Modello di Organizzazione, Gestione e Controllo

di

UCA ASSICURAZIONE SPESE LEGALI E PERITALI S.p.A.

ex D. Lgs. 8 giugno 2001, n. 231

INDICE

Scheda del documento

Tipologia di documento	Modello di Organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001
Redazione	Organismo di Vigilanza
Rilascio	Presidente e Amministratore Delegato
Approvazione	Consiglio di Amministrazione
Data ultima approvazione	18/12/2025
Data entrata in vigore	18/12/2025

Aggiornamenti e revisioni	
Versione	**Approvazioni**
1.0	Prima redazione (approvata il 07/09/2015)
2.0	Prima revisione (approvata il 14/12/2016)
3.0	Seconda revisione (approvata il 29/06/2017)
4.0	Terza revisione (approvata il 15/10/2018)
5.0	Quarta revisione (approvata il 19/12/2019)
6.0	Quinta revisione (approvata il 17/12/2020)
7.0	Sesta revisione (approvata il 23/03/2021)
8.0	Settima revisione (approvata il 03/08/2022)
9.0	Ottava revisione (approvata il 15/12/2023)
10.0	Nona revisione (approvata il 19/12/2024)
11.0	Decima revisione (approvata il 18/12/2025)

Definizioni

ANIA = Associazione Nazionale fra le Imprese Assicuratrici.

Aree aziendali = aree interne di organizzazione dell'Ente. Nello specifico, si tratta dell'Area Amministrazione, Finanza e Controllo, dell'Area Commerciale, dell'Area Organizzazione/IT, dell'Area Sinistri.

Attività sensibili = attività o processi leciti dell'Ente nel compimento dei quali è possibile, in astratto, ipotizzare la commissione di uno o più dei reati di cui al D.Lgs. 231/01.

Autorità Garante per la Privacy = il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente istituita dalla legge sulla privacy (legge 31 dicembre 1996, n. 675) che ha attuato nell'ordinamento giuridico italiano la direttiva comunitaria 95/46/CE- e oggi disciplinata dal Codice in materia di protezione dei dati personali (D.Lg. 30 giugno 2003, n. 196).

c.c. = codice civile.

C.C.N.L. = contratto collettivo nazionale di lavoro attraverso il quale la Compagnia disciplina il rapporto lavorativo con il personale dipendente.

C.d.A. = Consiglio di Amministrazione.

Circolare n. 83607/2012 = circolare della Guardia di Finanza avente ad oggetto l'attività della Guardia di Finanza a tutela del mercato dei capitali, di data 19 marzo 2012.

Codice etico = insieme dei valori fondanti e dei principi di condotta adottati da UCA.

Confisca = acquisizione coatta da parte dello Stato di beni o denari quale conseguenza della commissione di un reato.

c.p. = codice penale.

D.Lgs. 231/01 o Decreto = D.Lgs. di data 08 giugno 2001, n. 231, intitolato *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300"* e successive modifiche e integrazioni.

D.Lgs. 209/05 = Codice delle Assicurazioni Private o CAP.

D.Lgs. 152/06 = Codice dell'Ambiente.

D.Lgs. 231/07 (Decreto Antiriciclaggio) = recepisce la Direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, nonché la Direttiva 2006/70/CE che ne reca misure di esecuzione.

D.Lgs. 81/08 (Decreto Sicurezza) = Testo Unico sulla salute e sicurezza nei luoghi di lavoro.

D.Lgs. 24/2023 (Decreto *Whistleblowing*) = recepisce la direttiva (UE) 2019/1937, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

Destinatari = ai sensi dell'art. 5 del D. Lgs. 231/01, tutti coloro che rivestono funzioni di rappresentanza, amministrazione e direzione ovvero gestione e controllo ed i dipendenti; il Modello si applica altresì, nei limiti del rapporto in essere, ai soggetti che collaborano con l'Ente.

Dipendenti = soggetti legati da un rapporto di lavoro subordinato con UCA Assicurazione Spese Legali e Peritali S.p.A.

DVR = Documento di Valutazione dei Rischi. È lo strumento prescritto dal D. Lgs. 81/08 che valuta tutti i rischi per la salute e la sicurezza dei lavoratori e predispone le misure di prevenzione e protezione da adottare al fine di annullare detti rischi.

Ente = Compagnia di assicurazione UCA Assicurazione Spese legali e peritali S.p.A.

Intermediari = gli intermediari sia persone fisiche sia persone giuridiche, che agiscono in nome o per conto di UCA Assicurazione Spese Legali e Peritali S.p.A.

IVASS = Istituto per la Vigilanza sulle Assicurazioni Private e di interesse collettivo.

Linee Guida ANIA = linee guida per il settore assicurativo elaborate dall'ANIA *ex* art. 6, comma terzo, D.Lgs. 231/01.

Linee Guida Confindustria = linee guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo approvate il 7 marzo 2002 e aggiornate nel marzo 2014.

MOG = Modello di Organizzazione, Gestione e Controllo *ex* art. 6, D. Lgs. 231/01.

Organismo di Vigilanza (brevemente Organismo o anche OdV) = organismo deputato al controllo del funzionamento, dell'osservanza e dell'aggiornamento del MOG, dotato di autonomi poteri di iniziativa e controllo.

P.A. = Pubblica Amministrazione e, con riferimento ai reati nei confronti della Pubblica Amministrazione, i pubblici ufficiali e gli incaricati di un pubblico servizio.

Principio di legalità = principio in forza del quale l'Ente non può essere punito per un fatto non costituente reato, ovvero per un reato che non rientri tra quelli richiamati dal D.Lgs. 231/01.

Riserva di legge = attribuzione alla legge del potere di individuare i fatti costituenti reato ai sensi del D.Lgs. 231/01.

Quote = misura utilizzata per la determinazione delle sanzioni pecuniarie compresa tra un minimo di

100 e un massimo di 1.000.

Reati = reati di cui agli artt. 24 e ss. del D. Lgs. n. 231/01.

Regolamento IVASS n. 40 del 2 agosto 2018 = Regolamento recante disposizioni in materia di distribuzione assicurativa e riassicurativa di cui al Titolo IX del D.Lgs. 209/2005.

Regolamento UE 2016/679 (GDPR) = Regolamento (UE) del Parlamento e del Consiglio del 27 aprile 2016 n. 679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Sanzioni disciplinari = manifestazione del potere esercitabile dal datore di lavoro nei confronti del lavoratore a fronte di comportamenti di quest'ultimo che costituiscono inosservanza degli obblighi contrattuali.

Sanzioni interdittive = sanzioni che determinano una compressione della libertà organizzativa dell'Ente.

Sistema disciplinare = sistema disciplinare di cui all'art. 6, comma 2, lett. e) del D.Lgs. n. 231/01 consistente nell'insieme delle misure sanzionatorie applicabili in violazione del MOG.

Sistema 231 = inteso come insieme degli strumenti previsti dal Decreto, vale a dire il MOG e l'OdV.

