdV è inoltre tenuto a:

- documentare accuratamente tutte le attività svolte, le iniziative intraprese e le segnalazioni ricevute, garantendo la completa tracciabilità degli interventi e delle indicazioni fornite;
- registrare e conservare tutta la documentazione rilevante ai fini del corretto svolgimento del proprio incarico.

## 5.6. I poteri dell'Organismo di Vigilanza

Per garantire un'efficace vigilanza sull'applicazione del modello, l'OdV dispone di tutti i poteri necessari, tra cui la facoltà di:

- effettuare verifiche, anche a sorpresa, sulle procedure e sui documenti aziendali, qualora ritenuto opportuno o in presenza di situazioni critiche;
- accedere liberamente a tutte le funzioni, archivi e documenti dell'Ente senza necessità di autorizzazioni preventive, al fine di raccogliere informazioni, dati e documenti utili;
- convocare risorse aziendali per ottenere chiarimenti su attività, eventuali disfunzioni o violazioni del modello;
- avvalersi di consulenti esterni sotto la propria diretta supervisione e responsabilità;
- disporre delle risorse finanziarie assegnate dall'Organo amministrativo per adempiere ai propri compiti.

## 5.7 Obblighi di informazione all'Organismo di Vigilanza

L'art. 6, comma 2, lett. d) del Decreto prevede che il Modello debba includere "obblighi di informazione nei confronti dell'OdV" affinché quest'ultimo possa svolgere efficacemente le proprie funzioni di controllo.

Pertanto, tutti i destinatari del Modello – amministratori, revisori, dipendenti, consulenti, collaboratori e partner – sono tenuti a segnalare tempestivamente all'OdV qualsiasi informazione riguardante possibili violazioni del Modello Organizzativo adottato dall'Ente.

Per garantire la chiarezza dei flussi informativi da e verso l'OdV, è stata predisposta un'apposita procedura (n. 8), cui si rimanda per i dettagli operativi. Di seguito si riportano i principi fondamentali relativi alla gestione di tali flussi.

### A) Segnalazioni di possibili violazioni del Modello

I destinatari devono informare l'OdV di qualsiasi elemento che possa indicare la commissione, o il rischio di commissione, di reati o comportamenti non conformi ai principi del Modello. In particolare, devono essere segnalate immediatamente all'OdV le seguenti situazioni:

- **Ordini ricevuti** da superiori gerarchici che appaiano in contrasto con la legge, la normativa interna o il Modello;
- **Richieste o offerte indebite di denaro, doni o altre utilità** da o verso pubblici ufficiali, incaricati di pubblico servizio o soggetti collegati alla Pubblica Amministrazione;
- **Irregolarità contabili**, omissioni, trascuratezze o falsificazioni nella tenuta della contabilità e nella conservazione della documentazione contabile;
- **Provvedimenti e indagini** da parte della Polizia Giudiziaria o di altre Autorità che possano riguardare, anche indirettamente, l'Ente, il personale o i membri degli organi sociali;
- **Procedimenti disciplinari in corso** e relative sanzioni eventualmente applicate;
- **Segnalazioni non riscontrate** riguardanti carenze nei luoghi di lavoro, attrezzature inadeguate o dispositivi di protezione insufficienti, nonché qualsiasi altra situazione di rischio per la salute e sicurezza dei lavoratori.

## B) Informazioni rilevanti per l'attività dell'OdV

Oltre alle segnalazioni sopra indicate, devono essere comunicate all'OdV tutte le informazioni che possano incidere sullo svolgimento dei suoi compiti di vigilanza, tra cui:

- **Modifiche organizzative o procedurali** che possano avere un impatto, anche minimo, sul sistema 231;
- **Aggiornamenti dei poteri e delle deleghe** all'interno dell'Ente;
- **Procedure per l'ottenimento e l'utilizzo di finanziamenti pubblici**, contributi, mutui agevolati o altre erogazioni da enti statali, pubblici o comunitari;
- **Bilancio annuale** dell'Ente;
- **Comunicazioni del Sindaco Unico** relative a criticità emerse e non risolte.

L'OdV può stabilire ulteriori categorie di informazioni da trasmettere, definendo, previa informativa all'Organo amministrativo, le modalità e la periodicità delle comunicazioni, anche attraverso l'uso di flussogrammi o apposite schede di reportistica.

## C) Valutazione delle segnalazioni e attività ispettiva

L'OdV, una volta ricevuta una segnalazione, valuta la rilevanza delle informazioni ricevute e, se necessario, avvia un'attività ispettiva. Tale attività può essere svolta con il supporto di risorse interne o, in caso di particolari complessità o esigenze tecniche, con il contributo di professionisti esterni.

### Canali di segnalazione e tutela del segnalante

Ai sensi dell'art. 6, comma 2-bis, del D.Lgs. 231/2001, il Modello prevede l'istituzione di canali riservati attraverso i quali dipendenti e collaboratori possono inviare segnalazioni circostanziate e documentate su condotte illecite o violazioni del Modello.

Tali canali garantiscono la riservatezza del segnalante e sono gestiti direttamente dall'OdV, che assicura la protezione dell'identità di chi effettua la segnalazione.

Sono espressamente vietate e sanzionate:

- **Condotte ritorsive** nei confronti del segnalante, commesse da organi direttivi o da soggetti operanti per conto della Società;
- **Segnalazioni infondate effettuate con dolo o colpa grave**, volte a danneggiare terzi o a creare turbative ingiustificate.

## 5.8. Obblighi di informative dell'Organismo di Vigilanza nei confronti degli organi sociali

L'Organismo di Vigilanza (OdV) svolge un'attività costante e precisa di reporting nei confronti degli organi istituzionali. In particolare, con cadenza annuale, l'OdV relaziona per iscritto l'Organo amministrativo e il Sindaco Unico sulle attività svolte. Tale relazione include:

- Controlli effettuati ed esiti degli stessi;
- Verifiche specifiche eseguite e relativi risultati;
- Aggiornamenti della mappatura dei rischi, se necessari;
- Rendiconto del budget di spesa stanziato dall'Organo amministrativo;
- Piano annuale delle attività di verifica, controllo e aggiornamento previste per l'anno successivo, salvo eventuali emergenze.

### Contenuto del reporting

L'attività di reporting riguarda in particolare:

- Le attività complessive svolte dall'OdV;
- Eventuali criticità o problematiche emerse nell'attività di vigilanza;
- Le azioni correttive necessarie o proposte per garantire l'efficacia del Modello e il loro stato di attuazione;
- L'accertamento di comportamenti non conformi al Modello;
- La rilevazione di carenze organizzative o procedurali che espongono l'Ente a rischi di commissione di reati rilevanti ai sensi del Decreto;
- L'eventuale mancata o carente collaborazione delle risorse aziendali nelle attività di verifica e indagine;
- Qualsiasi informazione ritenuta utile ai fini della vigilanza.

L'OdV si rivolge all'Organo amministrativo ogni qualvolta lo ritenga opportuno per garantire un efficace svolgimento delle proprie funzioni. Allo stesso modo, l'Organo di Controllo e l'Organo amministrativo possono convocare l'OdV in qualsiasi momento.

Il contenuto delle riunioni viene verbalizzato, e le copie dei verbali sono conservate dall'OdV.

### **Conservazione delle informazioni**

Tutte le informazioni, segnalazioni e verbalizzazioni previste dal Modello devono essere conservate dall'OdV su supporto cartaceo o informatico per un periodo di 15 anni. L'accesso a tale documentazione è consentito agli Organi di Controllo e all'Organo amministrativo, salvo che non riguardi indagini a loro carico e fatte salve eventuali disposizioni di legge vigenti.

La documentazione relativa ai protocolli previsti nel Modello e dalle norme operative connesse deve essere conservata per 15 anni a cura del personale interessato.

L'OdV in carica riceve dai componenti precedenti la documentazione relativa alle attività svolte nel corso dei rispettivi mandati. Tale documentazione è gestita e conservata in un archivio, cartaceo o informatico, accessibile all'Organo Amministrativo, all'Organo di Controllo e ai componenti degli OdV succedutisi nel tempo, nel rispetto delle normative sulla riservatezza e tutela del segnalante.

### **5.9 Obblighi di comportamento che regolamentano l'attività dell'Organismo di Vigilanza**

I componenti dell'OdV, così come le risorse interne ed esterne di supporto, sono tenuti al rispetto delle norme etiche e comportamentali stabilite nel Codice Etico dell'Ente e degli standard specifici di condotta.

#### **Obblighi dei membri dell'OdV**

Nell'espletamento delle proprie funzioni, i membri dell'OdV devono:

- Assicurare lo svolgimento dei compiti assegnati con onestà, obiettività e accuratezza;
- Mantenere un atteggiamento leale, evitando azioni o omissioni che possano favorire violazioni del Modello;
- Non accettare doni o vantaggi dall'Ente, dal personale, dai clienti, dai fornitori o da soggetti della Pubblica Amministrazione, salvo quelli di modico valore rientranti nei normali rapporti professionali;
- Evitare qualsiasi comportamento che possa ledere il prestigio e la professionalità dell'OdV o dell'intera organizzazione aziendale;
- Segnalare all'Organo amministrativo eventuali impedimenti o difficoltà nell'espletamento delle proprie attività;
- Garantire la massima riservatezza nella gestione delle informazioni acquisite;
- Non utilizzare informazioni riservate in violazione delle norme sulla privacy o per ottenere vantaggi personali o per terzi;
- Riportare fedelmente i risultati della propria attività.

Qualsiasi violazione di tali obblighi sarà valutata e potrà comportare provvedimenti disciplinari o la revoca dell'incarico.

## 6. WHISTLEBLOWING

### 6.1 Premessa

La Legge 30 novembre 2017, n. 179, nota come Legge sul whistleblowing, ha introdotto disposizioni specifiche per la protezione di coloro che, nell'ambito di un rapporto di lavoro pubblico o privato, segnalano comportamenti illeciti o irregolarità di cui sono venuti a conoscenza.

La materia è stata dapprima novellata dalla direttiva (UE) "2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione" - che ha inteso favorire il contrasto alle violazioni del diritto dell'Unione individuando un corpo normativo comune agli Stati membri capace di favorire le segnalazioni di chi opera in o con organizzazioni pubbliche o private e che pertanto possa venire a conoscere di comportamenti lesivi del pubblico interesse.

La direttiva è stata quindi recepita dal Decreto Legislativo n. 24 del 10 marzo 2023.

Con l'introduzione e le successive integrazioni sulla materia, il legislatore ha cercato di allineare le normative per il settore pubblico con quelle previste per il settore privato, intervenendo con modifiche al Decreto Legislativo n. 231/2001, in particolare all'art. 6, che include nuovi commi relativi alla gestione delle segnalazioni da parte degli enti.

In particolare, gli interventi normativi hanno stabilito che i Modelli di Organizzazione, Gestione e Controllo debbano prevedere:

- canali sicuri e riservati per le segnalazioni di illeciti o violazioni del modello, fatti dai soggetti indicati all'art. 5, comma 1, lettere a) e b), che garantiscano la riservatezza dell'identità del segnalante;
- almeno un canale alternativo informatico che tuteli la privacy del segnalante;
- il divieto di atti di ritorsione nei confronti del segnalante, sia diretti che indiretti, legati alla segnalazione;
- l'introduzione di sanzioni disciplinari per chi viola le misure di tutela del segnalante o effettua segnalazioni infondate con dolo o colpa grave.

La normativa prevede inoltre che eventuali atti di discriminazione o ritorsione nei confronti del segnalante possano essere denunciati all'Ispettorato del Lavoro. In caso di licenziamento o altre misure penalizzanti nei confronti del segnalante, queste sono considerate nulle. L'onere della prova spetta al datore di lavoro, che dovrà dimostrare che tali misure siano motivate da ragioni estranee alla segnalazione stessa.

Il sistema di whistleblowing intende promuovere l'efficacia degli strumenti di contrasto alla corruzione e incentivare la segnalazione di illeciti, garantendo la protezione dei segnalanti e favorendo un ambiente di lavoro etico e trasparente. Le segnalazioni devono essere dettagliate e permettere alle persone preposte di effettuare verifiche adeguate. Le segnalazioni anonime sono ammesse solo se contengono informazioni sufficientemente precise e gravi.

Inoltre, sono garantite specifiche tutele contro atti di discriminazione o penalizzazione nei confronti dei segnalanti, inclusa la riservatezza dell'identità. Le segnalazioni devono essere inviate all'Organismo di Vigilanza (OdV) dell'ente, che è responsabile per la gestione e l'indagine sulle segnalazioni ricevute.

COM.E si impegna al fine di regolamentare, incentivare e proteggere, chi, nello svolgimento delle proprie mansioni lavorative, venendo a conoscenza di un illecito e/o di un'irregolarità sul luogo di lavoro, rilevanti ai fini del D. Lgs. n. 231/2001, decide di farne segnalazione (c.d. whistleblower).

A tal proposito, ha implementato una specifica procedura per agevolare le segnalazioni relative a:

- condotte illecite che integrano una o più fattispecie di reato da cui può derivare una responsabilità per l'ente ai sensi del Decreto;
- condotte che, pur non integrando alcuna fattispecie di reato, sono state attuate contravvenendo a regole di condotta, procedure, protocolli o disposizioni contenute all'interno del Modello o dei documenti ad esso allegati.

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 (art. 6, comma 2-bis, D. Lgs. n. 231/2001).

L'Ente, tramite i soggetti preposti, effettua tutte le opportune verifiche sui fatti segnalati, garantendo che tali verifiche siano svolte nel minor tempo possibile e nel rispetto dei principi generali di indipendenza e professionalità delle attività di controllo e di riservatezza.

Le segnalazioni anonime, ovvero quelle segnalazioni prive di elementi che consentano di identificare il loro autore, non sono ammesse. Tuttavia, tali segnalazioni saranno oggetto di ulteriori verifiche solo ove siano connotate da un contenuto adeguatamente dettagliato e circostanziato e aventi ad oggetto illeciti o irregolarità particolarmente gravi.

Tutti i dipendenti e i terzi interessati (ditte terze, consulenti, ecc.) possono effettuare segnalazioni relativamente a potenziali violazioni del Codice Etico e del Modello e su situazioni di potenziale rischio di commissione dei reati previsti dal D.Lgs. 231/01. In ottemperanza alle previsioni normative di cui alla Legge n. 179/2017, i segnalanti in buona fede sono garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione e in ogni caso sarà assicurata la riservatezza del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti dell'Ente o delle persone accusate erroneamente. Saranno inoltre opportunamente sanzionati comportamenti strumentalmente volti a rallentare l'attività dell'OdV.

## **7. II SISTEMA DISCIPLINARE E SANZIONATORIO**

### **7.1. Premesse**

In base agli articoli 6, comma 2, lettera e), e 7, comma 2, lettera b) del Decreto Legislativo, i modelli di organizzazione, gestione e controllo, necessari per ottenere l'esenzione da responsabilità in caso di commissione di reati, devono includere un sistema disciplinare che preveda sanzioni per il

mancato rispetto delle misure indicate nel Modello stesso. Le sanzioni disciplinari sono applicabili indipendentemente dall'avvio di un procedimento penale, poiché il Modello e il Codice Etico sono regole vincolanti per tutti i destinatari, la cui violazione deve essere sanzionata per ottemperare al Decreto Legislativo, anche in assenza di un reato o di una condanna. L'adozione del Modello è volta a rispettare la normativa vigente e a garantire una buona governance aziendale.

## **7.2. Definizione e Limiti della Responsabilità Disciplinare**

Questa sezione del Modello descrive le violazioni rilevanti ai sensi del Decreto Legislativo 231/2001, le relative sanzioni disciplinari e la procedura per la contestazione e l'applicazione delle sanzioni. Le sanzioni devono essere conformi ai Contratti Collettivi Nazionali del Lavoro e rispettare quanto previsto dall'articolo 7 della Legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori). Per i destinatari che non sono dipendenti (come i liberi professionisti), le misure sanzionatorie devono rispettare la legge e le condizioni contrattuali.

## **7.3. Destinatari e Loro Doveri**

I destinatari del sistema disciplinare sono gli stessi destinatari del Modello. Essi sono tenuti a rispettare i principi del Codice Etico e le misure di organizzazione e gestione definite nel Modello. Le violazioni delle regole del Modello (di seguito "infrazioni") comportano, a seconda del tipo di destinatario:

- Per i dipendenti: inadempimento contrattuale ai sensi degli articoli 2104 e 2106 del Codice Civile;
- Per amministratori e revisori: inosservanza dei doveri previsti dalla legge e dallo statuto (art. 2392 del Codice Civile);
- Per soggetti non dipendenti: inadempimento con applicazione di sanzioni contrattuali.

L'Organismo di Vigilanza (OdV) deve essere informato di ogni procedimento disciplinare in corso e verificare che tutti i soggetti siano informati del sistema sanzionatorio sin dall'inizio del loro rapporto con l'azienda.

## **7.4. Principi Generali Relativi alle Sanzioni**

Le sanzioni devono essere proporzionate e graduali in base alla gravità dell'infrazione. La determinazione della sanzione dipende da vari fattori, come:

- L'intenzionalità della violazione;
- La negligenza o imprudenza nel commettere la violazione;
- Le conseguenze dell'infrazione;
- La posizione del destinatario all'interno dell'organizzazione;
- Eventuali circostanze aggravanti o attenuanti, come precedenti sanzioni disciplinari;

- Il comportamento complessivo del destinatario, compreso il concorso di più soggetti nella violazione.

### 7.5. Sanzioni nei Confronti di Dipendenti

I dipendenti che violano le regole comportamentali del Modello sono soggetti a sanzioni disciplinari. Queste sanzioni seguono il sistema previsto dai Contratti Collettivi Nazionali del Lavoro e dalla Legge 300/70. Le sanzioni disciplinari includono:

1. **Richiamo Verbale:** per violazioni lievi o comportamenti negligenti;
2. **Richiamo Scritto:** per violazioni ripetute o gravi;
3. **Multa:** per violazioni che mettono in pericolo i beni aziendali;
4. **Sospensione dal Lavoro e dalla Retribuzione:** per gravi violazioni o comportamenti abitualmente negligenti;
5. **Licenziamento con Preavviso:** per comportamenti contrari agli interessi dell'azienda;
6. **Licenziamento senza Preavviso:** per violazioni gravi che possano compromettere l'integrità dell'azienda.

Ogni sanzione deve essere preceduta da una procedura di contestazione, con l'informazione al dipendente delle ragioni della sanzione.

### 7.6. Misure nei Confronti dei Soggetti di cui all'art. 5, 1° comma, lett. a) D.Lgs. 231/01

Nel caso in cui uno dei soggetti con funzioni di rappresentanza o direzione violi il Modello, l'OdV invia una relazione all'Organo amministrativo, indicando il soggetto responsabile, la condotta violata e le disposizioni del Modello violate. L'Organo amministrativo convoca il soggetto per discutere la violazione e determinare la sanzione, che può includere richiamo scritto, diffida, decurtazione del compenso o revoca dell'incarico.

### 7.7. Disciplina nei Rapporti con Collaboratori Esterni e Partners

Anche i collaboratori esterni e i partner commerciali sono soggetti a sanzioni in caso di violazione delle disposizioni contrattuali e del Codice Etico. Le sanzioni includono richiamo scritto, applicazione di clausole contrattuali specifiche e risarcimento del danno subito dall'azienda. L'OdV verifica che la Funzione referente segua correttamente la procedura di contestazione.

In ogni caso, l'azienda si riserva il diritto di richiedere il risarcimento del danno subito a causa delle violazioni.

## PARTE SPECIALE

### PREMESSA

La Parte Speciale del Modello ha la funzione di individuare, previa descrizione delle figure di reato contemplate dal Decreto ed astrattamente ipotizzabili in relazione all'attività svolta da COM.E, le aree a rischio di commissione dei reati individuati, indicando anche principi specifici di condotta (cd protocolli) relativi alla singola fattispecie criminosa con finalità di prevenzione, nonché gli specifici poteri di controllo affidati all'Organismo di Vigilanza. Obiettivo della Parte Speciale è che tutti i destinatari della stessa, ossia Dipendenti, Collaboratori, Organi Sociali, Consulenti e Partner di COM.E, conformino i propri comportamenti alle regole di condotta in essa contenute al fine di prevenire il verificarsi dei Reati in essa considerati.

Nello specifico, la Parte Speciale ha lo scopo di:

1. indicare le procedure che i Dipendenti, gli Organi Sociali, i Collaboratori, i Consulenti e Partner di COM.E sono chiamati ad osservare ai fini della corretta applicazione del Modello;
2. fornire ai responsabili delle funzioni aziendali e a tutte le funzioni di controllo, compreso l'Organismo di Vigilanza e il Sindaco Unico, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

La Parte Speciale del Modello di COM.E si compone di 13 (tredici) sezioni, distinte secondo la categoria dei reati astrattamente ipotizzabili nelle aree di attività a rischio.

Le sezioni delle quali si compone la presente parte speciale sono le seguenti tredici:

1. Reati contro la Pubblica Amministrazione
2. Reati societari
3. Reati informatici
4. Reati associativi
5. Reati di ricettazione, riciclaggio, impiego di denaro, beni o altre utilità di provenienza illecita e autoriciclaggio
6. Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare
7. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
8. Reati contro la personalità individuale: Intermediazione illecita e sfruttamento del lavoro
9. reati di xenofobia e razzismo
10. reati di abuso di mercato
11. Delitti in materia di violazione del diritto d'autore
12. Reati tributari
13. Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento dei valori

Inoltre, in allegato al Modello, sono riportati, a ulteriore completamento e dettaglio, la Matrice dei Rischi, le otto Procedure di evitamento dei reati e il Codice Etico, fermo restando il rimando agli altri documenti richiamati.

## IL SISTEMA DI ORGANIZZAZIONE E PREVENZIONE IN GENERALE

Tutte le attività compiute nell'ambito delle Aree a Rischio devono essere svolte conformandosi alle leggi vigenti e alle regole prescritte dal Modello, dal Codice Etico e dalle procedure gestionali ed operative esistenti.

In linea generale, il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative. La Società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati ai principi generali di:

- conoscibilità all'interno della Ente;
- chiara e formale delimitazione dei ruoli e funzioni;
- chiara descrizione delle linee di riporto.

Le procedure interne adottate da COM.E nelle aree a rischio di commissione dei reati inseriti nel novero del D.Lgs. 231/2001 sono fondate sui seguenti principi cardine:

- separatezza, all'interno di ciascun processo, tra il soggetto che lo inizia (impulso decisionale), il soggetto che lo esegue e lo conclude, e il soggetto che lo controlla;
- tracciabilità scritta di ciascun passaggio rilevante del processo;
- adeguatezza del livello di formalizzazione;
- il sistema di controllo interno, e quindi le procedure aziendali, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale ed organizzativa, ed il sistema di controllo della gestione;
- le norme inerenti al sistema amministrativo, contabile, finanziario, di *reporting*;
- l'attivazione di corsi di formazione e la diffusione di una propaganda di sensibilizzazione a tutti i livelli organizzativi;
- in generale, la normativa italiana e straniera applicabile.

Inoltre, i sistemi premianti dei soggetti con poteri di spesa o facoltà decisionali a rilevanza esterna devono essere basati su target di performance sostanzialmente raggiungibili.

Le regole di comportamento che devono essere osservate dal Personale, dai membri degli Organi Sociali e dai Collaboratori di COM.E (i "Destinatari"), nella misura in cui essi sono coinvolti nelle Aree a Rischio, in relazione ai diversi ruoli e obblighi nei confronti di COM.E, al fine di impedire il verificarsi di reati 231, sono riportate nei seguenti documenti:

- Codice Etico;
- Procedura n.1. Selezione e assunzione personale;
- Procedura n.2. Gestione del personale;
- Procedura n.3. Gare;
- Procedura n.4. Acquisti di beni e servizi;

- Procedura n.5. Contabilità, Adempimenti e Bilancio;
- Procedura n.6. Budgeting, Tesoreria e Controllo;
- Procedura n.7. Rapporti con la P.A.;
- Procedura n.8. Flussi informativi da e verso OdV;
- Procedura delle segnalazioni (Whistleblowing);
- Manuale Operativo della Qualità;
- DVR (Documento di valutazione dei rischi);
- DPD (Documento di protezione dei dati)

Le suddette Procedure sono al loro interno completate da Flow Chart e Griglie dei Controlli, proprio al fine di essere strumenti massimamente efficaci nell'effettivo utilizzo ordinario, anche per quanto attiene alle evidenze e ai controlli.

## IL SISTEMA DI DELEGHE E PROCURE

In linea di principio, il sistema di deleghe e procure deve essere caratterizzato da elementi di "sicurezza" ai fini della prevenzione dei Reati (rintracciabilità ed evidenziabilità delle attività a rischio) e, nel contempo, consentire comunque la gestione efficiente dell'attività aziendale.

Si intende per "delega" quell'atto interno di attribuzione di funzioni e compiti, con relativo trasferimento di responsabilità dal delegante al delegato, riflesso nel sistema di comunicazioni organizzative.

Si intende per "procura" il negozio giuridico unilaterale con cui la Ente attribuisce dei poteri di rappresentanza nei confronti dei terzi. Ai titolari di una funzione aziendale che necessitano, per lo svolgimento dei loro incarichi, di poteri di rappresentanza viene conferita una "procura generale funzionale" di estensione adeguata e coerente con le funzioni ed i poteri di gestione attribuiti al titolare attraverso la "delega".

I requisiti essenziali del sistema di deleghe, ai fini di una efficace prevenzione dei Reati sono:

- a) tutti coloro che intrattengono per conto di COM.E rapporti con la P.A. devono essere dotati di delega formale in tal senso;
- b) le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma, ed essere aggiornate in conseguenza dei mutamenti organizzativi;
- c) ciascuna delega deve definire in modo specifico ed inequivoco:
  - i poteri del delegato;
  - il soggetto (organo o individuo) delegante;
- d) i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- e) il delegato deve disporre di poteri decisionali e di spesa adeguati alle funzioni conferitegli.

I requisiti essenziali del sistema di attribuzione delle procure, ai fini di una efficace prevenzione dei Reati, sono i seguenti:

- a) le procure generali funzionali sono conferite esclusivamente a soggetti appartenenti alla Società o, nel caso dei Collaboratori, Professionisti e/o Consulenti, dotati di specifico contratto di incarico, che descriva i relativi poteri di gestione e, ove necessario, sono accompagnate da apposita comunicazione che fissi l'estensione dei poteri di rappresentanza ed eventualmente i limiti numerici di spesa, richiamando comunque il rispetto dei vincoli posti dai processi di approvazione del budget e degli eventuali extra budget e dai processi di monitoraggio delle attività a rischio da parte di funzioni diverse;
- b) la procura può essere conferita a persone fisiche espressamente individuate nella procura stessa, oppure a persone giuridiche, che agiranno a mezzo di propri procuratori investiti, nell'ambito della stessa, di analoghi poteri;
- c) l'Organo amministrativo garantisce un aggiornamento tempestivo delle procure, attribuendo, modificando e revocando le procure in base alle necessità aziendali (assunzione di nuove responsabilità, trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita la procura, dimissioni, licenziamento, ecc.).

L'OdV verifica nel primo periodo del suo insediamento e poi periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative (tali sono quei documenti interni all'azienda con cui vengono conferite le deleghe), raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrispondano ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie.

## **1. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE**

### **1.1 Descrizione delle fattispecie di reato**

La presente sezione della Parte Speciale si riferisce ai reati astrattamente ipotizzabili nell'ambito dei rapporti fra COM.E e la P.A.

Di seguito si descrivono brevemente le singole fattispecie contemplate nel Decreto agli artt. 24 e 25, limitatamente alle figure di reato che appaiono astrattamente ipotizzabili, tenuto conto della realtà operativa di COM.E.

#### ***Malversazione a danno dello Stato o dell'Unione Europea (art. 316-bis c.p.)***

Tale ipotesi di reato si perfeziona nel caso in cui un soggetto, estraneo alla pubblica amministrazione, dopo avere ricevuto contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, da parte dello Stato italiano o da altro ente pubblico o dalle Comunità europee, non proceda all'utilizzo delle somme ottenute per le finalità cui erano destinate.

Tenuto conto che il momento consumativo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

### ***Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.)***

Tale ipotesi di reato si perfeziona nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute - si ottengano, per sé o per altri, senza averne diritto, contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee.

Le pene sono aumentate se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso della sua qualità o dei suoi poteri e se il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000.

In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316-bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti. Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

### ***Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art. 640, comma 2 n. 1, c.p.)***

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea) o col pretesto di far esonerare taluno dal servizio militare.

Tale reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta) al fine di ottenere l'aggiudicazione della gara stessa.

### ***Istigazione alla corruzione (art. 322 c.p.)***

Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione - ovvero a fronte della offerta o promessa di denaro od altra utilità non dovuti, a un pubblico ufficiale o a un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri - questi rifiuti l'offerta illecitamente avanzatagli.

### ***Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)***

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno a terzi. In concreto, può integrarsi il reato in esame qualora, una volta ottenuto un finanziamento,

venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

Tale ipotesi di reati si configura anche se il fatto è commesso con sostituzione dell'identità digitale in danno di uno o più soggetti.

***Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (Art. 322 bis)***

Le disposizioni inerenti ai reati citati in intestazione, si applicano anche quando tali delitti sono stati commessi da:

- 1) membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;
- 2) funzionari e agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
- 3) persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
- 4) membri e addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;
- 5) coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;
- 5-bis) giudici, procuratori, procuratori aggiunti, funzionari e agenti della Corte penale internazionale, persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, membri ed addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale.
- 5-ter) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali;
- 5-quater) ai membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e ai giudici e funzionari delle corti internazionali.

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

- 1) alle persone indicate nel primo comma del presente articolo;
- 2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali.

***Concussione (art. 317 c.p.)***

Tale ipotesi di reato si perfeziona quando un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua qualità o dei suoi poteri, costringa taluno a dare o promettere indebitamente a sé o ad altri, denaro o altre utilità non dovutegli. Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal Decreto. In particolare, tale forma

di reato potrebbe ravvisarsi nell'ipotesi in cui un dipendente od un agente della Ente concorra nel reato del pubblico ufficiale, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute (sempre che, da tale comportamento, derivi in qualche modo un vantaggio per la Ente).

***Corruzione per l'esercizio della funzione (art. 318 c.p.) e corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)***

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceva (o ne accetti la promessa), per sé o per altri, denaro o altra utilità al fine di omettere o ritardare o compiere un atto del suo ufficio o un atto contrario al suo dovere d'ufficio (determinando un vantaggio in favore di colui che ha offerto denaro o altra utilità).

L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetta denaro per garantire l'aggiudicazione di una gara).

Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

Si sottolinea infine come l'oggetto della promessa possa consistere sia in una somma di danaro corrisposta al pubblico ufficiale, anche indirettamente o per interposta persona, sia in qualsiasi altra utilità anche di carattere non patrimoniale a favore del pubblico ufficiale o di soggetti a lui collegati (si pensi ad esempio all'attribuzione di una consulenza fittizia o all'assunzione di un familiare).

***Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)***

Tale norma punisce, sia il pubblico ufficiale e/o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induca il privato a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità, sia il privato che perfeziona la dazione o la promessa dell'indebito.

***Corruzione di persona incaricata di un pubblico servizio (art. 320 c. p.)***

Tale ipotesi di reato si configura nel caso in cui anche un incaricato di pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceva (o ne accetti la promessa), per sé o per altri, denaro o altra utilità per omettere o ritardare un atto del suo ufficio ovvero per compiere un atto contrario al suo dovere d'ufficio (determinando un vantaggio in favore di colui che ha offerto denaro o altra utilità).

***Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)***

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche (da parte dello Stato, di altri enti pubblici o delle Comunità europee).

Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

### ***Traffico di influenze illecite (art. 346 bis c.p.)***

Fuori dai casi di concorso nei reati di cui agli articoli 318, 319, 319-ter e nei reati di corruzione di cui all'articolo 322-bis, è costituito dalla condotta di chiunque utilizzando intenzionalmente allo scopo relazioni esistenti con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità economica, per remunerare un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, in relazione all'esercizio delle sue funzioni, ovvero per realizzare un'altra mediazione illecita.

Ai fini di cui al primo comma, per altra mediazione illecita si intende la mediazione per indurre il pubblico ufficiale o l'incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis a compiere un atto contrario ai doveri d'ufficio costituente reato dal quale possa derivare un vantaggio indebito.

La stessa pena si applica a chi indebitamente dà o promette denaro o altra utilità economica.

La pena è aumentata se il soggetto che indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità economica riveste la qualifica di pubblico ufficiale o di incaricato di un pubblico servizio o una delle qualifiche di cui all'articolo 322-bis.