SISTRI = sistema di controllo della tracciabilità dei rifiuti, nato su iniziativa del Ministero dell'Ambiente e della Tutela del Territorio e del Mare per permettere l'informatizzazione della tracciabilità dei rifiuti speciali a livello nazionale.

Soggetti in posizione apicale = persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché persone che ne esercitano, anche di fatto, la gestione e il controllo (*ex* art. 5, lett. a) del D. Lgs. 231/01).

Soggetti sottoposti all'altrui direzione o vigilanza = persone sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione apicale (*ex* art. 5, lett. b) del D. Lgs. 231/01).

UCA Assicurazione Spese legali e peritali S.p.A. o UCA Assicurazione S.p.A. o Compagnia = Compagnia di Assicurazione con sede legale in Torino, Piazza San Carlo, 161 - Palazzo Villa, legali rappresentanti Rag. Luigi Gilardi e Dott.ssa Adelaide Gilardi, P.IVA - N Iscr. Reg. Imprese 00903640019 - R.E.A. 115282 - Iscr. Sez. I Albo Imprese ISVAP N 1.00024 del 03/01/2008, Capitale Sociale € 6.000.000,00

Whistleblowing = segnalazione rivolta all'OdV, avente ad oggetto la comunicazione di condotte illecite, rilevanti ai fini del D.Lgs. 231/01, nonché ai fini del D.Lgs. 24/23.

Descrizione sintetica delle Politiche, delle Procedure e dei Processi adottati da UCA e richiamati nel Modello di Organizzazione, Gestione e Controllo

Politica degli Investimenti = illustra i principi nella selezione e gestione degli investimenti, in coerenza con il principio della persona prudente e tenendo conto del profilo di rischio e della durata delle passività detenute; illustra le modalità di identificazione, misurazione, monitoraggio, gestione, controllo e segnalazione dei rischi connessi a ciascuna tipologia di attività; illustra le modalità di identificazione e gestione di eventuali conflitti di interessi nell'attività di investimento; illustra le procedure e le tempistiche di monitoraggio dei risultati degli investimenti.

Politica delle Informazioni Statistiche = assicura la tracciabilità tempestiva delle operazioni aziendali e dei fatti di gestione; garantisce la qualità delle informazioni statistiche sulla base di processi e procedure di raccolta, elaborazione, revisione e segnalazione efficienti; garantisce che i dati, le informazioni e i documenti trasmessi all'IVASS sulle attività aziendali e sull'evoluzione dei rischi siano completi e aggiornati; assicura nel continuo l'integrità, la completezza, la correttezza e disponibilità delle informazioni e dei documenti trasmessi all'IVASS.

Politica delle Misure di Protezione dei Dati, di Sicurezza delle Informazioni e Politica per la Protezione delle Informazioni in Transito = delinea le misure adottate dall'azienda per assicurare la protezione dei dati in ogni fase del loro trattamento.

Politica di Acquisizione, Sviluppo e Manutenzione dei Sistemi ICT = definisce i criteri e le procedure per l'acquisizione, lo sviluppo e la manutenzione dei sistemi ICT, per garantire che siano sicuri, efficienti e conformi alle normative vigenti, proteggendo i dati aziendali e personali.

Politica di Continuità dell'Attività = presidia la gestione di situazioni ed eventi dannosi che possano compromettere la continuità dell'attività dell'impresa.

Politica di Crittografia e di Gestione delle Chiavi Crittografiche = definisce l'uso della crittografia e la gestione delle chiavi crittografiche all'interno dei sistemi informatici della Compagnia, al fine di proteggere i dati sensibili e garantire la riservatezza, l'integrità, l'autenticità e la disponibilità dei dati conservati. Si applica a tutti i dati gestiti dalla Compagnia, inclusi i dati relativi ai clienti, i dati finanziari e altre informazioni aziendali riservate.

Politica di Esternalizzazione e Scelta dei Fornitori e sull'utilizzo dei Servizi ICT, compresi quelli

a Supporto di Funzioni Essenziali o Importanti, prestati da Fornitori Terzi di Servizi ICT = definisce un quadro di riferimento per 1) l'esternalizzazione di funzioni e attività, anche essenziali o importanti di cui all'art. 64 del Reg. IVASS n. 38/2018, nel cui ambito sono individuati ruoli e responsabilità da un punto di vista organizzativo e procedurale; 2) la selezione e la gestione dei fornitori per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti; 3) la selezione e la gestione dei fornitori ICT e non ICT per attività esternalizzate e non esternalizzate.

Politica di Formazione dell'Organo Amministrativo, di Controllo e del Personale Rilevante = regola le modalità di formazione degli Amministratori, dei Sindaci e del Personale Rilevante al fine di garantire un'adeguata conoscenza del settore di attività in cui opera la Compagnia, nonché al fine favorire l'effettiva adesione di tutto il personale ai principi di integrità morale e ai valori etici.

Politica di Gestione degli Accessi = è deputata a garantire che l'accesso ai sistemi informatici, alle reti, ai dati e alle risorse informative della Compagnia avvenga in modo controllato e sicuro, onde proteggere la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni aziendali riducendo il rischio di accessi non autorizzati, furti di dati, perdite o compromissioni.

Politica di Gestione dei Reclami = sistematizza i principi, i criteri e le regole sulla base dei quali la Società garantisce efficienza e tempestività nella gestione dei reclami.

Politica relativa alla Gestione dei Rischi = disciplina il processo di gestione dei rischi, grazie al quale la Compagnia è in grado, attraverso un adeguato processo di analisi, di comprendere la natura dei rischi individuati, la loro origine, la possibilità o necessità di controllarli e gli effetti che possono derivarne.

Politica di Gestione del Capitale = definisce le procedure volte a regolare la classificazione, l'emissione, il monitoraggio, l'eventuale distribuzione, nonché il rimborso degli elementi dei fondi propri, monitorandone la corretta attuazione e assicurandone l'adeguatezza e l'aggiornamento nel tempo.

Politica di Gestione del Patrimonio Immobiliare = definisce i ruoli, le responsabilità e l'approccio della Compagnia in merito ai processi di gestione del patrimonio immobiliare.

Politica di Gestione del Rischio Liquidità = definisce i provvedimenti da adottare per tenere conto del rischio di liquidità, l'appropriatezza della composizione delle attività, un piano per far fronte a modifiche delle entrate e uscite di cassa attese; formalizza la procedura per determinare il livello di

disallineamento tra le entrate e le uscite di cassa sia delle attività che delle passività e l'individuazione del fabbisogno di liquidità globale a breve e medio termine, compresa una riserva di liquidità adeguata a far fronte ad un'eventuale carenza di liquidità.

Politica di Gestione del Rischio Operativo = rappresenta la gestione del rischio operativo insito nelle attività di business al fine di introdurre un processo efficiente per l'identificazione, la valutazione, il monitoraggio e la segnalazione dei rischi operativi e diffondere la cultura di gestione del rischio operativo all'interno della Compagnia.