La pena è altresì aumentata se i fatti sono commessi in relazione all'esercizio di attività giudiziarie o per remunerare il pubblico ufficiale o l'incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis in relazione al compimento di un atto contrario ai doveri d'ufficio o all'omissione o al ritardo di un atto del suo ufficio.

### ***Corruzione in atti giudiziari (art. 319-ter)***

Tale ipotesi di reato si configura nel caso in cui un soggetto, parte di un procedimento giudiziario, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario).

### ***Frode nelle pubbliche forniture (art. 356 c.p.)***

Tale ipotesi ricorre allorché un soggetto commetta frode – che secondo una parte della giurisprudenza più severa si identifica nella semplice mala fede contrattuale, a prescindere cioè dall'utilizzo di artifici e raggiri- nell'esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali che gli derivano da un contratto di fornitura concluso con lo Stato, o con un altro ente pubblico, ovvero con un'impresa esercente servizi pubblici o di pubblica necessità.

La persona fisica autrice del reato è punita con la reclusione da uno a cinque anni e con la multa non inferiore a euro 1.032.

### ***Turbata libertà degli incanti (art. 353 c.p.)***

La fattispecie di reato è stata introdotta dalla L. n. 137/2023.

Tale ipotesi di reato si configura nel caso in cui un soggetto, con violenza o minaccia o con doni promesse collusioni o altri mezzi fraudolenti impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche amministrazioni ovvero ne allontana gli offerenti.

La pena è aumentata se il colpevole è persona preposta dalla legge o dall'autorità agli incanti o alle licitazioni suddette.

Le pene stabilite in questo articolo si applicano anche nel caso di licitazioni private per conto di privati dirette da un pubblico ufficiale o da persona legalmente autorizzata ma sono ridotte alla metà.

### ***Turbata libertà del procedimento di scelta del contraente (art. 353 bis c.p.)***

La fattispecie di reato è stata introdotta dalla L. n. 137/2023 e punisce la condotta di chiunque con violenza o minaccia o con doni promesse collusioni o altri mezzi fraudolenti turba il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione

#### **1.1.1 La Pubblica Amministrazione**

L'individuazione delle fattispecie di reato contro la Pubblica Amministrazione rilevanti ai sensi del Decreto non può prescindere dalla esatta individuazione del significato di "Pubblica Amministrazione" e dalla fissazione di criteri generali idonei ad individuare i "soggetti passivi" dei reati rilevanti ai sensi del Decreto, soggetti la cui qualifica è necessaria ad integrare le fattispecie criminose previste dal Decreto.

#### **1.1.2 Enti della Pubblica Amministrazione**

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

Sebbene non esista nel codice penale una definizione di Pubblica Amministrazione, in base a quanto stabilito nella Relazione Ministeriale al codice stesso ed in relazione ai reati in esso previsti, sono ritenuti appartenere alla pubblica amministrazione quegli enti che svolgano "tutte le attività dello Stato e degli altri enti pubblici".

Nel tentativo di formulare una preliminare classificazione di soggetti giuridici appartenenti a tale categoria è possibile richiamare, da ultimo, l'art. 1, comma 2, D.Lgs. 165/2001 in tema di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, il quale definisce come amministrazioni pubbliche tutte le amministrazioni dello Stato.

Si riepilogano qui di seguito i caratteri distintivi degli enti della Pubblica Amministrazione.

<u>Ente della Pubblica Amministrazione</u>	Qualsiasi ente che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.
<u>Pubblica Amministrazione</u>	Tutte le attività dello Stato e degli altri enti pubblici.

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

1. Istituti e scuole di ogni ordine e grado e le istituzioni educative;
2. Enti ed amministrazioni dello Stato ad ordinamento autonomo, quali:
  - 2.1 Ministeri;
  - 2.2 Camera e Senato;
  - 2.3 Dipartimento Politiche Comunitarie;
  - 2.4 Autorità Garante della Concorrenza e del Mercato;
  - 2.5 Autorità per l'Energia Elettrica ed il Gas;
  - 2.6 Autorità per le Garanzie nelle Comunicazioni;
  - 2.7 Banca d'Italia;
  - 2.8 Consob;
  - 2.9 Autorità Garante per la protezione dei dati personali;
  - 2.10 Agenzia delle Entrate;
  - 2.11 Regioni;
  - 2.12 Province;
  - 2.13 Comuni;
  - 2.14 Comunità montane, loro consorzi e associazioni;
  - 2.15 Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
3. Tutti gli enti pubblici non economici nazionali, regionali e locali, quali:
  - 3.1 INPS (comprese le sopresse gestioni ex- INPDAL ed ex-INPDAP);
  - 3.2 CNR;
  - 3.3 INAIL;
  - 3.4 ISTAT;
  - 3.5 ENASARCO;
  - 3.6 IVASS;
  - 3.7 ASL;
  - 3.8 ENTI E MONOPOLI DI STATO.

In relazione all'attività effettivamente esercitata da COM.E, le entità identificabili come Pubblica Amministrazione di maggior rilievo per le attività definibili come "core" sono costituite dai Ministeri e dalla Presidenza del Consiglio dei Ministri per la fornitura di servizi giornalistici.

### 1.1.3 Pubblici Ufficiali ed Incaricati di Pubblico Servizio

È necessario precisare che i reati contro la Pubblica Amministrazione rilevanti ai sensi del Decreto necessitano, ai fini del loro perfezionamento, che il loro soggetto passivo (o, in alcuni casi, attivo) rivesta la qualifica di “*Pubblico Ufficiale*” o di “*Incaricato di Pubblico Servizio*”. Pertanto, i reati descritti non potranno considerarsi realizzati qualora non siano stati commessi da, o a carico di, soggetti che pur operanti nell'ambito della Pubblica Amministrazione non rivestano quella particolare qualifica funzionale.

#### *I Pubblici Ufficiali*

Ai sensi dell'art. 357, primo comma, codice penale, è considerato pubblico ufficiale “*agli effetti della legge penale*” colui il quale esercita “*una pubblica funzione legislativa, giudiziaria o amministrativa*”.

Il secondo comma si preoccupa poi di definire la nozione di “*pubblica funzione amministrativa*”. Non è stata invece compiuta un'analogia attività definitoria per precisare la nozione di “*funzione legislativa*” e “*funzione giudiziaria*” in quanto la individuazione dei soggetti che rispettivamente le esercitano non ha di solito dato luogo a particolari difficoltà interpretative.

Pertanto, il secondo comma dell'articolo in esame precisa che, agli effetti della legge penale “*è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi*”.

In altre parole, è definita pubblica la funzione amministrativa disciplinata da “*norme di diritto pubblico*”, ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Il secondo comma dell'art. 357 c.p. traduce poi in termini normativi alcuni dei principali criteri di massima individuati dalla giurisprudenza e dalla dottrina per differenziare la nozione di “*pubblica funzione*” da quella di “*servizio pubblico*”.

I caratteri distintivi della prima figura possono essere sintetizzati come segue:

#### Pubblico Ufficiale

Colui che esercita una pubblica funzione legislativa, giudiziaria o amministrativa.

#### Pubblica funzione amministrativa

Funzione disciplinata da norme di diritto pubblico e da atti autoritativi, estrinsecantesi nella formazione e nella manifestazione della volontà della Pubblica Amministrazione, o nell'esercizio di poteri autoritativi o certificativi.

#### Norme di diritto pubblico

Norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico.

### ***Gli Incaricati di Pubblico Servizio***

*Secondo l'articolo 358 c.p., “sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale”.*

Il “servizio”, affinché possa definirsi pubblico, deve essere disciplinato – così come la “pubblica funzione” - da norme di diritto pubblico ma, rispetto alla pubblica funzione, non presuppone l'esercizio di poteri di natura certificativa, autorizzativa e deliberativa.

La legge, inoltre, precisa che non può mai costituire “servizio pubblico” lo svolgimento di “semplici mansioni di ordine” né la “prestazione di opera meramente materiale”.

La giurisprudenza ha individuato una serie di “indici rivelatori” del carattere pubblicistico dell'ente, per i quali è emblematica la casistica in tema di per azioni a partecipazione pubblica. In particolare, si fa riferimento ai seguenti indici:

1. la sottoposizione ad un'attività di controllo e di indirizzo a fini sociali, nonché ad un potere di nomina e revoca degli amministratori da parte dello Stato o di altri enti pubblici;
2. la presenza di una convenzione e/o concessione con la Pubblica Amministrazione;
3. l'apporto finanziario da parte dello Stato;
4. la presenza dell'interesse pubblico in seno all'attività economica.

Sulla base di quanto sopra riportato, l'elemento discriminante per indicare se un soggetto rivesta o meno la qualità di “incaricato di un pubblico servizio” è rappresentato non dalla natura giuridica assunta o detenuta dall'ente, ma dalle funzioni affidate al soggetto, le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale.

I caratteri peculiari della figura dell'incaricato di pubblico servizio sono sintetizzati nel seguente specchio:

#### Incaricati di Pubblico Servizio

Coloro che, a qualunque titolo, prestano un pubblico servizio.

#### Pubblico servizio

Un'attività:

1. disciplinata da norme di diritto pubblico;
2. caratterizzata dalla mancanza di poteri di natura deliberativa, autorizzativa e certificativa (tipici della pubblica funzione amministrativa).

Non può mai costituire pubblico servizio lo svolgimento di semplici mansioni di ordine né la prestazione di opera meramente materiale.

## **1.2 Le Aree a Rischio/Attività sensibili nei rapporti con la P.A.**

Le Aree a Rischio, che COM.E ha individuato negli ambiti della propria attività implicanti rapporti con la P.A. sono le seguenti:

1. Selezione e assunzione del personale
2. Gestione del Personale
3. Formazione
4. Gare
5. Selezione, contrattualizzazione e monitoraggio del Fornitore
6. Fatturazione
7. Gestione della Contabilità
8. Adempimenti civilistici, previdenziali e fiscali
9. Budgeting e controllo di gestione
10. Gestione incassi e pagamenti
11. Gestione cassa
12. Visite Ispettive P.A.
13. Comunicazione, incontri e richieste di autorizzazioni P.A.
14. Gestione della sicurezza, ambiente e qualità
15. Trattamento dei dati sensibili e gestione del sistema informativo
16. Gestione dei servizi giornalistici.

## **1.3 Principi di condotta nelle Aree a Rischio**

I seguenti divieti si applicano sia ai Dipendenti ed ai membri degli Organi Sociali di COM.E – in via diretta – sia ai Collaboratori, ai Consulenti e ai Partner in forza di apposite clausole contrattuali.

A fini di prevenzione, è fatto divieto di:

- ✓ effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri;
- ✓ distribuire e/o ricevere omaggi e regali, vale a dire ogni forma di regalo offerto eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore illeciti nella conduzione di qualsiasi attività aziendale. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società. In ogni caso, gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere benefico, scientifico, culturale, o l'immagine di COM.E;
- ✓ accordare o promettere favori di qualsivoglia genere e specie (assunzione, stage, contratti di consulenza etc.) o accordare vantaggi di qualsiasi natura in favore di terzi (anche privati), pubblici ufficiali o incaricati di pubblico servizio appartenenti alla Pubblica Amministrazione, agli enti pubblici e/o ai soggetti ad essi assimilati dello Stato italiano, delle Comunità Europee e degli Stati

esteri, nonché a beneficio di altri individui o entità giuridiche comunque riconducibili alla sfera di interesse dei soggetti sopra indicati;

- ✓ fornire, redigere o consegnare ai pubblici ufficiali o agli incaricati di pubblico servizio appartenenti alla Pubblica Amministrazione, agli enti pubblici e/o ai soggetti ad essi assimilati dello Stato italiano, delle Comunità Europee e degli Stati esteri dichiarazioni, dati o documenti in genere aventi contenuti inesatti, errati, incompleti, lacunosi e/o falsi al fine di ottenere certificazioni, permessi, autorizzazioni e/o licenze di qualsivoglia genere o specie, o conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- ✓ presentare dichiarazioni non veritiere ad organismi pubblici al fine di conseguire finanziamenti, contributi o erogazioni di qualsiasi natura;
- ✓ destinare somme ricevute da organismi pubblici a titolo di erogazioni, contributi o finanziamenti a scopi diversi da quelli per cui sono stati ottenuti;
- ✓ assegnare o delegare l'uso di auto aziendali, sia personali sia in pool, a soggetti diversi da quelli espressamente autorizzati dalla Società;
- ✓ ricevere prestazioni da parte di società di service, di consulenti e di fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale con gli stessi;
- ✓ effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine di COM.E;
- ✓ riconoscere compensi in favore di fornitori di beni e servizi nonché di consulenti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- ✓ mettere in atto o favorire operazioni in conflitto di interesse, nonché attività in grado di interferire con la capacità di assumere decisioni imparziali nel rispetto del Codice Etico e delle normative applicabili;
- ✓ farsi rappresentare da un consulente o da altro soggetto "terzo" quando si possano creare conflitti d'interesse;
- ✓ effettuare azioni finalizzate a sollecitare o ad ottenere da Istituzioni Pubbliche informazioni riservate al di là di quanto consentito dalla legge.

È altresì fatto obbligo di:

- ✓ gestire in modo trasparente e nel rispetto dei poteri di rappresentanza riconosciuti all'interno della Società qualsiasi rapporto professionale instaurato con membri della Pubblica Amministrazione o con soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio;
- ✓ adottare un comportamento improntato ai principi di integrità, onestà, trasparenza e buona fede in relazione a qualsiasi attività da intraprendersi nell'ambito di ogni attività aziendale;
- ✓ garantire il rispetto dei principi di correttezza, trasparenza e buona fede in qualsiasi rapporto professionale che si intraprenda con membri della Pubblica Amministrazione o con soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio;
- ✓ rifiutare qualsiasi pressione indebita da parte di un pubblico ufficiale o di un incaricato di pubblico servizio, anche qualora ne siano ventilati come possibili conseguenze vantaggi per la Società;
- ✓ definire per iscritto qualsiasi tipo di accordo con consulenti, professionisti e collaboratori in modo da rendere evidenti i termini dell'accordo stesso, con particolare riguardo alla tipologia di incarico/transazione e alle condizioni economiche sottostanti nel rispetto delle deleghe e procure definite;
- ✓ dare immediata comunicazione al Presidente degli omaggi e/o dei regali ricevuti da funzionari o esponenti pubblici e provvedere direttamente, o tramite la Società, alla riconsegna al donante in caso di divergenza rispetto ai predetti criteri.

I **Protocolli specifici** per la prevenzione dei reati di cui sopra sono riportati nelle Procedure allegate al presente Modello.

## 2. REATI SOCIETARI

### 2.1 Le fattispecie dei reati societari (art. 25- *ter* del Decreto)

La presente Parte Speciale si riferisce ai reati societari, ossia ai reati commessi da soggetti qualificati nell'ambito dell'attività di gestione sociale, descrivendone brevemente qui di seguito le singole fattispecie contemplate nel Decreto all'art. 25 – *ter* astrattamente configurabili nell'ambito della Società.

#### *False comunicazioni sociali (artt. 2621, 2621 bis e 2622 c.c.)*

Questo reato si perfeziona:

- con la consapevole rappresentazione, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge e dirette ai soci, ai creditori o al pubblico, di fatti materiali non rispondenti al vero e concretamente idonei ad indurre in errore i destinatari della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene con l'intenzione di ingannare i soci, i creditori o il pubblico, ovvero
- con l'omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge.

Si precisa che:

- la condotta deve essere rivolta a conseguire per l'autore del reato, o per terzi, un ingiusto profitto;
- le informazioni false od omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene;
- la responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;
- i fatti previsti dall'art. 2621 sono puniti anche se di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta (art. 2621 bis c.c.).

#### *Corruzione tra privati (art. 2635 comma *ter* c.c.)*

La fattispecie di corruzione tra privati è stata da ultimo modificata dal D. Lgs n. 38 del 2017. Ora il nuovo reato prevede che: *“Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i*

*liquidatori, di Ente o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni. Si applica la stessa pena se il fatto è commesso da chi nell'ambito organizzativo della Ente o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo.*

*Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.*

*Chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuti alle persone indicate nel primo e nel secondo comma, è punito con le pene ivi previste.*

*Le pene stabilite nei commi precedenti sono raddoppiate se si tratta di Ente con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.*

*Si procede a querela della persona offesa, salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi.*

*Fermo quanto previsto dall'articolo 2641, la misura della confisca per valore equivalente non può essere inferiore al valore delle utilità date, promesse o offerte”.*

La fattispecie si configura come un reato a concorso necessario, per cui è essenziale che siano poste in essere due condotte corruttive:

- a. la condotta corruttiva attiva di colui che offre, dà o promette denaro o altra utilità ai soggetti di cui all'art. 2635 co.1;
- b. la condotta corruttiva passiva di colui che- avendo ricevuto o essendo destinatario di una promessa o dazione di denaro o altra utilità, per sé o per altri, o avendola sollecitata- compia od ometta atti, in violazione dei propri obblighi d'ufficio o di fedeltà.

Si noti che la condotta corruttiva passiva può essere compiuta solo dai soggetti specificamente elencati nel comma primo dell'art. 2635 c.c. e che, quindi, possono essere corrotti solo coloro che ricoprono i seguenti ruoli:

- gli amministratori;
- i direttori generali;
- i dirigenti preposti alla redazione dei documenti contabili societari;
- i sindaci;
- i liquidatori;
- soggetti che esercitano funzioni direttive;

(di seguito definiti complessivamente anche i “**Soggetti Corruptibili**”).

La nuova formulazione- a seguito della recente novella legislativa- estende ora il novero dei soggetti attivi includendo tra gli autori del reato, oltre a coloro che rivestono posizioni apicali di

amministrazione o di controllo, anche coloro che svolgono attività lavorativa con l'esercizio di funzioni direttive presso Ente o enti privati.

La responsabilità amministrativa dell'ente ex D.Lgs. 231/2001 si estende solo nei confronti dell'ente nel cui interesse o vantaggio ha operato il soggetto corruttore attivo.

La novella ha ora ampliato le condotte attraverso cui si perviene all'accordo corruttivo includendo nella corruzione passiva anche la sollecitazione del denaro o di altra utilità non dovuti da parte del soggetto "intraneo" (ossia il soggetto attivo nel reato proprio), qualora ad essa segua la conclusione dell'accordo corruttivo mediante promessa o dazione di quanto richiesto; ed estendendo altresì la fattispecie di corruzione attiva all'offerta delle utilità non dovute da parte dell'estraneo, qualora essa venga accettata dal soggetto "intraneo".

Inoltre, tra le modalità della condotta, sia nell'ipotesi attiva che in quella passiva, a seguito della novella è stata prevista la commissione della stessa anche per interposta persona.

Significativo, infine, il fatto che nel nuovo testo dell'art. 2635 c.c. scompaia il riferimento alla necessità che la condotta «cagioni nocumento alla Ente», con conseguente trasformazione della fattispecie da reato di danno a reato di pericolo.

#### ***Istigazione alla corruzione tra privati (art. 2635 bis c.c.)***

Il D. Lgs n. 38 del 2017 ha introdotto tale nuova fattispecie di reato, che prevede che: *“chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di Ente o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo. La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di Ente o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per se' o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata. Si procede a querela della persona offesa”.*

La novella del D.Lgs. 38/2017 ha anche introdotto l'**art. 2635-ter** del codice civile disciplina le pene accessorie, stabilendo che *“La condanna per il reato di cui all'articolo 2635, primo comma, importa in ogni caso l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese di cui all'articolo 32-bis del codice penale nei confronti di chi sia già stato condannato per il medesimo reato o per quello di cui all'articolo 2635-bis, secondo comma”.*

Da tali novità in tema di reati societari discendono modifiche al d.lgs. 231/2001 in tema di responsabilità degli enti per illeciti da reato:

- per il delitto di corruzione tra privati, nei casi previsti dal terzo comma dell'articolo 2635, si applica ora la sanzione pecuniaria da 400 a 600 quote (anziché da 200 a 400);
- per l'istigazione alla corruzione da 200 a 400 quote.

Alla sanzione pecuniaria si sommano le sanzioni interdittive di cui all'art. 9 del d.lgs. 231/2001 che, si ricorda, sono le seguenti:

- interdizione dall'esercizio dell'attività;
- sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi;
- divieto di pubblicizzare beni o servizi.

### ***Aggiotaggio (Art. 2637)***

Tale norma incriminatrice speciale punisce chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.

### ***Omessa comunicazione del conflitto di interessi (Art. 2629 bis c.c.)***

Tale reato si configura allorché l'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante viola gli obblighi di comunicazione dell'esistenza del conflitto, se dalla violazione siano derivati danni alla società o a terzi.

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

La condotta criminosa si realizza attraverso l'esposizione nelle comunicazioni alle autorità di vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero con l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima.

### ***Impedito controllo (art. 2625 c.c.)***

Il reato consiste nell'impedire od ostacolare, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali, ovvero alle società di revisione.

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

La "condotta tipica", necessaria per il perfezionamento di questo reato, richiede che si determini, con atti simulati o con frode, la maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

### ***Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)***

Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.

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

### ***Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)***

Questo reato si perfeziona con l'acquisto o la sottoscrizione di azioni o quote sociali o della società controllante, che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

Si precisa che, se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio, relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

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

La fattispecie si perfeziona con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori. Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

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

La "condotta tipica", necessaria per il perfezionamento di questo reato, prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione, anche simulata, dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli.

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

Tale ipotesi si ha quando: viene formato o aumentato fittiziamente il capitale della società mediante attribuzione di azioni o quote sociali per una somma inferiore al loro valore nominale; vengono sottoscritte reciprocamente azioni o quote; vengono sopravvalutati in modo rilevante i conferimenti dei beni in natura, i crediti ovvero il patrimonio della società, nel caso di trasformazione.

### ***False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D. Lgs. 19/2023)***

Il 22 marzo 2023 è entrato in vigore il D. Lgs. 19/2023 recante “Attuazione della direttiva (UE)

2019/2121 del Parlamento europeo e del Consiglio, del 27 novembre 2019, che modifica la direttiva (UE) 2017/1132 per quanto riguarda le trasformazioni, le fusioni e le scissioni transfrontaliere”, che ha introdotto un nuovo reato presupposto da cui può derivare la responsabilità amministrativa degli enti ai sensi del D. Lgs. 231/2001.

L’art. 54 del D. Lgs. 19/2023 punisce con la reclusione da 6 mesi a 3 anni *“chiunque, al fine di far apparire adempiute le condizioni per il rilascio del certificato preliminare di cui all’articolo 29, forma documenti in tutto o in parte falsi, altera documenti veri, rende dichiarazioni false oppure omette informazioni rilevanti”*. In caso di condanna ad una pena non inferiore a mesi 8 di reclusione, al responsabile sarà applicata altresì la pena accessoria dell’interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese, prevista dall’art. 32-bis c.p. Dunque, la condotta si realizza mediante la formazione di documenti falsi, l’alterazione di documenti veri, la presentazione di false dichiarazioni, ovvero l’omissione di informazioni rilevanti. Con riferimento all’elemento soggettivo, il delitto è punito a titolo di dolo specifico consistente nel fine di far apparire adempiute le condizioni per il rilascio del certificato preliminare di cui all’art. 29 del D. Lgs. 19/2023.

## **2.2 Le Aree a Rischio/Sensibili nell’ambito dell’attività di gestione societaria**

Le Aree Sensibili che COM.E ha individuato nell’ambito dell’attività di gestione societaria interna sono i seguenti:

1. Selezione e assunzione del personale
2. Gestione del Personale
3. Formazione
4. Gare
5. Selezione, contrattualizzazione e monitoraggio del Fornitore
6. Fatturazione
7. Gestione della Contabilità
8. Adempimenti civilistici, previdenziali e fiscali
9. Budgeting e controllo di gestione
10. Gestione incassi e pagamenti
11. Gestione cassa
12. Gestione della sicurezza e ambiente e qualità
13. Trattamento dei dati sensibili
14. Gestione dei servizi giornalistici

## **2.3 Principi di condotta nelle Aree a Rischio**

Nel compimento delle attività di gestione sociale maggiormente esposte al rischio di commissione dei reati rilevanti ai sensi dell'articolo 25-*ter* del Decreto, è fatto divieto agli Organi Sociali di COM.E, ed ai Dipendenti, Collaboratori e Consulenti nella misura necessaria alla funzioni dagli stessi svolte, di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25- *ter* del Decreto); sono altresì proibite le violazioni ai principi di condotta indicati nella presente sezione ed alle procedure adottate da COM.E per la gestione sociale.

In particolare, sono stabiliti i seguenti obblighi:

- ✓ tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
- ✓ tenere comportamenti corretti, nel rispetto delle norme di legge e delle procedure aziendali interne, ponendo la massima attenzione ed accuratezza nell'acquisizione, elaborazione ed illustrazione dei dati contabili, necessari per consentire una rappresentazione chiara della situazione patrimoniale, economica e finanziaria della Società e sull'evoluzione della sua attività;
- ✓ osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- ✓ salvaguardare il regolare funzionamento della Società e degli organi sociali garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- ✓ tenere un comportamento corretto nei rapporti di collaborazione e nelle transazioni commerciali (ad esempio con Banche e Assicurazioni), non riconoscendo o promettendo denaro o altra utilità per indurre la controparte a compiere e/o ad omettere atti con violazione dei propri obblighi e con indebito interesse e/o vantaggio a favore della Società;
- ✓ dare o promettere denaro, beni o altra utilità estranea all'oggetto del contratto durante o a motivo delle trattative commerciali in corso.

Nell'ambito dei suddetti comportamenti è fatto divieto di:

- a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società;
- b) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- c) illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della Società e sull'evoluzione della sua attività;
- d) ripartire eventuali utili determinati dalla gestione in un determinato esercizio;

e) porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino, lo svolgimento dell'attività di controllo e di revisione da parte dell'organo di controllo (Revisore dei Conti);

f) determinare o influenzare l'assunzione delle deliberazioni del Consiglio dei Benemeriti, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della propria volontà.

Segnatamente, per ogni operazione contabile deve essere conservata agli atti sociali una adeguata documentazione di supporto dell'attività svolta in modo da consentire:

- l'agevole registrazione contabile;
- l'individuazione dei diversi livelli di responsabilità;
- la ricostruzione accurata dell'operazione, anche al fine di ridurre la probabilità di errori interpretativi.

I **Protocolli specifici** per la prevenzione dei reati di cui sopra sono riportati nelle Procedure allegate al presente Modello.

### **3. REATI INFORMATICI**

#### **3.1 Descrizione delle fattispecie di reato**

L'articolo 24- *bis* del Decreto prevede la responsabilità amministrativa dell'ente per alcune fattispecie di reati commessi in violazione delle norme in materia di sistemi informatici e trattamento dei dati personali.

Si descrivono brevemente, qui di seguito, le singole fattispecie contemplate nel Decreto all'art. 24 – *bis*.

Anche in questo caso, le condotte contemplate nel presente paragrafo generano la responsabilità amministrativa da reato dell'ente esclusivamente quando siano poste in essere a vantaggio o nell'interesse di quest'ultimo.

#### ***Falsità in documenti informatici (art. 491-bis c.p.)***

Il reato previsto dall'art. 491 bis c.p. è stato da ultimo novellato dall'art. 2, comma 1, lett. e), D.Lgs. 15 gennaio 2016, n. 7.

La fattispecie prende ora in considerazione unicamente i documenti informatici pubblici, escludendo invece dalla penale rilevanza le falsità in atti privati.

Il nuovo testo è il seguente: *“Se alcuna delle falsità in atti previste dal codice penale riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici.”*

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali. Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (D. Lgs. 82/2005 e succ. modifiche ed integrazioni).

A titolo esemplificativo, integrano il delitto di falsità in documenti informatici la condotta di fraudolento inserimento di dati falsi nelle banche dati pubbliche, oppure la condotta dell'addetto alla gestione degli archivi informatici pubblici che proceda, deliberatamente, alla modifica di dati in modo da falsificarli.

Nei casi di condanna per il presente delitto si applica la sanzione pecuniaria sino a quattrocento quote e le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

### ***Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)***

Il reato di cui all'art. 615 ter c.p. è stato da ultimo novellato dalla L. n. 90/2024.

Tale reato si perfeziona quando un soggetto si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La sanzione prevista per tale ipotesi di reato è più grave se:

- il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
- il colpevole per commettere il fatto usa minaccia o violenza sulle cose o alle persone, ovvero se è palesemente armato;
- dal fatto deriva la distruzione o il danneggiamento ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Il delitto di accesso abusivo a sistema informatico rientra tra i delitti contro la libertà individuale. Il bene che viene protetto dalla norma è il domicilio informatico, pur se vi è chi sostiene che il bene tutelato sia, invece, l'integrità dei dati e dei programmi contenuti nel sistema informatico. L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema.

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema, oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

Il delitto potrebbe essere commesso da parte di qualunque dipendente accedendo abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), ad esempio, per prendere cognizione di dati riservati di un partner commerciale (ad esempio, appaltatore o subappaltatore) o un consulente. Ancora, il delitto di accesso abusivo a sistema informatico si considera integrato nel caso in cui un

soggetto accede abusivamente ad un sistema informatico e procede alla stampa di un documento contenuto nell'archivio del PC altrui, pur non effettuando alcuna sottrazione materiale di file (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).

***Detenzione e diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 - quater c.p.)***

Il reato di cui all'art. 615 quater c.p. è stato da ultimo novellato dalla L. n. 90/2024.

Tale ipotesi di reato si perfeziona quando un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica o consegna, mette in altro modo a disposizione di altri o installa, apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Il legislatore ha introdotto nell'ordinamento questa fattispecie di reato al fine di prevenire le ipotesi di accesso abusivo a sistemi informatici. Con l'art. 615- *quater* c.p. sono punite, pertanto, le condotte preliminari all'accesso abusivo, poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico. I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (es. badge, carte di credito, bancomat e smart card).

Questo delitto si perfeziona tanto nel caso in cui il soggetto che sia legittimamente in possesso dei dispositivi di cui sopra (ad esempio, un operatore di sistema) li comunichi senza autorizzazione a terzi, quanto nel caso in cui un soggetto faccia illecitamente uso di questi dispositivi.

La condotta è abusiva nel caso in cui i codici di accesso siano ottenuti a seguito della violazione di una norma anche contrattuale che vieti detta condotta (es. policy Internet).

L'art. 615- *quater*, inoltre, punisce chi rilascia delle istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Risponde, ad esempio, del delitto di diffusione abusiva di codici di accesso, il dipendente autorizzato ad un certo livello di accesso al sistema informatico che ottenga il livello di accesso superiore, procurandosi codici o altri strumenti di accesso mediante lo sfruttamento della propria posizione all'interno dell'Ente, oppure carpirca in altro modo fraudolento o ingannatorio il codice di accesso.

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

Il reato di cui all'art. 617 quater c.p. è stato da ultimo novellato dalla L. n. 90/2024.

Tale fattispecie di reato è integrata qualora taluno, fraudolentemente, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, nonché nel caso in cui qualcuno riveli, parzialmente o integralmente, il contenuto delle comunicazioni mediante qualsiasi mezzo di informazione al pubblico.

La sanzione prevista per tale ipotesi di reato è più grave se il fatto è commesso:

- 1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-ter, terzo comma;
- 2) in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema.

La norma tutela la libertà e la riservatezza delle comunicazioni informatiche o telematiche durante la fase di trasmissione al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi.

La frodolenza consiste nella modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione.

Perché possa realizzarsi questo delitto è necessario che la comunicazione sia attuale, vale a dire in corso, nonché personale, ossia diretta ad un numero di soggetti determinati o determinabili (siano essi persone fisiche o giuridiche). Nel caso in cui la comunicazione sia rivolta ad un numero indeterminato di soggetti, la stessa si considera, infatti, rivolta al pubblico.

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, o comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

Il reato si perfeziona, ad esempio, con il vantaggio concreto dell'ente, nel caso in cui un dipendente esegua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di un concorrente.

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

Il reato di cui all'art. 635 bis c.p. è stato da ultimo novellato dalla L. n. 90/2024.

Tale fattispecie di reato si perfeziona quando taluno distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui. La sanzione è più grave:

- 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
- 2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.

Costituisce danneggiamento di informazioni, dati e programmi informatici ai sensi dell'art. 635-bis c.p., ad esempio, la condotta di chi proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare di questi dati. Il fatto del danneggiamento potrebbe essere commesso in vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento da parte del fornitore.

### ***Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)***

Il reato di cui all'art. 635 ter c.p. è stato da ultimo novellato dalla L. n. 90/2024.

Tale ipotesi di reato si configura quando taluno commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico. Il reato è aggravato:

- 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
- 2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;
- 3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.