Politica di Gestione delle Attività e delle Passività = illustra la procedura di individuazione e valutazione dei diversi tipi di disallineamento strutturale tra attività e passività; le correlazioni tra i rischi di diverse categorie di attività e passività e tra i rischi di diverse obbligazioni di assicurazione e di riassicurazione; i disallineamenti intenzionali consentiti; la metodologia sottostante e la frequenza delle verifiche in condizioni di stress, nonché le verifiche di scenario da eseguire; le tecniche di attenuazione del rischio.

Politica di Gestione delle Identità = assicura una gestione efficace e sicura dei diritti di accesso ai dati, alle informazioni e alle risorse ICT, mediante l'identificazione e l'autenticazione univoca di tutte le persone fisiche e dei sistemi, garantendo l'assegnazione e il monitoraggio degli account utente univoci in conformità alle normative applicabili. Mira a definire un processo strutturato per il ciclo di vita delle identità, ove possibile con soluzioni automatizzate. Assicura che le identità digitali siano gestite e protette in modo conforme alle normative europee sulla resilienza operativa.

Politica di Organizzazione, Gestione e Controllo della Distribuzione = definisce i principi generali adottati dalla Compagnia con riferimento al controllo della rete distributiva.

Politica di Remunerazione e Incentivazione degli Amministratori, Organi di Controllo, Personale Rilevante, Funzioni Fondamentali ed Altri Dipendenti = definisce principi e regole per la definizione, la revisione, il monitoraggio e il controllo dei sistemi e delle pratiche retributive per i amministratori, organi di controllo, ulteriore personale rilevante e per le altre persone dipendenti della Compagnia; nello specifico, definisce gli elementi della retribuzione complessiva, i sistemi di incentivazione, i benefit e i requisiti di compliance; inoltre, impone approcci alla retribuzione che contribuiscano alla sostenibilità della Compagnia ed al rispetto delle norme di legge, regolamentari,

statutarie e del Codice Etico, promuovendo l'adozione di comportamenti ad essi conformi.

Politica di Remunerazione e Incentivazione degli Intermediari Assicurativi = mira a tutelare il cliente contro pratiche retributive scorrette dell'Intermediario o di suoi dipendenti o collaboratori; a prevenire situazioni di conflitto tra gli interessi della Compagnia e dell'Intermediario da un lato e gli interessi e le esigenze del cliente dall'altro; a evitare pratiche retributive basate in modo esclusivo o prevalente su risultati di breve termine, tali da incentivare una eccessiva esposizione al rischio; a definire delle pratiche remunerative che non inducano l'Intermediario a violare le generali regole di comportamento.

Politica per la Valutazione delle Attività e delle Passività diverse dalle riserve tecniche = disciplina la valutazione delle attività e passività diverse dalle riserve tecniche, definendo le metodologie di valutazione e i requisiti per garantire un'adeguata documentazione relativa al processo di valutazione e ai relativi controlli; illustrando i principi e i presidi adottati per assicurare l'affidabilità, la completezza e la coerenza dei dati; attribuendo alle Funzioni aziendali responsabili la competenza della valutazione dei dati relativi alle attività e passività diverse dalle riserve tecniche; definendo i contenuti minimi della relazione periodica al Consiglio di Amministrazione.

Politica relativa al Sistema di Controllo Interno = definisce i processi e gli organi aziendali coinvolti nell'individuazione e nel controllo dei rischi d'impresa e i processi di monitoraggio e segnalazione affinché gli organi di vertice siano costantemente aggiornati sull'attività di tutte le funzioni di controllo interno e sulle deleghe operative della Compagnia; garantisce la tracciabilità dei processi decisionali e la documentazione dell'operato degli organi di vertice e di controllo; prevede un adeguato sistema di trasmissione delle informazioni per ogni livello dell'impresa; garantisce il rispetto delle disposizioni legislative, regolamentari ed amministrative applicabili alla Compagnia; garantisce la disponibilità ed affidabilità delle informazioni finanziarie e non.

Politica relativa alla Funzione Attuariale = regolamenta le modalità di istituzione della Funzione Attuariale e di nomina del Titolare della Funzione, la modalità di esternalizzazione la responsabilità ed i compiti della Funzione Attuariale; definisce le linee guida del piano di lavoro; regolamenta le attività svolte, le modalità operative, i flussi informativi e le interrelazioni tra la Funzione Attuariale e le altre Funzioni, con gli Organi di Controllo e con le Aree Operative.

Politica relativa alla Funzione di Revisione Interna = descrive e disciplina ruolo responsabilità,

compiti e ambiti di competenza della Funzione di Revisione Interna della Compagnia.

Politica relativa alla Funzione di Verifica di Conformità alle Norme = definisce l'inquadramento della Funzione all'interno della struttura organizzativa della Compagnia, garantendone l'indipendenza, l'autonomia e l'obiettività di giudizio; definisce il rapporto con le altre Funzioni Fondamentali e gli ulteriori organi deputati al controllo aziendale; individua i compiti della Funzione e le garanzie per lo svolgimento dell'attività; definisce le modalità operative e gli obblighi di segnalazione della Funzione.

Politica relativa alle Risorse Umane per la sicurezza delle informazioni = garantisce la sicurezza delle informazioni e delle risorse tecnologiche attraverso una gestione rigorosa delle responsabilità e dei comportamenti del personale e dei fornitori terzi. In particolare, essa stabilisce l'assegnazione di specifiche responsabilità di sicurezza, assicurando che tutti coloro che utilizzano o accedono alle risorse ICT della Compagnia siano informati sulle politiche di sicurezza e le rispettino scrupolosamente.

Politica di Sicurezza Fisica e Ambientale = è deputata a garantire la protezione continua delle risorse critiche, la sicurezza del personale e la tutela dei dati e delle informazioni sensibili.

Politica sui Conflitti di Interesse = illustra la politica in materia di conflitti di interesse a tutela del cliente, con specifico riferimento alle fasi di costruzione ed esecuzione del contratto assicurativo, nonché della sua distribuzione.

Politica sull'Informativa al Pubblico e Politica sulle Informazioni da Fornire all'IVASS = definisce gli indirizzi da seguire per la raccolta dei dati e delle informazioni da trasmettere all'IVASS per finalità di vigilanza nella "relazione RSR", nonché dei dati e delle informazioni non sensibili, utili per la collettività, per la conoscenza delle generali condizioni della Compagnia, da indicare nella "relazione SFCR".

Politica sulla Sicurezza delle ICT Operations = garantisce la sicurezza operativa dei sistemi ICT attraverso l'implementazione di misure di sicurezza che proteggano l'integrità, la disponibilità e la riservatezza dei dati e delle infrastrutture, minimizzando i rischi derivanti da vulnerabilità e assicurando che i processi critici siano protetti da intrusioni, errori e malfunzionamenti.