Questo delitto si distingue da quello contemplato dall'articolo 635 – *bis* c.p. poiché in questo caso il danneggiamento ha ad oggetto beni di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati alla soddisfazione di un interesse di natura pubblica.

Perché il reato si perfezioni è sufficiente che l'autore tenga una condotta finalizzata al deterioramento o alla soppressione dei dati.

### ***Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)***

Il reato di cui all'art. 635 quater c.p. è stato da ultimo novellato dalla L. n. 90/2024.

Questo reato si perfeziona quando taluno, mediante le condotte di cui all'art. 635-*bis* c.p. (danneggiamento di dati, informazioni e programmi informatici), ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento. La pena è aumentata:

- 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
- 2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.

Si tenga conto che, qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema, si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635 – *bis* c.p.

Costituisce ipotesi di danneggiamento di sistemi informatici o telematici, ad esempio, il danneggiamento o cancellazione di dati o programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio attraverso l'inserimento nel sistema di un virus).

### ***Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635 – quater 1 c.p.)***

Il reato di cui all'art. 635 quater 1 c.p. è stato introdotto dalla L. n. 90/2024.

Questo reato si perfeziona quando taluno, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici.

Il reato è aggravato quando ricorre taluna delle circostanze di cui all'art. 615 ter, secondo comma, n. 1) e quando il fatto riguarda sistemi informatici o telematici di cui all'art. 615 ter c.p.

### ***Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635 - quinquies c.p.)***

Il reato di cui all'art. 635 quinquies c.p. è stato da ultimo novellato dalla L. n. 90/2024. Questa fattispecie criminosa si configura quando, mediante le condotte di cui all'art. 635 bis c.p. ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, vengano compiuti atti diretti a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblico interesse o ad ostacolarne gravemente il funzionamento.

La sanzione è aggravata:

- 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
- 2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;
- 3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

La sanzione è sensibilmente aggravata quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3).

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblico interesse, diversamente dal delitto di danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 – ter c.p.), quel che rileva è che il sistema sia utilizzato per il perseguimento del pubblico interesse, indipendentemente dalla proprietà privata o pubblica del sistema. Ne consegue che il danneggiamento di un sistema informatico di proprietà di un ente pubblico, non utilizzato per il perseguimento di un pubblico interesse, non sarà sanzionabile ai sensi dell'art. 635 – quinquies c.p., ma, piuttosto, ai sensi dell'art. 634 – quater c.p., considerandosi il sistema informatico di proprietà pubblica alla stregua di qualsiasi altro sistema informatico.

Costituisce fattispecie di reato rilevante ai sensi del Decreto, ad esempio, la condotta del dipendente addetto al sistema informatico di un cliente (sistema che deve perseguire uno scopo di pubblica utilità) che, in sede di esecuzione di un contratto di appalto con la Pubblica Amministrazione o con persone incaricate di pubblico servizio, danneggi una parte del sistema medesimo al fine di occultare un inadempimento contrattuale della Ente dalla quale dipende.

### ***Estorsione mediante reati informatici (art. 629, comma 3, c.p.)***

La fattispecie in esame è stata introdotta da L. n. 90/2024.

Questo reato si configura quando taluno, mediante le condotte di cui agli articoli 615-ter, 617-*quater*, 617-*sexies*, 635-*bis*, 635-*quater* e 635-*quinqüies* ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

La pena è aumentata se concorre taluna delle circostanze indicate nel terzo comma dell'art. 628 c.p. nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o infermità.

Con questa novità il legislatore ha ritenuto opportuno prevedere un'autonoma fattispecie di reato per gli attacchi c.d. *ransomware* ovvero sia per quelle condotte volte a cifrare illecitamente i dati di terzi e a chiedere il pagamento di una somma per la decifrazione degli stessi.

### 3.2 Le aree di attività a rischio/sensibili di commissione dei fatti descritti

I reati informatici si riferiscono al trattamento dei dati sensibili e giudiziari nonché all'utilizzo della rete informatica aziendale intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi, composta da:

- ✓ infrastruttura e servizi di rete;
- ✓ acquisti di beni e servizi;
- ✓ assunzione e gestione del personale;
- ✓ Trattamento dei dati;
- ✓ Gestione del sistema informativo
- ✓ Gestione dei servizi giornalistici.

L'infrastruttura di rete è costituita dalle apparecchiature e dal relativo software che consentono i collegamenti all'interno della sede aziendale e la connessione da e verso l'esterno dell'azienda; i servizi di rete sono, invece, le utilities di carattere generale a disposizione dei Dipendenti, distribuite o messe a disposizione centralmente, quali servizi di posta elettronica, accesso a Internet, anagrafiche centralizzate, ecc. Applicazioni e servizi di rete aziendali sono resi disponibili agli utenti attraverso i server, mentre i punti di accesso alla rete aziendale sono le postazioni di lavoro fisse e mobili assegnate agli utenti stessi.

La realtà aziendale è caratterizzata dal diffuso utilizzo della rete aziendale, di sistemi informatici e dell'accesso ad Internet da parte dei Dipendenti e di tutti i collaboratori che, a vario titolo, consentono ai lanci delle informazioni in tempo reale sul web. Le aree a rischio di commissione dei reati ex art. 24 – *bis* del Decreto possono pertanto essere così individuate:

- (i) ordinarie attività giornalistiche svolte dal personale di COM.E tramite l'utilizzo della rete aziendale, del servizio di posta elettronica e dell'accesso ad Internet, necessario all'effettuazione dei lanci;
- (ii) attività di gestione della rete informatica aziendale al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT nonché la sicurezza informatica.

Inoltre, COM.E risulta essere esposto al rischio di commissione dei delitti informatici relativi con riferimento principalmente allo svolgimento delle attività relative:

- ✓ Gestione dei servizi giornalistici
- ✓ Accesso e gestione di sistemi informatici o telematici protetti da misure di sicurezza
- ✓ Utilizzo della rete aziendale, del servizio di posta elettronica e dell'accesso ad Internet
- ✓ Gestione della rete informatica aziendale
- ✓ Creazione, gestione e diffusione di documenti informatici e, segnatamente, delle cartelle cliniche
- ✓ Realizzazione della prestazione e compilazione documenti su piattaforme del SSN e SSR
- ✓ Gestione dei flussi finanziari e rimborsi spese

COM.E, pertanto, ispirandosi ai principi di necessità, correttezza e segretezza enunciati nel Regolamento UE 679/29016 e del Codice della Privacy, come modificato dal D. Lgs. n. 101/2018, adotta un adeguato **Sistema di sicurezza** basato su:

- ✓ regolamentazione dei comportamenti;
- ✓ formazione e addestramento (training on the job);
- ✓ controllo del personale.

Esso rappresenta un valido strumento per contrastare i rischi di:

- ✓ distruzione o perdita, anche accidentale, dei dati personali oggetto del trattamento;
- ✓ accesso non autorizzato, soprattutto laddove si tratti di operare direttamente sulle piattaforme informatiche di proprietà pubblica;
- ✓ trattamento non consentito o non conforme alle finalità della raccolta.

### 3.3 Principi di condotta nelle Aree a Rischio

A fini preventivi, sono stabiliti i seguenti divieti:

- ✓ alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- ✓ accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati ovvero accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;  
detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- ✓ detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- ✓ svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- ✓ svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate e installare apparecchiature idonee a tal fine;
- ✓ svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- ✓ svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

- ✓ eseguire di propria iniziativa modifiche o aggiornamenti di sistemi operativi o di programmi applicativi se non espressamente segnalati dalle Funzioni competenti;
- ✓ introdurre nella rete o sui server programmi non autorizzati (ad esempio “malicious code”);
- ✓ installare software e/o programmi non autorizzati dall’ente, nonché in violazione degli accordi contrattuali di licenza d’uso e/o di leggi e regolamenti che disciplinano il diritto d’autore;
- ✓ utilizzare gli strumenti informatici per lo svolgimento di attività illecite, per visionare, memorizzare, stampare, copiare, riprodurre, ricevere e diffondere materiale illegale, di proprietà altrui, osceno o simile;
- ✓ detenere o diffondere indebitamente il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- ✓ procurarsi illegalmente, conservare, riprodurre, diffondere, distribuire e/o utilizzare nelle attività sociali (es.: preparazione di materiale per convention, eventi istituzionali; ecc.) materiale ottenuto in violazione delle norme in materia di protezione del diritto d’autore;
- ✓ ostacolare o omettere, anche con artifici e raggiri, l’adempimento degli obblighi derivanti dalla normativa in materia di protezione del diritto d’autore.

In considerazione di ciò, i Destinatari del Modello devono:

- ✓ utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
- ✓ non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza autorizzazione scritta;
- ✓ in caso di smarrimento o furto avvisare immediatamente il Presidente, l’Amministratore di Sistema dell’IdO e presentare denuncia all’Autorità Giudiziaria preposta;
- ✓ evitare di introdurre e/o conservare sul luogo di lavoro (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi;
- ✓ evitare di trasferire all’esterno del luogo di lavoro e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà aziendale, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione di uno degli amministratori;
- ✓ evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l’utilizzo dello stesso ad altre persone;
- ✓ evitare l’utilizzo di passwords di altri utenti aziendali, neanche per l’accesso ad aree protette in nome e per conto dello stesso;
- ✓ evitare l’utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- ✓ utilizzare la connessione a internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;  
segnalare immediatamente ad uno degli amministratori utilizzi e/o funzionamenti anomali delle risorse informatiche;
- ✓ impiegare sulle apparecchiature di lavoro solo prodotti ufficialmente acquisiti dall’azienda stessa;
- ✓ astenersi dall’effettuare copie non specificamente autorizzate di dati e di software;
- ✓ astenersi dall’utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- ✓ interpellare il Responsabile del Sistema Informativo in caso di dimenticanza delle procedure di autenticazione di accesso al proprio terminale;
- ✓ non forzare l’accesso a cartelle e/o files dedicate/i (il cui utilizzo è consentito, quindi, solo a predeterminate postazioni);
- ✓ interpellare il Responsabile del Sistema Informativo per procedere alla forzatura delle cartelle dedicate: questi potrà procedere alla forzatura, e quindi allo sblocco, a favore di altri utenti solo se autorizzato, per iscritto, dal Rappresentante Legale.

I **Protocolli specifici** per la prevenzione dei reati di cui sopra sono riportati nelle Procedure allegate al presente Modello.

#### **4. REATI ASSOCIATIVI**

##### **4.1 Descrizione delle fattispecie di reato**

Si descrivono qui di seguito le singole fattispecie di reato per le quali l'art. 24-ter del D.Lgs. n. 231/2001 prevede una responsabilità degli enti nei casi in cui tali reati siano stati compiuti nell'interesse o a vantaggio degli stessi, applicando la sanzione pecuniaria da trecento ad ottocento quote e sanzioni interdittive (inclusa altresì la sanzione dell'interdizione definitiva dall'esercizio dell'attività laddove l'ente sia stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati qui considerati).

La descrizione che segue è limitata alle fattispecie di reato astrattamente ipotizzabili tenuto conto della realtà operativa di COM.E.

##### ***Associazione per delinquere (art. 416 c.p.)***

Si configura la fattispecie dell'associazione per delinquere quando tre o più persone si associano allo scopo di commettere più delitti.

Ai sensi dell'articolo 416 c.p., coloro che promuovono o costituiscono od organizzano l'associazione sono puniti, per ciò solo, con la reclusione da tre a sette anni. Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni. I capi soggiacciono alla stessa pena stabilita per i promotori. Se gli associati scendono in armi le campagne o le pubbliche vie, si applica la reclusione da cinque a quindici anni. La pena è aumentata se il numero degli associati è di dieci o più.

Se l'associazione è diretta a commettere taluno dei delitti di cui agli articoli 600 (Riduzione o mantenimento in schiavitù o in servitù), 601 (Tratta di persone) e 602 (Acquisto e alienazione di schiavi) c.p., nonché all'articolo 12, comma 3-bis, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286 (Disposizioni contro le immigrazioni clandestine), si applica la reclusione da cinque a quindici anni nei casi previsti dal primo comma e da quattro a nove anni nei casi previsti dal secondo comma.

##### ***Scambio elettorale politico-mafioso (art. 416-ter c.p.)***

Costituisce reato rilevante ai fini della responsabilità amministrativa da reato degli enti lo scambio elettorale politico – mafioso, che si configura quando qualcuno accetta la promessa di procurare voti

mediante la modalità mafiose di cui all'articolo 416-bis in cambio dell'erogazione o della promessa di erogazione di denaro o di altre utilità.

È ugualmente punito chi promette di procurare voti con le suddette modalità mafiose.

#### **4.2. Aree a Rischio/Sensibili**

I delitti descritti nel precedente capitolo assumono rilevanza ai fini della configurazione della responsabilità amministrativa da reato degli enti ex Decreto allorquando sono posti in essere, sia in territorio italiano che all'estero, (anche) da soggetti facenti parte dell'ente – in qualità di soggetti apicali e / o sottoposti – (anche) nell'interesse dell'ente, eventualmente utilizzando l'ente stesso quale strumento per la commissione dei delitti medesimi.

In generale, i delitti associativi qui considerati possono interessare qualsiasi tipo di ente, indipendentemente dall'attività svolta (ad esempio, frodi fiscali, traffico illecito di rifiuti, ed ogni altro reato tipicamente legato all'attività di impresa commesso mediante l'avvalimento del vincolo associativo criminoso).

In considerazione della realtà propria di COM.E, quest'ultima appare in astratto esposta, per la natura della sua attività ed in relazione allo svolgimento della medesima, al rischio di commissione di reati di tipo associativo (art. 416 e 416-ter c.p.) che potrebbero essere astrattamente posti in essere da uno o più soggetti appartenenti alla Società, (anche) al fine di procurare un vantaggio alla stessa o comunque nell'interesse di quest'ultima, in relazione alle seguenti aree di attività dell'Ente:

1. Gestione dei servizi giornalistici;
2. Gestione dei rapporti con le autorità pubbliche per il rilascio di autorizzazioni, accreditamenti, concessioni, nulla-osta, etc.;
3. Gestione del personale;
4. Gestione e monitoraggio dei fornitori;
5. Gestione acquisti e contrattualistica;
6. Formazione del personale;
7. Selezione del personale, costituzione del rapporto di lavoro e gestione del personale;
8. Gestione pagamenti.

#### **4.3. Principi di condotta nelle Aree a Rischio**

Nell'espletamento delle attività aziendali è espressamente vietato ai membri degli Organi di vertice, ai Dipendenti e ai Collaboratori dell'Ente di porre in essere comportamenti, anche omissivi, tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente Parte Speciale (art. 24-ter Decreto).

È fatto altresì obbligo ai membri degli Organi di vertice, ai Dipendenti e ai Collaboratori, nei limiti delle proprie competenze ed attività, di COM.E di:

- ✓ osservare scrupolosamente le disposizioni del Codice Etico di COM.E;
- ✓ astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle considerate dall'articolo 24 - ter, possano potenzialmente diventarlo;
- ✓ non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità;
- ✓ tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e delle procedure aziendali interne;
- ✓ non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
- ✓ non effettuare elargizioni in denaro a individui, Ente od organizzazioni anche solo sospettate di svolgere attività criminali organizzate;
- ✓ selezionare il personale, di qualunque livello, i Collaboratori e i Consulenti sulla base dei criteri di (i) professionalità specifica rispetto all'incarico o alle mansioni, (ii) quanto ai dipendenti, uguaglianza di trattamento, (iii) affidabilità rispetto al rischio di infiltrazione criminale;
- ✓ effettuare la scelta dei Partner, anche stranieri, con cui la Ente intende instaurare rapporti commerciali e/o finanziari, solo dopo aver compiuto le necessarie verifiche relative al possesso, da parte dei Partner, dei requisiti di onorabilità, professionalità ed affidabilità;
- ✓ non sottostare a richieste estorsive di qualsiasi tipo (pizzo, messa a posto, offerte, ecc.), da chiunque formulate e denunciare senza indugio le dette eventuali richieste all'autorità di polizia;
- ✓ in caso di attentati ai beni aziendali o di minacce, informare immediatamente le autorità di polizia, fornendo senza reticenze tutte le informazioni e le notizie possedute, non solo in relazione agli eventi lesivi specifici, ma anche in ordine ad eventuali antefatti e circostanze rilevanti ai fini delle indagini.

I **Protocolli specifici** per la prevenzione del reato di cui sopra è riportata nelle Procedure allegate al presente Modello.