Politica di Operatività Infragruppo = sebbene non faccia parte di alcun gruppo societario, UCA ha adottato tale politica in quanto intrattiene relazioni con parti correlate; la politica dota la Compagnia di

adeguati meccanismi di gestione del rischio e di controllo interno, monitorando costantemente tutte le operazioni con parti correlate, al fine di evitare conflitti di interesse.

Procedura Asset And Liability Management (ALM) = individua e definisce gli attori, le principali fasi/attività e i presidi organizzativi e documentali del processo di gestione delle attività e delle passività.

Procedura Backup = definisce i metodi adottati per garantire il backup, il ripristino e il recupero tempestivo dei dati e dei sistemi ICT.

Procedura Change Management e Procedure per l'Acquisizione, lo Sviluppo e la Manutenzione dei Sistemi ICT = descrive il processo di gestione dei cambiamenti evolutivi, anche alla luce di quanto previsto dal Regolamento DORA; a tal fine, individua e definisce gli attori, le principali fasi/attività e i presidi organizzativi e documentali che garantiscono la ricostruibilità del processo.

Procedura Comunicati Stampa = è la procedura inerente alla formulazione e all'invio dei comunicati stampa alle testate giornalistiche, ai social media della Compagnia, nonché più in generale alle attività di comunicazione verso l'esterno; individua e definisce gli attori, le principali fasi/attività e i presidi organizzativi e documentali che garantiscono la ricostruibilità del processo di comunicazione.

Procedura di Gestione degli Incidenti di Natura ICT = illustra la procedura per fronteggiare e porre rimedio ad incidenti, che includono potenziali attacchi informatici, altri eventi che possono danneggiare la riservatezza, l'autenticità, l'integrità o la disponibilità delle informazioni gestite negli asset informatici della Società.

Procedura di Gestione dei Processi e delle Procedure = per le attività operative che non risultano regolate da specifiche Politiche, la Compagnia si dota dei seguenti principi di gestione: rispetto del sistema organizzativo in essere; segregazione delle attività operative e di controllo; tracciabilità e documentabilità delle informazioni e delle operazioni; ripartizione e attribuzione dei poteri autorizzativi e decisionali.

Procedura di Gestione dei Progetti Rilevanti = definisce le fasi del processo operativo di avvio, pianificazione, esecuzione e chiusura dei progetti rilevanti, quali a titolo esemplificativo l'implementazione di nuovi prodotti, modifiche sostanziali ai prodotti esistenti, cambiamenti di natura organizzativa, la modifica sostanziale ai compiti e responsabilità di Aree/Uffici esistenti,

l'implementazione di nuovi sistemi informativi o modifiche sostanziali ai sistemi informativi, l'attività di adeguamento normativo/regolamentare, operazioni di carattere straordinario.

Procedura di Gestione del Personale = definisce gli attori, le principali fasi/attività e i presidi organizzativi e documentali che garantiscono la ricostruibilità del processo operativo di ricerca, selezione, formazione e amministrazione del personale.

Procedura di Gestione di Sicurezza della Rete = definisce le modalità operative e di controllo per garantire la protezione delle infrastrutture di rete aziendali, riducendo i rischi legati ad accessi non autorizzati, perdite di dati, incidenti informatici e garantendo la continuità operativa dei servizi IT.

Procedura di Logging = definisce le linee guida per l'implementazione, la gestione e la protezione dei log nei sistemi IT della Compagnia, al fine di garantirne la sicurezza e l'integrità.

Procedura di Valutazione degli Immobili = definisce gli attori, le principali fasi/attività e i presidi organizzativi e **documentali** che garantiscono la ricostruibilità del processo di valutazione immobiliare.

Procedura Formazione Rete Distributiva = disciplina la formazione della rete distributiva, per garantire l'aggiornamento professionale della Rete con riguardo alla tipologia di prodotti intermediati, all'evoluzione della normativa di riferimento nonché all'utilizzo degli strumenti informatici messi a disposizione dalla Compagnia.

Procedura Gara di Produzione = descrive le attività che l'Ufficio Marketing, con il supporto degli altri uffici competenti e dei consulenti esterni, attua per la predisposizione, lo svolgimento ed il monitoraggio della Gara di Produzione.

Procedura Gestione delle Risorse ICT = è deputata a censire e mappare il parco applicativo software e hardware della Compagnia, identificando gli asset principali; definisce inoltre i criteri per la valutazione delle criticità dei patrimoni informativi e dei servizi ICT a supporto delle funzioni commerciali.

Procedura Gestione delle Vulnerabilità e Patch e Gestione delle Capacità e Prestazioni = definisce le modalità operative per l'esecuzione del Vulnerability Assessment, del Penetration Test e la gestione delle patch, sia all'interno dell'infrastruttura aziendale che presso i fornitori esterni, al fine di garantire

un elevato livello di sicurezza delle informazioni, riducendo i rischi associati a vulnerabilità note e sconosciute e assicurare la continuità operativa dei sistemi critici.

Procedura ICT Continuity & Disaster Recovery = definisce l'insieme delle attività e delle misure preventive e/o di riparazione volte a minimizzare gli effetti distruttivi o dannosi di un evento che può colpire la Compagnia, garantendo la continuità delle attività.

Procedura in materia di Gestione Toner = descrive il processo di approvvigionamento e smaltimento toner delle stampanti presenti negli uffici della Compagnia e di quelle consegnate dalla Compagnia alla rete commerciale e ai dipendenti interni per l'attività di smart working.

Procedura per la Gestione delle Identità e dei Diritti di Accesso Fisici e Logici = definisce le modalità di corretta gestione delle identità digitali e degli account utente, per assicurare un controllo efficace e sicuro degli accessi ai patrimoni informativi e alle risorse ICT aziendali.

Procedura per la Protezione delle Informazioni in Transito = definisce le misure e le responsabilità necessarie a garantire la protezione delle informazioni durante il loro transito, sia all'interno che all'esterno dell'organizzazione. L'obiettivo principale è assicurare che le informazioni trasmesse mantengano la loro riservatezza, integrità, disponibilità e autenticità.

Procedura per la Sicurezza dei Dati e dei Sistemi = descrive le misure tecniche, organizzative e operative adottate per garantire un elevato livello di sicurezza dei dati e dei sistemi ICT, proteggere la riservatezza, integrità e disponibilità dei dati, garantire la resilienza operativa digitale dell'organizzazione, prevenire la perdita, compromissione o accesso non autorizzato ai dati e ai sistemi, definire un quadro strutturato per l'attuazione e la revisione delle misure di sicurezza.

Procedura Rapporti con le Autorità = descrive il processo inerente alla gestione dei rapporti con le Pubbliche Amministrazioni e le Autorità di Vigilanza, ai fini dell'esecuzione di adempimenti informativi e di segnalazione dovuti in forza della normativa di settore di riferimento e alla predisposizione e invio di eventuali comunicazioni e segnalazioni a fronte di potenziali richieste formulate dalle Autorità, ovvero per comunicazioni e scambio informazioni di interesse, nonché alla gestione dei rapporti con le Autorità in sede di eventuali sopralluoghi / ispezioni.

Procedura Segreteria Societaria = l'Ufficio Segreteria Societaria supporta la Compagnia negli adempimenti di natura societaria, di concerto con i consulenti fiscali e/o legali; la procedura descrive:

l'attività di gestione amministrativa delle attività e degli adempimenti; la procedura di predisposizione e invio delle segnalazioni verso l'Autorità di Vigilanza, l'ANIA, l'ISTAT, la Banca d'Italia e gli altri soggetti che a vario titolo debbano ricevere dalla – o possano richiedere alla – Compagnia informazioni o documentazione.

Procedura sui Flussi Informativi verso l'Alta Direzione = istituisce canali informativi idonei a garantire la ricezione da parte dell'Alta Direzione delle informazioni relative alle diverse attività svolte dalle Aree / Uffici coinvolti, al fine di garantire la trasparenza della gestione dell'impresa e assicurare le condizioni per un'efficace ed effettiva azione di indirizzo e controllo sull'attività della Società e sull'esercizio dell'Impresa da parte dell'Alta Direzione.

Procedura sui Processi e Responsabilità nelle procedure di Trasmissione dei Dati Anagrafici e Societari = definisce i processi e le responsabilità afferenti i passaggi informativi necessari a garantire la correttezza delle procedure di trasmissione dei dati necessari per il popolamento e l'aggiornamento del Registro delle imprese e dei gruppi assicurativi.

Procedura Ufficio Antifrode = descrive l'attività volta a garantire la corretta e tempestiva gestione delle segnalazioni individuando le situazioni illegalità tali da costituire frode, o tentativo di frode da parte degli Assicurati/Contraenti, degli Intermediari o di terzi a danno di UCA.

Procedura Ufficio Assunzione Rischi = individua e definisce gli attori, le principali fasi/attività e i presidi organizzativi e documentali che garantiscono il controllo costante e la ricostruibilità del processo di assunzione del rischio, individuando le tipologie di rischio/attività non direttamente assumibili dall'Intermediario e che necessitano di preventiva autorizzazione dell'Ufficio Assunzione Rischi.

Procedura Ufficio Contenzioso = descrive la struttura organizzativa, le attività relative all'Ufficio Contenzioso, la procedura di controllo interno di primo livello e i flussi informativi, per garantire la gestione ordinata e il costante monitoraggio del portafoglio, sia dal punto di vista dei crediti verso gli assicurati sia dal punto di vista dell'annullamento dei contratti su richiesta degli assicurati, degli Intermediari e dell'Alta Direzione.

Procedura Ufficio Contratti = individua e definisce gli attori, le principali fasi/attività e i presidi organizzativi e documentali che garantiscono il controllo costante e la ricostruibilità del processo

relativo alla gestione degli adempimenti dell'Ufficio Contratti.

Procedura Ufficio Gestione Tecnico – Legale = descrive le diverse attività che l'Ufficio svolge nell'ambito del Processo di governo e controllo dei prodotti, in ambito contenziosi nei confronti della Compagnia, in ambito Commerciale, nonché nel monitoraggio degli aggiornamenti normativi e giurisprudenziali.

Procedura Ufficio Relazioni con la Clientela = disciplina le fasi del processo di risposta alle richieste di informazioni presentate dalla Clientela, dalla ricezione della richiesta alla sua valutazione, fino all' invio della risposta e alla successiva chiusura e archiviazione.

PARTE GENERALE

Premessa

L'Ente, in coerenza con i principi sanciti nel Codice Etico adottato e al fine di assicurare la massima correttezza e trasparenza sul mercato, ha ritenuto conforme alle proprie politiche aziendali adottare il Modello di Organizzazione, Gestione e Controllo (altrimenti detto "Modello" o "MOG") previsto dal D.Lgs. 231/01 (di seguito, per brevità, anche detto Decreto).

In questo senso l'Ente ha istituito un Organismo di Vigilanza (di seguito anche "OdV") a composizione collegiale e mista, al quale è stata affidata la funzione di controllo del rispetto e dell'adeguatezza del Modello, di aggiornamento del medesimo, nonché di Gestore dei canali di segnalazione interna ai sensi del Decreto *Whistleblowing*.

Il presente documento, costituente il MOG dell'Ente, richiama integralmente il Codice Etico della Compagnia ed individua i principi e le procedure che devono essere osservati da tutti i destinatari del Modello nello svolgimento delle c.d. attività sensibili.

Esso costituisce regolamento interno per i destinatari e viene aggiornato periodicamente sulla base delle politiche e procedure via via approvate, così da costituire fonte e al tempo stesso monitoraggio *in continuum* della Compagnia per quanto oggetto del rischio *de quo*.

Introduzione

Il D.Lgs. 8 giugno 2001, n. 231, entrato in vigore il 4 luglio 2001, ha introdotto per la prima volta nel nostro ordinamento una forma di responsabilità amministrativa dell'Ente per gli illeciti amministrativi dipendenti da reato.

Così facendo, il Legislatore ha voluto derogare al principio espresso nell'antico brocardo "*societas delinquere non potest*", secondo il quale l'Ente non poteva mai essere ritenuto responsabile di un reato per carenza della capacità di azione.

La propensione per la qualificazione della responsabilità dell'Ente quale responsabilità amministrativa ha l'evidente finalità di assicurare, in parte, il rispetto del principio della personalità della responsabilità penale sancito dall'art. 27 della Costituzione.

Sulla base di queste premesse va comunque preso atto che la responsabilità introdotta dal Decreto costituisce un *tertium genus* di responsabilità, formalmente definita "amministrativa", ma sostanzialmente con i caratteri propri del sistema penale.

L'Ente risponderà per la "colpa in organizzazione", che sussiste quando la consumazione del reato è

dipesa da una “mancanza” presente nell’ambiente lavorativo nel quale il singolo autore ha operato.
L’Ente, tuttavia, non è chiamato a rispondere di un qualsiasi reato posto in essere dal dirigente o dal sottoposto, ma dovrà rispondere esclusivamente dei reati tassativamente elencati dal D.Lgs. 231/01: i c.d. “reati presupposto”.
Il Decreto introduce una disciplina volta, tuttavia, ad evitare la condanna dell’Ente prevedendo, attraverso l’adozione di appositi strumenti, quali il Modello di Organizzazione, Gestione e Controllo (brevemente MOG) e l’Organismo di Vigilanza (brevemente OdV), la limitazione o l’esclusione dalla responsabilità in parola.