## **5. RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI, O ALTRA UTILITÀ DI PROVENIENZA ILLECITA E AUTORICICLAGGIO**

La presente sezione della Parte Speciale descrive le fattispecie di reato, rilevanti ai fini di una eventuale responsabilità amministrativa da reato di COM.E, elencate dall'art. 25-*octies* del Decreto, introdotto nel corpus dello stesso dal D. Lgs. 231/ 2007 (di seguito il "Decreto Antiriciclaggio").

## 5.1 Descrizione delle fattispecie di reato

Le fattispecie di reato contemplate dall'art. 25 - *octies* del Decreto possono essere così brevemente descritte:

### *Ricettazione (art. 648 c.p.)*

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

La condotta è punita anche quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno e nel minimo a sei mesi.

### *Riciclaggio (art. 648-bis c. p.)*

Commette il reato di riciclaggio chi sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

La pena è inferiore quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno e nel minimo a sei mesi.

### *Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)*

La fattispecie di reato in esame presuppone, per il suo perfezionamento, che l'autore impieghi in attività economiche o finanziarie denaro, beni o altre utilità di provenienza delittuosa, anche quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno e nel minimo a sei mesi. Si precisa che le ipotesi criminose suindicate si considerano perfezionate anche se le attività che hanno generato i beni da riciclare si sono svolte nel territorio di un altro Stato comunitario o di un Paese terzo.

### *Autoriciclaggio (art. 648-ter.1 c.p.)*

La fattispecie di reato si realizza quando il soggetto agente, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Ai fini della consumazione del reato, pertanto, non rileva il mero godimento del denaro, dei beni o delle altre utilità provenienti da attività delittuose, ma è necessaria un'ulteriore condotta specificamente finalizzata ad occultarne la provenienza.

Anche in questa ipotesi, il fatto rileva anche quando riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi.

La legislazione italiana in tema di prevenzione delle ipotesi di reato contemplate nella presente sezione della Parte Speciale ha introdotto norme tese ad ostacolare le pratiche di riciclaggio, vietando, tra l'altro, l'effettuazione di operazioni di trasferimento di importi rilevanti con strumenti anonimi ed assicurando la ricostruzione delle operazioni attraverso l'identificazione della clientela e la registrazione dei dati in appositi archivi.

Nello specifico, il corpo normativo in materia di riciclaggio è costituito anzitutto dal Decreto Antiriciclaggio, che ha in parte abrogato e sostituito la legge 5 luglio 1991 n. 197. Il Decreto Antiriciclaggio prevede, in sostanza, i seguenti strumenti di contrasto del fenomeno del riciclaggio di proventi illeciti:

1. la previsione di un divieto di trasferimento di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) in Euro o in valuta estera, effettuato a qualsiasi titolo tra soggetti diversi quando il valore dell'operazione è pari o superiore a Euro 3.000,00. Il trasferimento può tuttavia essere eseguito per il tramite di banche, istituti di moneta elettronica e Poste Italiane S.p.A.;
2. l'obbligo di adeguata verifica della clientela da parte di alcuni soggetti (elencati agli artt. 11, 12, 13 e 14 del Decreto Antiriciclaggio) in relazione ai rapporti e alle operazioni inerenti allo svolgimento dell'attività istituzionale o professionale degli stessi;
3. l'obbligo da parte di alcuni soggetti (elencati negli artt. 11, 12, 13 e 14 del Decreto Antiriciclaggio) di conservare, nei limiti previsti dall'art. 36 del Decreto Antiriciclaggio, i documenti o le copie e registrare le informazioni acquisite per assolvere gli obblighi di adeguata verifica della clientela affinché possano essere utilizzati per qualsiasi indagine su eventuali operazioni di riciclaggio o di finanziamento del terrorismo o per corrispondenti analisi effettuate dall'UIF o da qualsiasi altra autorità competente;
4. l'obbligo di segnalazione da parte di alcuni soggetti (elencati negli artt. 10, comma 2, 11, 12, 13 e 14 del Decreto Antiriciclaggio) all'UIF, di tutte quelle operazioni, poste in essere dalla clientela, ritenute "sospette" ovvero obbligo di segnalazione all'UIF quando i medesimi soggetti sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento al terrorismo.

Benché COM.E non figuri tra i destinatari del Decreto Antiriciclaggio (intermediari finanziari e altri soggetti esercenti attività finanziaria, avvocati, notai, revisori contabili, soggetti incaricati del recupero di crediti per conto terzi, soggetti incaricati del trasporto di denaro contante, gestori di case da gioco, soggetti che effettuano offerte, attraverso internet, di giochi, scommesse o concorsi pronostici con vincite in denaro), si è ritenuto opportuno citare tale normativa in quanto dalla stessa è possibile ricavare indirettamente alcune regole di comportamento funzionali a limitare il rischio di verifica dei reati in esame all'interno di COM.E.

## **5.2 Aree a Rischio/Sensibili**

Premesso che COM.E pone in essere normali attività di servizi in relazione alla propria attività, ricevendo ed effettuando pagamenti tramite bonifici bancari, e considerato che la medesima ha adottato procedure per la gestione delle risorse finanziarie e che ricorre normalmente a Partner e Consulenti abituali e di comprovata affidabilità, le Aree a Rischio appaiono essere le seguenti:

1. Selezione e assunzione del personale
2. Gestione del Personale
3. Selezione, contrattualizzazione e monitoraggio del Fornitore
4. Adempimenti civilistici, previdenziali e fiscali
5. Budgeting e controllo di gestione
6. Gestione incassi e pagamenti
7. Gestione cassa
8. Comunicazione, incontri e richieste di autorizzazioni P.A.

### 5.3 Principi di condotta nelle Aree a Rischio

La presente sezione della Parte Speciale prevede l'espresso obbligo a carico dei Dipendenti, dei membri degli Organi Sociali e dei Collaboratori di COM.E di osservare i seguenti principi di condotta:

- ✓ non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza o la vicinanza a organizzazioni criminali o comunque illecite;
- ✓ non realizzare operazioni finanziarie e/o commerciali con controparti che utilizzano strutture sociali opache e/o che impediscono l'identificazione univoca dell'assetto dell'Ente e/o dei reali beneficiari dell'operazione;
- ✓ tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione dell'anagrafica fornitori/clienti;
- ✓ rispettare la disciplina generale in tema di mezzi di pagamento prevista dal D.Lgs. 231/2007 (i.e. normativa assegni, divieto di possedere titoli al portatore oltre determinate soglie e/o il divieto di trasferimento per denaro contante oltre i limiti di legge in vigore);
- ✓ non accettare pagamenti e non effettuare fatturazioni nei confronti di soggetti diversi da quelli che assumono ruolo di controparti contrattuale e in assenza di adeguata giustificazione;
- ✓ sospendere/interrompere un rapporto con il fornitore laddove si evidenziassero comportamenti non in linea con la normativa, le leggi e i principi di controllo statuiti nel presente documento. Le segnalazioni, nonché le eventuali interruzioni dei rapporti devono essere effettuate con la massima tempestività;
- ✓ garantire la corretta gestione della politica fiscale, anche con riguardo alle eventuali transazioni con i Paesi di cui alla c.d. "black list" definite nelle disposizioni normative vigenti e con quelli a regime fiscale privilegiato indicati al D.M. 23 gennaio 2002 e loro successive modifiche ed integrazioni;
- ✓ individuare ed attuare specifici programmi di controllo interno con particolare riguardo alla gestione dei pagamenti e della tesoreria, agli accordi/joint venture con altre imprese, ai rapporti infragruppo, nonché ai rapporti con controparti aventi sede sociale e/o operativa in Paesi a fiscalità privilegiata;
- ✓ attuare la formazione ed informazione degli esponenti aziendali sui temi relativi alla prevenzione dei fenomeni di riciclaggio;
- ✓ dare evidenza delle attività e dei controlli svolti.

Tenuto conto, infine, dell'attività svolta da COM.E e della platea dei soggetti destinatari delle prestazioni, si ritiene che lo svolgimento delle attività ad esse inerenti non destino particolari rischi nell'ambito di tali reati.

I **Protocolli specifici** per la prevenzione dei reati di cui sopra sono riportati nelle Procedure allegate al presente Modello.

## **6. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE**

### **6.1 Descrizione della fattispecie di reato**

La presente Sezione si riferisce ai delitti di:

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

Introdotta dal Decreto Legislativo 16 luglio 2012, n. 109, entrato in vigore il 9 agosto 2012, regola l'attuazione della Direttiva 2009/52/CE, attraverso il quale è stato aggiunto nel corpus del Decreto l'art. 25-duodecies. Tale reato si configura qualora il soggetto che riveste la qualifica di "datore di lavoro" occupi alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, o sia stato revocato o annullato, laddove i lavoratori occupati siano:

- a) in numero superiore a tre;
- b) minori in età non lavorativa;
- c) sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-bis, c.p.

In particolare, le condizioni lavorative di cui al punto c) che precede riguardano l'esposizione dei lavoratori a situazioni di grave pericolo con riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

La sanzione prevista per l'ente è una sanzione pecuniaria entro il valore massimo di Euro 150.000.

#### ***Procurato ingresso illecito di stranieri e favoreggiamento dell'immigrazione clandestina (art. 12, commi 3, 3 bis e 3 ter, D.Lgs. 286/98)***

Salvo che il fatto costituisca più grave reato, chiunque, in violazione delle disposizioni del presente testo unico, promuove, dirige, organizza, finanzia o effettua il trasporto di stranieri nel territorio dello Stato ovvero compie altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente, è punito con la reclusione da sei a sedici anni e con la multa di 15.000 euro per ogni persona nel caso in cui: a) il fatto riguarda l'ingresso o la permanenza illegale nel territorio dello Stato di cinque o più persone; b) la persona trasportata è stata esposta a pericolo per la sua vita o per la sua incolumità per procurarne l'ingresso o la permanenza illegale;

c) la persona trasportata e' stata sottoposta a trattamento inumano o degradante per procurarne l'ingresso o la permanenza illegale; d) il fatto e' commesso da tre o piu' persone in concorso tra loro o utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti; e) gli autori del fatto hanno la disponibilita' di armi o materie esplodenti. Se i fatti di cui al comma 3 sono commessi ricorrendo due o piu' delle ipotesi di cui alle lettere a), b), c), d) ed e) del medesimo comma, la pena ivi prevista e' aumentata.

La pena detentiva e' aumentata da un terzo alla meta' e si applica la multa di 25.000 euro per ogni persona se i fatti di cui ai commi 1 e 3: a) sono commessi al fine di reclutare persone da destinare alla prostituzione o comunque allo sfruttamento sessuale o lavorativo ovvero riguardano l'ingresso di minori da impiegare in attivita' illecite al fine di favorirne lo sfruttamento; b) sono commessi al fine di trarre profitto, anche indiretto.

***Favoreggiamento della permanenza illecita di stranieri nel territorio dello Stato (art. 12, comma 5, D.Lgs. 286/98)***

Fuori dei casi previsti dai commi precedenti, e salvo che il fatto non costituisca piu' grave reato, chiunque, al fine di trarre un ingiusto profitto dalla condizione di illegalita' dello straniero o nell'ambito delle attivita' punite a norma del presente articolo, favorisce la permanenza di questi nel territorio dello Stato in violazione delle norme del presente testo unico, e' punito con la reclusione fino a quattro anni e con la multa fino a lire trenta milioni. Quando il fatto e' commesso in concorso da due o piu' persone, ovvero riguarda la permanenza di cinque o piu' persone, la pena e' aumentata da un terzo alla meta'.

***Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12 bis, D. Lgs. n. 286/1998)***

12. Il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è punito con la reclusione da sei mesi a tre anni e con la multa di 5000 euro per ogni lavoratore impiegato.

12-bis. Le pene per il fatto previsto dal comma 12 sono aumentate da un terzo alla metà:

- a) se i lavoratori occupati sono in numero superiore a tre;
- b) se i lavoratori occupati sono minori in età non lavorativa;
- c) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di cui al terzo comma dell'articolo 603-bis del codice penale.

articolo è stato modificato dalla L. n. 187/2024.

## 6.2 Aree a Rischio/Sensibili

Le Aree a Rischio che COM.E ha individuato in relazione al reato considerate nella presente Parte Speciale sono le seguenti:

1. Selezione e assunzione del personale
2. Gestione del Personale
3. Formazione
4. Comunicazione, incontri e richieste di autorizzazioni P.A.

## 6.3 Principi di condotta nelle Aree a Rischio

I principi contenuti nella presente sezione sono rivolti a chi riveste la qualifica di “Datore di lavoro” e alle Funzioni coinvolte nella gestione, anche come supporto, delle attività di competenza dello stesso.

Al fine di prevenire il più possibile il reato considerato, dovranno essere rispettati i seguenti principi comportamentali:

- ✓ è vietato porre in essere o partecipare alla realizzazione di condotte tali che, considerate individualmente o collettivamente, possano integrare il Delitto di impiego di cittadini di paesi terzi con soggiorno irregolare;
- ✓ è vietato porre in essere e adottare comportamenti che, sebbene non integrino, di per sé, tale fattispecie di reato, possano potenzialmente diventare idonei alla realizzazione del medesimo;
- ✓ è necessario rispettare gli obblighi di legge in tema di impiego di lavoratori stranieri e permesso di soggiorno;
- ✓ è necessario assicurare la verifica della regolarità del permesso di soggiorno in caso di assunzione di lavoratori stranieri ed un monitoraggio periodico finalizzato a verificare la validità/scadenza dei permessi di soggiorno stessi;
- ✓ in caso di lavori affidati a soggetti terzi mediante subappalti, viene sottoposta ad ogni fornitore una dichiarazione preventiva con cui lo stesso si impegna a non utilizzare, per l'espletamento delle attività oggetto del contratto, cittadini di paesi terzi con soggiorno irregolare, nonché a rispettare tutte le normative applicabili in tema di lavoro minorile e delle donne, condizioni igienico sanitarie, sicurezza e impiego di personale proveniente da paesi terzi;
- ✓ i contratti con le controparti contengono specifiche clausole che liberano COM.E da qualsiasi responsabilità nel caso in cui la controparte commetta reati ex 231 e quindi (per quanto qui rileva) utilizzi, per lo svolgimento delle prestazioni oggetto del contratto, cittadini di paesi terzi senza regolare permesso di soggiorno;
- ✓ la Società non può impiegare lavoratori stranieri del tutto privi di permesso di soggiorno o con un permesso revocato o scaduto, del quale non sia stata presentata domanda di rinnovo, documentata dalla relativa ricevuta postale;
- ✓ è vietato l'impiego di uno straniero in Italia per motivi di turismo, anche se regolarmente munito della prescritta dichiarazione di presenza;
- ✓ è vietato favorire la permanenza dello straniero nel territorio dello Stato al fine di trarre un ingiusto profitto dalla condizione di illegalità in cui lo stesso versa.

I **Protocolli specifici** per la prevenzione dei reati di cui sopra sono riportati nelle Procedure allegate al presente Modello.

## **7. INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA**

### **7.1 Descrizione della fattispecie di reato**

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

La fattispecie di reato in esame richiede, per il suo perfezionamento, che un soggetto, facendo ricorso ai mezzi della minaccia, della violenza o dell'offerta o promessa di denaro o di altra utilità induca a non rendere dichiarazioni, ovvero a renderle mendaci, tutti coloro che sono chiamati a rendere, davanti all'Autorità Giudiziaria, dichiarazioni utilizzabili in un procedimento penale pur avendo facoltà di non rispondere.

Le condotte individuate dalla norma in esame devono realizzarsi attraverso mezzi tassativamente delineati dalla norma incriminatrice e dunque consistere in una violenza, una minaccia ovvero in un'offerta o promessa di denaro o di altra utilità.

Appare opportuno sottolineare che tale fattispecie di reato ha rilevanza ai fini della responsabilità amministrativa da reato degli enti, così come prevista dal Decreto, nei limiti in cui le condotte criminose che la caratterizzano siano poste in essere dai soggetti apicali o sottoposti della Ente nell'interesse (anche) della Ente medesima (es. induzione di un imputato in un procedimento / testimone-imputato in un procedimento connesso a non rendere dichiarazioni che possano comportare la rivelazione di fatti aventi rilevanza penale nei quali sia coinvolto un ente).

### **7.2 Le Aree a Rischio/Sensibili**

Il reato *de quo* appare astrattamente configurabile ogniqualvolta un qualunque soggetto operante nella Società, sia esso un soggetto apicale, ovvero un soggetto sottoposto, ponga in essere una delle condotte tipizzate dall'articolo 377 – bis c.p. con lo specifico fine di indurre un imputato / testimone-imputato in un procedimento connesso a non rendere dichiarazioni/a rendere dichiarazioni mendaci al fine di procurare un vantaggio (anche) alla Società.

Le possibili aree a rischio sono:

1. Gestione di contenziosi;
2. Monitoraggio dell'attività svolta dai consulenti legali;
3. Gestione dei sistemi informativi;
4. Gestione delle attività giornalistiche.

### **7.3 Principi di condotta nelle Aree a Rischio**

Nell'espletamento della propria attività, i Dipendenti, i membri degli Organi Sociali, ed i Collaboratori di COM.E devono rispettare i seguenti principi generali di comportamento.

A tutti i soggetti indicati è fatto divieto di:

- ✓ porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare fattispecie di reato richiamate nella presente sezione della Parte Speciale;
- ✓ porre in essere, collaborare o dare causa alla realizzazione di comportamenti i quali, sebbene risultino tali da non costituire di per sé reato, possano potenzialmente diventarlo.

È inoltre necessario:

- ✓ che sia garantito il pieno rispetto del Codice Etico di COM.E;
- ✓ che tutte le attività e le operazioni svolte per conto di COM.E siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza.

I **Protocolli specifici** per la prevenzione dei reati di cui sopra sono riportati nelle Procedure allegate al presente Modello.

## **8. REATI CONTRO LA PERSONALITA' INDIVIDUALE**

### **8.1 Descrizione della fattispecie di reato**

Si descrive qui di seguito la fattispecie di reato per il quale l'art. 25-*quinquies* del D.Lgs. n. 231/2001 prevede una responsabilità degli enti nei casi in cui tali reati siano stati compiuti nell'interesse o a vantaggio degli stessi, applicando la sanzione pecuniaria da cinquecento a mille euro per ciascun lavoratore reclutato e la pena di reclusione da uno a sei anni.

La descrizione che segue è limitata alle fattispecie di reato astrattamente ipotizzabili tenuto conto della realtà operativa di COM.E.

#### ***Intermediazione illecita e sfruttamento del lavoro (art 603bis c.p.)***

Si riferisce allo sfruttamento della forza lavoro relativamente a retribuzioni fortemente al di sotto dei limiti contrattuali, sproporzionate rispetto alla mole o al tipo di lavoro, reiterati comportamenti non congruenti con la normativa riguardante gli orari di lavoro, riposo e ferie, reiterate violazioni delle norme sulla sicurezza ed igiene sul lavoro, imposizione di condizioni di sorveglianza e/o situazioni alloggiative degradanti.

In particolare, il nuovo art. 603-bis del codice penale, come modificato dalla Legge 199 del 2016, prevede che: *“Salvo che il fatto costituisca più grave reato, è punito con la reclusione da uno a sei anni e con la multa da 500 a 1.000 euro per ciascun lavoratore reclutato, chiunque: 1) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori 2) utilizza, assume o impiega manodopera, anche mediante l'attività di*

*intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno. Se i fatti sono commessi mediante violenza o minaccia, si applica la pena della reclusione da cinque a otto anni e la multa da 1.000 a 2.000 euro per ciascun lavoratore reclutato. Ai fini del presente articolo, costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni: 1) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato; 2) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie; 3) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro; 4) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti. Costituiscono aggravante specifica e comportano l'aumento della pena da un terzo alla metà: 1) il fatto che il numero di lavoratori reclutati sia superiore a tre; 2) il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa; 3) l'aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro”.*

Il Legislatore ha quindi inteso rafforzare il contrasto al cosiddetto “caporalato”.

Il reato in esame, oggi, risulta slegato dal requisito dello svolgimento di “un’attività organizzata di intermediazione”, andando a colpire non solo chi “recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento...”, ma altresì chiunque “utilizza, assume o impiega manodopera, anche mediante l’attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno”.

A ciò deve aggiungersi che integra il reato *de quo*, rispetto alla fattispecie previgente, anche la condotta non caratterizzata da violenza, minaccia o intimidazione, posto che la violenza e la minaccia sono divenute circostanze aggravanti e non più elementi costitutivi del reato.

Anche gli “indici di sfruttamento” enunciati dall’art. 603-bis c.p. assumono una connotazione più ampia, essendo oggi alcuni di essi parametrati, ad esempio, non più a condotte sistematiche di sotto-retribuzione e violazione delle norme su orari, riposi, aspettativa e ferie, bensì a siffatte condotte anche solo “reiterate”.

Di particolare rilievo è anche l’indice di sfruttamento relativo alla “sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro” che oggi, a differenza di prima, rileva anche laddove non sia tale da esporre il lavoratore a pericolo per la salute, la sicurezza o l’incolumità personale.

Il “grave pericolo” infatti rileva ora solo quale circostanza aggravante ai sensi del comma 4 punto 3).

Inoltre, è da evidenziare che nel contesto di tale indice non rileva neppure la reiterazione della condotta.

L’intervento legislativo mira al contrasto del reato in esame anche attraverso altri strumenti, quali:

- l’introduzione, con l’art. 603-bis.1 c.p., di un’attenuante in caso di comportamenti collaborativi;
- una nuova ipotesi di confisca obbligatoria, con l’introduzione dell’art. 603-bis.2 c.p.;
- la previsione di un “controllo giudiziario dell’azienda”, con nomina di un “amministratore giudiziario” destinato ad affiancare l’imprenditore;
- la previsione dell’arresto obbligatorio in flagranza, con modifica dell’art. 380, co. 2 c.p.p.;

– l'estensione al reato in esame della particolare confisca di cui all'art. 12-sexies D.L. 306/1992.

## **8.2 Aree a Rischio/Sensibili**

Le Aree a Rischio che COM.E ha individuato in relazione al reato considerate nella presente Parte Speciale sono le seguenti:

1. Selezione e assunzione del personale;
2. Gestione del Personale;
3. Gestione dei sistemi informativi;
4. Selezione, contrattualizzazione e monitoraggio del Fornitore;
5. Gestione della sicurezza e qualità.

## **8.3 Principi specifici di condotta nelle Aree a Rischio**

Al fine di prevenire il reato considerato nella presente Sezione, dovranno essere rispettati i seguenti principi comportamentali:

- ✓ Rispetto del contratto di lavoro e delle correlate prescrizioni in tema di orari e sicurezza
- ✓ Rispetto della normativa inerente all'igiene sia negli ambulatori sia presso gli uffici di IdO, ove la Società ha sede ed opera
- ✓ Rispetto degli standard di cui al Manuale della Qualità;
- ✓ Esercizio di azioni preventive volte a tutelare la salute e la sicurezza dei lavoratori
- ✓ Ottimizzazione delle attività mirata ad una corretta gestione della protezione dell'Ambiente e della Salute e Sicurezza del personale.

**I Protocolli specifici** per la prevenzione dei reati di cui sopra sono riportati nelle Procedure allegate al presente Modello.

## **9. REATI DI RAZZISMO E XENOFOBIA**

### **9.1 Descrizione della fattispecie di reato**

I reati di razzismo e xenofobia sono stati introdotti dall'art.3 comma 3 bis della legge 654/1975. Ad oggi però il richiamo contenuto nell'articolo. 25 terdecis del D. Lgs 231/2001 deve intendersi riferito all'art. 604 bis c.p. stanti le modifiche introdotte dall'art. 7 del D. Lgs 21/2018.

La presente sezione di Parte Speciale si riferisce ai reati di razzismo e xenofobia richiamati dalle disposizioni di cui all'art. 25-terdecies del D. Lgs. 231/2001. Per effetto dell'entrata in vigore della Legge Europea n. 167 del 20 novembre 2017 e le successive modifiche introdotte dal D. Lgs. n. 21/2018, il novero dei reati che possono generare una responsabilità amministrativa per gli enti si è arricchito con la fattispecie richiamata dall'articolo 604 bis c.p., il quale punisce:

- a) chi propaganda idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi;
- b) chi, in qualsiasi modo, istiga a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi.

La citata disposizione vieta, altresì, la costituzione e/o l'appartenenza ad ogni organizzazione, associazione, movimento o gruppo avente tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi e punisce chi partecipa a tali organizzazioni, associazioni, movimenti o gruppi, o presta assistenza alla loro attività, per il solo fatto della partecipazione o dell'assistenza, unitamente – con pene più gravi- coloro che promuovono o dirigono tali organizzazioni, associazioni, movimenti o gruppi.

Le pene sono, inoltre, aumentate se la propaganda ovvero l'istigazione e l'incitamento siano commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale

## **9.2 Le Aree a Rischio/Sensibili**

La probabilità di accadimento dei suddetti reati in COM.E è remota, tuttavia le forme di discriminazione religiosa e razziale sono vietate e condannate sia dalle regole contenute nel Codice Etico della società sia dai principi e dalle linee guida del presente Modello. Inoltre, allo stato attuale, appare alquanto improbabile che il personale di COM.E compia attività di propaganda ovvero di istigazione o di incitamento a crimini di genocidio o contro l'umanità, allo scopo di generare un vantaggio a favore della società. In un'ottica prudenziale, non potendo escludere a priori condotte illecite che possano integrare le suddette fattispecie dei reati, si è proceduto alla valutazione del rischio con i principali Process Owner. Dall'analisi svolta si ritiene che, in relazione al reato sopra esplicitato, le aree che presentano un'esposizione al rischio, seppur remoto, risultano essere:

1. Comunicazioni interne ed esterne
2. Controllo di gestione

3. Attività di tesoreria
4. Gestione dei servizi giornalistici
5. Gestione dei pagamenti.

Nell'espletamento di tutte le attività esposte a rischio di reato della presente sezione, oltre al rispetto di quanto indicato nel paragrafo successivo, la Società ha previsto l'attivazione di corsi di formazione e la diffusione di una propaganda di sensibilizzazione a tutti i livelli organizzativi.

### 9.3 Principi specifici di condotta nelle Aree a Rischio

Al fine di prevenire il reato considerato nella presente Sezione, dovranno essere rispettati i seguenti principi comportamentali:

- ✓ ai collaboratori esterni deve essere resa nota l'adozione del Modello e del Codice Etico, da parte di COM.E: il rispetto dei principi contenuti in tali documenti costituisce obbligo contrattuale a carico di tali soggetti. La presente parte speciale prevede, nell'espletamento delle attività considerate a rischio, l'espresso divieto per gli esponenti aziendali ed i collaboratori esterni di:
  - porre in essere, promuovere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nell'articolo 25-terdecies del Decreto – Reati di razzismo e xenofobia;
  - utilizzare anche occasionalmente COM.E, o una sua unità organizzativa, allo scopo di consentire o agevolare la commissione dei reati di cui sopra;
  - nel corso dell'attività aziendale promuovere, costituire, organizzare o dirigere associazioni che si propongono il compimento di atti di razzismo e xenofobia;
  - fornire, direttamente o indirettamente, tramite sponsorizzazioni o donazioni le risorse monetarie a favore di soggetti che intendano porre in essere reati di razzismo e xenofobia;
  - operare in contrasto con le regole etiche e le procedure aziendali che disciplinano le attività di pubblicità e di sponsorizzazione;
  - assumere o assegnare commesse o effettuare qualsivoglia operazione commerciale e/o finanziaria, sia in via diretta, che per il tramite di interposta persona, che abbia come scopo quello di concorrere al compimento di atti di razzismo e xenofobia;
  - affittare o concedere in comodato d'uso gratuito locali e spazi aziendali ad organizzazioni e movimenti aventi come scopo quello di incitare alla propaganda politica o alla commissione dei reati disciplinati nella presente parte speciale.

**I Protocolli specifici** per la prevenzione dei reati di cui sopra sono riportati nelle Procedure allegate al presente Modello.

## **10. REATI DI ABUSO DI MERCATO**

### **10.1 Descrizione delle fattispecie di reato**

In tale sezione vengono analizzate delle figure di reato astrattamente ipotizzabili per COM.E, tenuto conto che la sua attività si svolge nell'ambito dei servizi giornalistici e dell'informazione.

#### ***Manipolazione del mercato (art. 185 TUF – D. Lgs. 58/98)***

Tale reato punisce chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari ed ancor più gravemente tenuto conto della rilevante offensività del fatto, delle qualità personali del colpevole o dell'entità del prodotto o del profitto conseguito dal reato.

L'oggetto della condotta vietata, inoltre, non è limitato agli strumenti finanziari ma esteso anche a:

- a) i contratti a pronti su merci che non sono prodotti energetici all'ingrosso, idonei a provocare una sensibile alterazione del prezzo o del valore degli strumenti finanziari di cui all'articolo 180, comma 1, lettera a);
- b) gli strumenti finanziari, compresi i contratti derivati o gli strumenti derivati per il trasferimento del rischio di credito, idonei a provocare una sensibile alterazione del prezzo o del valore di un contratto a pronti su merci, qualora il prezzo o il valore dipendano dal prezzo o dal valore di tali strumenti finanziari.

#### ***Abuso di informazioni privilegiate (Art. 184)***

Punisce chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:

- a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;
- b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato effettuato ai sensi dell'articolo 11 del regolamento (UE) n. 596/2014;
- c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a), nonchè chiunque essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose compie taluna delle azioni sopra descritte.

Le pene sono altresì aumentate in ragione della rilevante offensività del fatto, delle qualità personali del colpevole o dell'entità del prodotto o del profitto conseguito dal reato.

## 10.2 Le Aree a Rischio/Sensibili

La probabilità di accadimento dei suddetti reati in COM.E è remota, tuttavia, in un'ottica prudenziale, non potendo escludere a priori condotte illecite che possano integrare le suddette fattispecie dei reati, si è proceduto alla valutazione del rischio con i principali Process Owner. Dall'analisi svolta si ritiene che, in relazione al reato sopra esplicitato, le aree che presentano un'esposizione al rischio, seppur remoto, risultano essere:

1. Gestione dei servizi giornalistici
2. Comunicazioni interne ed esterne
3. Controllo di gestione
4. Attività di tesoreria
5. Gestione dei pagamenti
6. Gestione incassi
7. Gestione dei sistemi informativi
8. Comunicazioni, incontri e richieste di autorizzazioni P.A.

Nell'espletamento di tutte le attività esposte a rischio di reato della presente sezione, oltre al rispetto di quanto indicato nel paragrafo successivo, la Società ha previsto l'attivazione di corsi di formazione e la diffusione di una propaganda di sensibilizzazione a tutti i livelli organizzativi.

## 10.3 Principi specifici di condotta nelle Aree a Rischio

Al fine di prevenire il reato considerato nella presente Sezione, dovranno essere rispettati i seguenti principi comportamentali:

- ✓ i compiti assegnati devono essere svolti con onestà, obiettività ed accuratezza;
- ✓ garantire un atteggiamento leale nello svolgimento del proprio ruolo evitando che, con la propria azione o con la propria inerzia, si commetta o si renda possibile una violazione delle norme etiche e/o di comportamento;
- ✓ assicurare, nella gestione delle informazioni acquisite la massima riservatezza. È in ogni caso fatto divieto di utilizzare informazioni riservate quando questo possa configurare violazione delle norme sulla privacy o di qualsiasi altra norma di legge, arrecare vantaggi personali di qualsiasi tipo sia a chi le utilizza, sia a qualsiasi altra risorsa interna od esterna all'Ente.

I **Protocolli specifici** per la prevenzione dei reati di cui sopra sono riportati nelle Procedure allegate al presente Modello.

## **11. DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE**

### **11.1 Descrizione delle fattispecie di reato**

#### ***Divulgazione di opere dell'ingegno attraverso rete telematica (Art. 171 della L. n. 633/41)***

Punisce chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

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

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

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

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

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

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

Punisce, inoltre, l'ipotesi in cui i reati di cui sopra siano commessi sopra un'opera altrui non destinata alla pubblicità ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

#### ***Reati in materia di software e banche dati (Art. 171 bis comma 1 L. n. 633/41)***

La fattispecie è stata modificata dalla L. 166/2024.

Tale norma punisce chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati ai sensi della presente legge

La pena è la medesima se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

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

***Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis comma 2 L. n. 633/1941)***

La norma punisce chiunque, al fine di trarne profitto, su supporti non contrassegnati ai sensi della presente legge riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-*quinquies* e 64-*sexies*, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-*bis* e 102-*ter*, ovvero distribuisce, vende o concede in locazione una banca di dati.