CAPITOLO 1 PRINCIPI INTRODOTTI DAL D. LGS. 231/01

1.1 Le Linee Guida

Il presente Modello è stato ragionato prendendo in considerazione le esigenze del settore assicurativo nel quale opera l’Ente e, quindi, le prescrizioni dettate dalle Linee Guida di ANIA[1].
Le Linee Guida di ANIA non hanno carattere vincolante come si evince dall’art. 6, comma 3, del D.Lgs. 231/01, tuttavia costituiscono una base per l’eventuale adozione del MOG da parte dell’impresa di assicurazione.
Come ribadito dall’ANIA, il Modello deve essere studiato e realizzato in modo da risultare idoneo alla finalità richiesta dalla normativa di cui al Decreto, vale a dire la prevenzione del rischio reato non in astratto, ma nel concreto della specifica realtà dell’Ente, così da potersi inserire in modo efficace e costruttivo nel quotidiano svolgersi di tale realtà e da divenirne parte integrante.
Le Linee Guida di ANIA suggeriscono di costruire il MOG solo dopo aver effettuato una approfondita indagine circa l’organizzazione dell’Ente con la collaborazione anche di eventuali funzioni di controllo interno, così da riuscire ad individuare gli ambiti e le attività che potrebbero dare luogo al rischio di commissione dei reati e degli illeciti considerati dal D.Lgs. 231/01.
In un'ottica di prevenzione l’ANIA ritiene opportuno:

- elencare i reati e gli illeciti considerati dal D.Lgs. 231/01;
- descrivere l’organizzazione dell’Ente nel suo complesso;
- individuare, nel quadro dell’attività realizzata dall’Ente, gli ambiti e le attività che potrebbero dare luogo alla commissione dei reati considerati dal Decreto con conseguente responsabilità anche per l’Ente;

[1] Il riferimento è alle Linee Guida per il settore assicurativo pubblicate dall’ANIA il 14 febbraio 2003.

- esplicitare le attribuzioni delle deleghe e dei poteri e la relativa estensione, ovviamente in relazione ai reati considerati dal Decreto;
- evitare eccessive concentrazioni di potere in capo a singoli uffici o singole persone;
- garantire una chiara ed organica attribuzione di compiti;
- assicurare che gli assetti organizzativi vengano effettivamente attuati;
- determinare una serie di procedure da seguire per assumere decisioni che ricadono in capo all'Ente e che possono esporlo a responsabilità ai sensi del D.Lgs. 231/01;
- prevedere forme di tutela delle disposizioni del MOG, così da evitare la loro elusione;
- imporre procedure di trasparenza e controllo nella formazione delle provviste economiche;
- prevedere in capo a tutti i soggetti che interagiscono all'interno dell'Ente precisi obblighi di informazione verso l'OdV;
- coinvolgere tutto il personale e i collaboratori esterni nell'osservanza del MOG, ad esempio contemplando un sistema di segnalazioni delle violazioni del MOG direttamente all'OdV;
- prevedere lo svolgimento di specifici corsi per la formazione del personale e di quanti altri sottoposti alla direzione o vigilanza dell'Ente e la loro sensibilizzazione con riguardo al rischio di commissione dei reati considerati dal Decreto;
- prevedere la comminazione di sanzioni appropriate per il caso di mancato rispetto delle disposizioni recate dal Modello;
- prevedere di portare i principi che hanno guidato alla realizzazione del Modello a conoscenza (nella forma che si ritenga più idonea) delle entità o delle figure che collaborano o interagiscono con l'Ente, nonché di portare l'intero Modello a conoscenza dei soggetti sottoposti alla direzione o alla vigilanza dell'Ente;
- prevedere di inserire nei contratti che regolano i rapporti tra l'Ente e le figure ricomprese nella sua organizzazione una clausola attraverso la cui sottoscrizione i soggetti dichiarano di conoscere il Modello, o perlomeno i principi ispiratori del medesimo;
- prevedere una costante attività di verifica ed aggiornamento del MOG.

L'obiettivo finale del MOG è procedimentalizzare l'esercizio delle attività c.d. sensibili, al fine di eliminare il rischio che in capo all'Ente possa essere configurata la colpa in organizzazione presupposto della responsabilità amministrativa.

Il sistema di controlli preventivi introdotto attraverso l'adozione del MOG da parte dell'Ente dovrà essere tale che lo stesso:

- nel caso di reati dolosi, non possa essere aggirato se non fraudolentemente;
- nel caso di reati colposi, come tali incompatibili con l'intenzionalità fraudolenta, risulti comunque violato, nonostante la puntuale osservanza degli obblighi di vigilanza da parte dell'apposito organismo (OdV).

1.2 I soggetti interessati

Il D.Lgs. 231/01 si rivolge agli Enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica. Sono esclusi lo Stato, gli Enti pubblici territoriali, gli altri Enti pubblici non economici e gli Enti che svolgono funzioni di rilievo costituzionale.

1.3 Gli elementi costitutivi del reato

Il Decreto individua due categorie distinte di soggetti che, attraverso l'assunzione di una condotta penalmente rilevante, possono determinare l'insorgere della responsabilità amministrativa in capo all'Ente.

L'art. 5 del D.Lgs. 231/01 distingue:

- le persone che rivestono funzioni di rappresentanza, amministrazione o direzione dell'Ente e le persone che esercitano la gestione o il controllo dello stesso (c.d. soggetti apicali).
  Il riferimento è, ad esempio, agli amministratori, ai direttori generali, ai liquidatori, a destinatari di norme in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
- le persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui al superiore punto (c.d. soggetti sottoposti).
  In questa categoria vengono inclusi i dipendenti ma anche i collaboratori e i consulenti esterni.

La circostanza che l'Ente sia ritenuto responsabile per una condotta imputabile ad un soggetto diverso non costituisce una violazione del principio costituzionale della personalità della responsabilità penale e, quindi, non può essere considerata come un'ipotesi di responsabilità oggettiva. Invero, in forza del rapporto di immedesimazione organica con il suo dirigente apicale, l'Ente risponde per fatto proprio[2]. La condizione affinché la persona giuridica risponda delle attività poste in essere da tali soggetti è che la persona fisica abbia commesso il fatto nell'interesse o a vantaggio dell'Ente.

[2] In questo senso, cfr. C. Cass. 27735/2010: *"È manifestamente infondata la q.l.c. dell'art. 5 d.lgs. 8 giugno 2001 n. 231, sollevata con riferimento all'art. 27 cost., poiché l'ente non è chiamato a rispondere di un fatto altrui, bensì proprio, atteso che il reato commesso nel suo interesse o a suo vantaggio da soggetti inseriti nella compagine della persona giuridica deve considerarsi tale in forza del rapporto di immedesimazione organica che lega i primi alla seconda"*.

Se, viceversa, la persona fisica ha agito nell'interesse esclusivo proprio o di terzi, l'Ente non è responsabile[3].

I concetti di interesse e di vantaggio dell'Ente non vanno intesi come sinonimi. In particolare, l'interesse della persona giuridica va valutato *ex ante* e costituisce la prefigurazione di un indebito arricchimento, mentre il vantaggio richiede una verifica *ex post*, dopo che il reato è stato portato a compimento.

È stato difficile mettere in relazione questi presupposti oggettivi (l'interesse o il vantaggio dell'Ente) con i reati di tipo colposo individuati dal D.Lgs. 231/01 (ci si è chiesti come possa configurarsi un vantaggio o un interesse per un Ente in presenza, ad esempio, di un omicidio colposo).

Il ragionamento logico-giuridico muove dal presupposto che all'Ente viene contestata un'inadeguatezza organizzativa che è ben traducibile in una colpa, nel senso di non cura degli interessi pregiudicabili, magari conseguente ad una volontà di contenimento dei costi, che si traduce, a sua volta, in un vantaggio.

1.4 La responsabilità dell'Ente

L'art. 8 del D.Lgs. 231/01 attribuisce la responsabilità in capo all'Ente anche quando:

a) l'autore del reato non è stato identificato o non è imputabile;

b) il reato si estingue per una causa diversa dall'amnistia.

Pertanto, va distinta la colpevolezza dell'individuo (della quale si occupa il sistema penale tradizionale) dalla responsabilità dell'Ente, disciplinata per l'appunto dal D.Lgs. 231/01.

Nella fattispecie di cui alla superiore lett. a) rientra anche l'ipotesi della assoluzione della persona fisica per non avere commesso il fatto, così che l'Ente potrebbe essere condannato per l'illecito dipendente dallo stesso fatto per il quale l'accusato è stato prosciolto.

In tali situazioni il processo avrà luogo esclusivamente a carico della persona giuridica, non essendo possibile accertare la responsabilità penale dell'autore del reato.

In questo senso si afferma l'autonomia processuale dell'illecito amministrativo, la cui cognizione non è preclusa da particolari esiti dell'accertamento penale.La responsabilità dell'Ente permane anche in caso di morte del reo prima della condanna, di intervenuta prescrizione del reato presupposto e di remissione della querela.

[3] Sul punto, la giurisprudenza di legittimità (cfr. Cass. 9.07.2009) ha precisato che l'Ente non risponde quando il reato presupposto del singolo non integra "neppure parzialmente" l'interesse dell'Ente medesimo.

Nell'ipotesi di amnistia, se l'imputato rinuncia alla sua applicazione, non si procederà comunque nei confronti dell'Ente. La *ratio* di tale scelta va rinvenuta nella volontà di non vincolare il destino processuale dell'Ente alle scelte individuali dell'imputato. L'Ente in ogni caso può decidere di rinunciare all'amnistia.

L'individuazione del soggetto che ha commesso il reato e della posizione dal medesimo rivestita all'interno dell'Ente ha delle ripercussioni sull'attribuzione della responsabilità amministrativa in capo a quest'ultimo. In particolare, il riferimento è all'onere della prova, che si atteggia diversamente quando a commettere il reato è un soggetto che riveste una funzione apicale piuttosto che un soggetto a questo sottoposto. L'art. 6 del D.Lgs. 231/01 prevede che se il reato è stato commesso da soggetti che rivestono una posizione apicale all'interno dell'Ente, questo non è responsabile se prova:

a) di avere adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione, Gestione e Controllo (MOG) idoneo a prevenire i reati della specie di quelli che si sono verificati;
b) di essere dotato di un Organismo di Vigilanza (OdV);
c) che il soggetto agente ha commesso il reato eludendo fraudolentemente il MOG;
d) che non vi è stata omessa o insufficiente vigilanza da parte dell'OdV.

Viceversa, se il reato è stato commesso da un soggetto sottoposto, l'Ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza (art. 7 D.Lgs. 231/01).

Questa situazione è esclusa se l'Ente prima della commissione del reato ha adottato ed efficacemente attuato il MOG.

Pertanto, si può notare che, nel primo caso, l'onere di provare la circostanza esimente della responsabilità ricade sull'Ente. Nel secondo caso, invece, spetterà al Pubblico Ministero dimostrare la responsabilità dell'Ente stesso.

Come precisato nella Circolare della Guardia di Finanza n. 83607/12 il MOG adottato dall'Ente, per fungere da scriminante, deve essere costruito in modo tale da evitare il compimento di determinate condotte illecite; non è sufficiente la mera adozione del Modello, essendo necessaria una efficace ed effettiva attuazione del Modello organizzativo adottato.

In merito, è da rilevare che il legislatore, nonostante l'importanza attribuita nel sistema del D.Lgs. n. 231/2001 ai modelli organizzativi, non ne ha imposto *ex lege* l'adozione.

Tuttavia, non si può non considerare come l'adozione del MOG possa essere considerata come una misura ormai praticamente necessaria, e dunque, obbligatoria nei fatti, se non altro per beneficiare del c.d. “scudo protettivo” previsto dal Decreto.

1.5 Il sistema sanzionatorio disciplinato dal D. Lgs. 231/01

Il D.Lgs. 231/01, all’art. 9 individua la tipologia di sanzioni applicabili all’Ente che subisce una pronunzia di condanna. L’elenco di cui all’art. 9 fa riferimento alle seguenti tipologie di sanzioni:

- pecuniarie;
- interdittive: l’interdizione dall’esercizio dell’attività; la sospensione o la revoca delle autorizzazioni, delle licenze o delle concessioni funzionali alla commissione dell’illecito; il divieto di contrarre con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; l’esclusione da agevolazioni, finanziamenti o contributi e l’eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi;
- la confisca;
- la pubblicazione della sentenza.

La sanzione pecuniaria, che trova sempre applicazione nell’ipotesi di condanna dell’Ente, ha natura principalmente afflittiva e non risarcitoria, nel senso che viene irrogata con lo scopo di punire l’illecito commesso e non di reintegrare un danno patrimoniale subito da terzi.

La sua determinazione avviene attraverso l’applicazione del c.d. meccanismo delle quote, che prevede una struttura bifasica. Inizialmente il giudice individua il numero delle quote da attribuire all’Ente (compreso tra un minimo di 100 e un massimo di 1.000 quote) facendo applicazione dei criteri di cui all’art. 11 del Decreto, ovvero prendendo in considerazione: la gravità del fatto, il grado di responsabilità dell’Ente, l’atteggiamento assunto dall’Ente al fine di eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

Successivamente, sulla base della sola valutazione delle condizioni economiche e patrimoniali dell’Ente, il giudice dovrà determinare il valore della singola quota, compreso tra un minimo di € 258,00 e un massimo di € 1.549,00. Come affermato al punto 5.1. della Relazione al Decreto, per accertare le condizioni economiche e patrimoniali dell’Ente, il giudice potrà avvalersi dei bilanci o delle altre scritture comunque idonee a fotografare tali condizioni. In taluni casi, la prova potrà essere conseguita anche tenendo in considerazione le dimensioni dell’Ente e la sua posizione sul mercato.

L'art. 12 del Decreto prevede una serie di casi in cui la sanzione pecuniaria irrogata all'Ente può subire delle decurtazioni. Precisamente, la sanzione pecuniaria è ridotta della metà e comunque non può superare l'importo di € 103.291,00 se:

- l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne ha ricavato un vantaggio, o ne ha ricavato un vantaggio minimo;
- ovvero quando il danno cagionato è di particolare tenuità.