***Reati in materia di opere dell'ingegno destinate ai circuiti radiotelevisivi e cinematografico oppure letterarie, scientifiche e didattiche (Art. 171-ter L. n. 633/1941)***

La fattispecie è stata modificata dalla L. n. 166/2024

Tale reato punisce chiunque, a fini di lucro:

- a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
- b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
- c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);
- d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi

titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta l'apposizione di contrassegno ai sensi della predetta legge, privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

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

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

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

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

h-bis) abusivamente, anche con le modalità indicate al comma 1 dell'articolo 85-*bis* del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, esegue la fissazione su supporto digitale, audio, video o audiovisivo, in tutto o in parte, di un'opera cinematografica, audiovisiva o editoriale ovvero effettua la riproduzione, l'esecuzione o la comunicazione al pubblico della fissazione abusivamente eseguita.

Punisce, altresì, chiunque:

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

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

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

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

### *Violazioni nei confronti della SIAE (Art. 171 septies della L. n. 644/1941)*

La norma incriminatrice è stata modificata dalla L. 166/2024 che ha disposto l'abrogazione della lettera a) dell'articolo

Punisce chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge

### **11.2 Aree a Rischio/Sensibili**

L'esposizione al rischio di incorrere nei Reati in esame è ordinariamente connessa all'operatività aziendale e coinvolge, oltre che le figure apicali, tutti i soggetti che vi partecipano quotidianamente.

Tra le attività principali di COM.E, infatti, si annovera quella di insegnamento, nell'ambito della quale può ragionevolmente innestarsi l'attività di produzione di libri, saggi, testi, dispense ed opere letterarie in senso letterario. Oltre a tale specifico ambito, le ulteriori aree sensibili sono individuabili nelle seguenti:

1. Sistema informativo;
2. Selezione, contrattualizzazione e monitoraggio del Fornitore
3. Fatturazione
4. Gestione della Contabilità
5. Budgeting e controllo di gestione
6. Gestione incassi e pagamenti
7. Gestione cassa

### **11.3 Principi di condotta nelle Aree a Rischio**

Al fine di prevenire i reati considerati nella presente Sezione, dovranno essere rispettati i seguenti principi comportamentali:

- ✓ acquistare, utilizzare e scaricare sui dispositivi aziendali unicamente softwares e fare uso unicamente di banche dati previa sottoscrizione di apposite licenze e regolarmente muniti di contrassegno da parte del produttore;
- ✓ non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali siano conosciute o sospettate attività illecite;
- ✓ non realizzare operazioni commerciali con controparti che utilizzano strutture societarie opache e/o che impediscono l'identificazione univoca dell'assetto societario (proprietà) e/o dei reali beneficiari dell'operazione;
- ✓ tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione dell'anagrafica fornitori/clienti;

- ✓ rispettare la disciplina generale in tema di mezzi di pagamento prevista dal D.Lgs. 231/2007 (i.e. normativa assegni, divieto di possedere titoli al portatore oltre determinate soglie e/o il divieto di trasferimento per denaro contante oltre i limiti di legge in vigore);
- ✓ non accettare pagamenti e non effettuare fatturazioni nei confronti di soggetti diversi da quelli che assumono ruolo di controparti contrattuale e in assenza di adeguata giustificazione;
- ✓ sospendere/interrompere un rapporto con il fornitore laddove si evidenziassero comportamenti non in linea con la normativa, le leggi e i principi di controllo statuiti nel presente documento. Le segnalazioni, nonché le eventuali interruzioni dei rapporti devono essere effettuate con la massima tempestività;
- ✓ le attività relative alla gestione dei servizi IT da parte di COM.E devono essere svolte solo in virtù di apposito contratto di servizio che ne disciplina condizioni e modalità;
- ✓ adottare specifiche procedure per la gestione delle credenziali di accesso ai sistemi ed il loro monitoraggio periodico;
- ✓ deve essere rispettato il principio di separazione di ruoli e responsabilità nelle fasi dei processi interni dell'Ente.

È inoltre vietato:

- ✓ installare software e/o programmi non autorizzati dall'ente, nonché in violazione degli accordi contrattuali di licenza d'uso e/o di leggi e regolamenti che disciplinano il diritto d'autore;
- ✓ utilizzare gli strumenti informatici per lo svolgimento di attività illecite, per visionare, memorizzare, stampare, copiare, riprodurre, ricevere e diffondere materiale illegale, di proprietà altrui, osceno o similare;
- ✓ detenere o diffondere indebitamente il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- ✓ procurarsi illegalmente, conservare, riprodurre, diffondere, distribuire e/o utilizzare nelle attività sociali (es.: preparazione di materiale per convention, eventi istituzionali; ecc.) materiale ottenuto in violazione delle norme in materia di protezione del diritto d'autore;
- ✓ ostacolare o omettere, anche con artifici e raggiri, l'adempimento degli obblighi derivanti dalla normativa in materia di protezione del diritto d'autore.

I **Protocolli specifici** per la prevenzione dei reati di cui sopra sono riportati nelle Procedure allegate al presente Modello.

## **12. REATI TRIBUTARI**

I reati tributari introdotti dall'art. 39 del D.L. n. 124/2019, convertito in L. 157/2019 sono riconducibili ai reati di mera condotta, a consumazione istantanea, qualificati come delitti:

- ✓ Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti e mediante altri artifici;
- ✓ Emissione di fatture o altri documenti per operazioni inesistenti;
- ✓ di occultamento o distruzione di documenti contabili;
- ✓ di sottrazione fraudolenta al pagamento di imposte.

Il D. Lgs. n. 75/2020 ha ampliato il catalogo dei reati presupposto inserendo anche:

- ✓ dichiarazione infedele;
- ✓ omessa dichiarazione;
- ✓ indebita compensazione,

In tali ultime ipotesi, il D. Lgs. 156/2022, ha chiarito che le condotte sono rilevanti ai fini della responsabilità amministrativa dell'ente solo quando sono commessi al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegue o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro.

## 12.1 Descrizione delle fattispecie di reato

### ***Art. 2. Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti***

1. È punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.

2. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

2-bis. Se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

### ***Art. 3. Dichiarazione fraudolenta mediante altri artifici***

1. Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:

- a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;
- b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

2. Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

#### ***Art. 4. Dichiarazione Infedele***

1. Fuori dei casi previsti dagli articoli 2 e 3, è punito con la reclusione da due anni a quattro anni e sei mesi chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:

- a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila;
- b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni.

1-bis. Ai fini dell'applicazione della disposizione del comma 1, non si tiene conto della non corretta classificazione, della valutazione di elementi attivi o passivi oggettivamente esistenti, rispetto ai quali i criteri concretamente applicati sono stati comunque indicati nel bilancio ovvero in altra documentazione rilevante ai fini fiscali, della violazione dei criteri di determinazione dell'esercizio di competenza, della non inerenza, della non deducibilità di elementi passivi reali.

1-ter. Fuori dei casi di cui al comma 1-bis, non danno luogo a fatti punibili le valutazioni che complessivamente considerate, differiscono in misura inferiore al 10 per cento da quelle corrette. Degli importi compresi in tale percentuale non si tiene conto nella verifica del superamento delle soglie di punibilità previste dal comma 1, lettere a) e b).

La fattispecie, ai fini della responsabilità amministrativa dell'ente, rileva esclusivamente quando il delitto è commesso al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegua o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro.

#### ***Art. 5. Omessa dichiarazione***

1. È punito con la reclusione da due a cinque anni chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila.

1-bis. È punito con la reclusione da due a cinque anni chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.

2. Ai fini della disposizione prevista dai commi 1 e 1-bis non si considera omessa la dichiarazione presentata entro novanta giorni dalla scadenza del termine o non sottoscritta o non redatta su uno stampato conforme al modello prescritto.

La fattispecie, ai fini della responsabilità amministrativa dell'ente, rileva esclusivamente quando il delitto è commesso al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegna o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro.

#### ***Art. 8. Emissione di fatture o altri documenti per operazioni inesistenti***

1. È punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

2. Ai fini dell'applicazione della disposizione prevista dal comma 1, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

2-bis. Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

#### ***Art. 10. Occultamento o distruzione di documenti contabili***

1. Salvo che il fatto costituisca più grave reato è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

#### ***Art. 10 quater. Indebita compensazione***

La fattispecie di reato è stata introdotta nel catalogo dei reati presupposto dal D. Lgs. n. 75/2020 e modificata dal D. Lgs. 87/2024.

Rileva esclusivamente quando il delitto è commesso al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegna o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro.

1. È punito con la reclusione da sei mesi a due anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a cinquantamila euro.

2. È punito con la reclusione da un anno e sei mesi a sei anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai cinquantamila euro.

2-bis. La punibilità dell'agente per il reato di cui al comma 1 è esclusa quando, anche per la natura tecnica delle valutazioni, sussistono condizioni di obiettiva incertezza in ordine agli specifici elementi o alle particolari qualità che fondano la spettanza del credito.

### ***Art. 11. Sottrazione fraudolenta al pagamento di imposte***

1. È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

2. È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

Si precisa che per "**dichiarazioni**" si intendono le dichiarazioni presentate in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche o di sostituto d'imposta, nei casi previsti dalla legge e con l'espressione "**imposta evasa**" si intende la differenza tra l'imposta effettivamente dovuta e quella indicata nella dichiarazione, ovvero l'intera imposta dovuta nel caso di omessa dichiarazione, al netto delle somme versate dal contribuente o da terzi a titolo di acconto, di ritenuta o comunque in pagamento di detta imposta prima della presentazione della dichiarazione o della scadenza del relativo termine; non si considera imposta evasa quella teorica e non effettivamente dovuta collegata a una rettifica in diminuzione di perdite dell'esercizio o di perdite pregresse spettanti e utilizzabili.

Per "**fatture o altri documenti per operazioni inesistenti**" si intendono le fatture o gli altri documenti aventi rilievo probatorio analogo in base alle norme tributarie, emessi a fronte di operazioni non realmente effettuate in tutto o in parte o che indicano i corrispettivi o l'IVA in misura superiore a quella reale, ovvero che riferiscono l'operazione a soggetti diversi da quelli effettivi.

Il concetto di inesistenza deve essere inteso in senso lato, comprensivo di ogni genere di divergenza tra la realtà documentata nella dichiarazione e quella effettiva.

I documenti diversi dalle fatture sono solo quelli idonei ad assolvere ad una funzione probatoria nei confronti dell'Amministrazione finanziaria quali: fatture redatte con modalità alternative (nota, parcella, conto e simili), scontrini e ricevute fiscali, documenti di trasporto, auto fatture.

Le soglie di punibilità previste nelle specifiche norme, quando si riferiscono all'imposta evasa, si intendono estese anche all'ammontare dell'indebito rimborso richiesto o dell'inesistente credito di imposta esposto nella dichiarazione.

Inoltre, l'ente è responsabile anche laddove intervenga il pagamento del debito tributario, comprensivo di interessi e sanzioni, non operando in suo favore la causa di non punibilità prevista dall'art. 13 del richiamato D. Lgs. 74/2000 a favore del solo agente persona fisica.

## **12.2 Aree a Rischio/Sensibili**

L'esposizione al rischio di incorrere nei Reati tributari è ordinariamente connessa all'operatività aziendale e coinvolge, oltre che le figure apicali, tutti i soggetti che partecipano alla gestione amministrativa e contabile della Società:

1. Selezione e gestione del Personale
2. Selezione, contrattualizzazione e monitoraggio del Fornitore
3. Fatturazione
4. Gestione della Contabilità
5. Adempimenti civilistici, previdenziali e fiscali
6. Budgeting e controllo di gestione
7. Gestione incassi e pagamenti
8. Gestione cassa

## **12.3 Principi di condotta nelle Aree a Rischio**

I membri degli Organi Sociali, i Dipendenti ed i Collaboratori di COM.E, nella misura in cui gli stessi possano essere coinvolti nelle Attività Sensibili, hanno l'obbligo di attenersi a regole di condotta conformi a quanto prescritto nella presente sezione della Parte Speciale al fine di prevenire e impedire il verificarsi dei Reati ivi considerati ed astrattamente ipotizzabili in relazione alle Aree a Rischio e quanto regolamentato dalle relative Procedure già elencate:

Costituisce, pertanto, elemento di fondamentale importanza poter documentare, a fronte di pagamenti emessi o ricevuti, l'effettività della prestazione.

Essa sarà dimostrabile, in relazione ad acquisti o vendite, dagli ordini delle merci e dai relativi documenti di trasporto (o similari) e, in relazione alla fornitura di servizi, dai report che i Consulenti devono fornire attestante le attività svolte.

Nell'espletamento delle attività aziendali è espressamente vietato a chiunque porre in essere comportamenti, anche omissivi, tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente sezione della Parte Speciale.

I **Protocolli specifici** per la prevenzione dei reati di cui sopra sono riportati nelle Procedure allegate al presente Modello.

### **13. DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E TRASFERIMENTO FRAUDOLENTO DEI VALORI**

Il D. Lgs. n. 184 dell'8 novembre 2021 (in attuazione della legge delega 22 aprile 2021, n. 53 recante "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea", ha introdotto nel D. Lgs. 231/01 l'art. 25 octies 1 (Delitti in materia di strumenti di pagamento diversi dai contanti), estendendo la responsabilità amministrativa degli enti ai reati:

- ✓ Indebito utilizzo e falsificazione di strumenti di pagamento diverso dai contanti (Art. 493 ter c.p.);
- ✓ Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (Art. 493 quater c.p.);
- ✓ Frode informatica, nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (Art. 640 ter c.p.).

La Legge n. 137/2023 è intervenuta anche sull'art. 25 octies 1 del D. Lgs. 231/01 estendendo il catalogo dei reati presupposto con l'aggiunta del reato di

- ✓ Trasferimento fraudolento dei valori (Art. 512 bis c.p.)

#### **13.1 Descrizione delle fattispecie di reato**

Si riportano di seguito le fattispecie di reato che, a seguito di apposita mappatura dei rischi, sono ritenute sensibili in relazione all'organizzazione e ai processi in uso alla Società:

##### ***Art. 493 ter c.p.. Indebito utilizzo e falsificazione di strumenti di pagamento diverso dai contanti***

Il reato punisce la condotta di chi al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi o comunque ogni altro strumento di pagamento diverso dai contanti.

Analogamente, viene punito chi al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è ordinata la confisca delle cose che servirono o furono destinate a commettere il reato, nonché del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.

***Art. 640 ter, comma 2, c.p.. Frode informatica, nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale***

Il comma 2 dell'art. 640 ter c.p. prevede un aggravamento di pena nel caso in cui la frode informatica produca un trasferimento di denaro, di valore monetario o di valuta virtuale.

### **13.2 Aree a Rischio/Sensibili**

L'esposizione al rischio di incorrere nei Reati di cui all'art. 25 octies 1 del D. Lgs. 231/01 è ordinariamente connessa all'operatività aziendale e coinvolge, oltre che le figure apicali, tutti i soggetti che partecipano alla gestione amministrativa e contabile della Società:

9. Selezione e gestione del Personale
10. Selezione, contrattualizzazione e monitoraggio del Fornitore
11. Fatturazione
12. Gestione della Contabilità
13. Adempimenti civilistici, previdenziali e fiscali
14. Budgeting e controllo di gestione
15. Gestione incassi e pagamenti
16. Gestione cassa

### **13.3 Principi di condotta nelle Aree a Rischio**

I membri degli Organi Sociali, i Dipendenti ed i Collaboratori di COM.E, nella misura in cui gli stessi possano essere coinvolti nelle Attività Sensibili, hanno l'obbligo di attenersi a regole di condotta

conformi a quanto prescritto nella presente sezione della Parte Speciale al fine di prevenire e impedire il verificarsi dei Reati ivi considerati ed astrattamente ipotizzabili in relazione alle Aree a Rischio e quanto regolamentato dalle relative Procedure già elencate:

Costituisce, pertanto, elemento di fondamentale importanza poter documentare, a fronte di pagamenti emessi o ricevuti, l'effettività della prestazione.

Essa sarà dimostrabile, in relazione ad acquisti o vendite, dagli ordini delle merci e dai relativi documenti di trasporto (o similari) e, in relazione alla fornitura di servizi, dai report che i Consulenti devono fornire attestante le attività svolte.

Nell'espletamento delle attività aziendali è espressamente vietato a chiunque porre in essere comportamenti, anche omissivi, tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente sezione della Parte Speciale.

**I Protocolli specifici** per la prevenzione dei reati di cui sopra sono riportati nelle Procedure allegate al presente Modello.

**Allegati:**

**Allegato 1: Matrice dei Rischi**

**Allegato 2: Mappatura dei Processi e Procedure**

**Allegato 3: Procedure**

**Allegato 4: Codice Etico**