La sanzione pecuniaria è invece ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado, l'Ente:

- ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato, ovvero si è efficacemente adoperato in tal senso;
- ha attuato e reso operativo un MOG idoneo a prevenire reati della specie di quello verificatosi.

Qualora dovessero concorrere entrambe le condizioni anzidette la sanzione è ridotta dalla metà ai due terzi.

In ogni caso la sanzione pecuniaria non potrà mai essere inferiore a € 10.329,00.

La sanzione pecuniaria, determinata nei termini di cui sopra, viene sempre applicata in presenza di un illecito; diversamente per le sanzioni interdittive (già sopra indicate) che saranno applicate solo se ricorre almeno una delle seguenti condizioni (cfr. art. 13 del Decreto):

- l'Ente ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
- in caso di reiterazione degli illeciti.

Le sanzioni interdittive possono essere applicate anche in via cautelare, su richiesta del Pubblico Ministero, qualora sussistano gravi indizi della responsabilità dell'Ente e vi siano fondati e specifici elementi tali da far ritenere il concreto pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede.

In particolare, fra le sanzioni interdittive, quella concernente l'interdizione dall'esercizio dell'attività viene vista come *extrema ratio* e proprio per questo può essere applicata solo quando l'irrogazione di altre sanzioni risulta inadeguata.

In determinate ipotesi il giudice può, in luogo dell'applicazione della sanzione interdittiva che prevede l'interruzione dell'attività dell'Ente, disporre la prosecuzione dell'attività da parte di un commissario giudiziale per una durata pari a quella della pena interdittiva. Ciò può accadere quando l'Ente svolge un pubblico servizio o un servizio di pubblica necessità, la cui interruzione recherebbe

grave pregiudizio alla collettività, ovvero quando l'interruzione dell'attività dell'Ente è suscettibile di provocare gravi ripercussioni sull'occupazione del territorio.

Attesa la particolare gravità delle sanzioni interdittive esse non si applicano quando, prima della dichiarazione di apertura del dibattimento di primo grado, concorrono le seguenti condizioni:

a) l'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze del reato o, comunque, si è adoperato in tal senso;
b) l'Ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'attuazione di un MOG;
c) l'Ente ha messo a disposizione il profitto conseguito ai fini della confisca.

Con la sentenza di condanna dell'Ente è sempre disposta la confisca del prezzo (denaro o altra utilità economica data o promessa per indurre o determinare un altro soggetto a commettere il reato) o del profitto del reato (utilità economica immediata ricavata), salvo per la parte che può essere restituita al danneggiato e fatti salvi i diritti acquistati dai terzi in buona fede.

La pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'Ente viene applicata una sanzione interdittiva. La pubblicazione potrà avvenire per estratto o per intero, in uno o più giornali indicati dal giudice nella sentenza, nonché mediante affissione nel Comune ove l'Ente ha la sede. Le spese di pubblicazione saranno poste a carico dell'Ente.

Il termine di prescrizione per le sanzioni amministrative è di cinque anni, decorrenti dalla data di consumazione del reato, fatte salve le cause interruttive e sospensive della prescrizione previste dall'art. 22 D.Lgs. 231/01.

Poiché numerosi reati presupposto contenuti nel D.Lgs. 231/01 rientrano tra i reati puniti fino a 5 anni di reclusione (si ricordano, a mero titolo esemplificativo e non esaustivo: art. 316 *bis* c.p. - malversazione a danno dello Stato; art. 316 *ter* c.p. - indebita percezione di erogazioni a danno dello Stato; art. 615 *ter* c.p. - accesso abusivo ad un sistema informatico o telematico; art. 615 *quater* c.p. - detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;), si richiama il D.Lgs. 16 marzo 2015, n. 28, recante "Disposizioni in materia di non punibilità per particolare tenuità del fatto, a norma dell'articolo 1, comma 1, lettera m), della legge 28 aprile 2014, n. 67", che ha inserito nel Codice Penale un articolo, il 131 *bis*, rubricato - Esclusione della punibilità per particolare tenuità del fatto - ai sensi del quale nei reati per i quali è prevista la pena detentiva non superiore nel massimo a cinque anni, ovvero la pena pecuniaria, sola o congiunta alla pena detentiva, la punibilità è esclusa quando, per le modalità della condotta e per l'esiguità del danno o del pericolo, valutate ai sensi dell'art. 133, primo comma, l'offesa è di particolare tenuità e il comportamento risulta non abituale.

In particolare, si precisa che l'offesa non può essere ritenuta di particolare tenuità quando l'autore ha agito per motivi abietti o futili, o con crudeltà, anche in danno di animali, o ha adoperato sevizie o, ancora, ha profittato delle condizioni di minorata difesa della vittima, anche in riferimento all'età della stessa ovvero quando la condotta ha cagionato o da essa sono derivate, quali conseguenze non volute, la morte o le lesioni gravissime di una persona.

Il comportamento deve essere considerato come abituale nel caso in cui l'autore sia stato dichiarato delinquente abituale, professionale o per tendenza ovvero abbia commesso più reati della stessa indole, anche se ciascun fatto, isolatamente considerato, sia di particolare tenuità, nonché nel caso in cui si tratti di reati che abbiano ad oggetto condotte plurime, abituali e reiterate.

Alla data di redazione del presente Modello manca ancora un indirizzo univoco, sia da parte della giurisprudenza, sia da parte della dottrina, se la causa di non punibilità introdotta dall'art. 131 *bis* c.p. si applichi anche all'Ente, ovvero sia riferibile esclusivamente alla persona fisica che ha commesso il fatto.

Secondo un orientamento l'art. 131 *bis* c.p. rappresenta una causa di non punibilità anche per le persone giuridiche e gli altri soggetti destinatari del D.Lgs. 231/01, con la conseguenza che in presenza di un reato con i caratteri di cui all'articolo medesimo non sarebbe punito né l'autore del fatto, né l'Ente nella cui struttura il soggetto agente è inserito, con eccezione dei casi in cui sia ravvisabile una diversa volontà legislativa.

Un'altra opinione giunge al risultato opposto, partendo dal presupposto che la particolare tenuità del fatto integra una causa di non punibilità del reato che lascia integro il reato come fatto antigiuridico, ma fa venire meno la sua punibilità in quanto ritenuto di scarsa offensività. Sulla scorta di tale premessa, questo secondo orientamento richiama la Relazione governativa al D. Lgs. 231/01 che dichiara la non estensibilità delle cause di non punibilità all'Ente, ribadendo l'autonomia della responsabilità di quest'ultimo. Conseguentemente, in presenza di un fatto di lieve entità può accadere che la persona fisica ottenga la declaratoria di non punibilità e, viceversa, l'Ente subisca una condanna ai sensi del D.Lgs. 231/01.

Tale orientamento è stato da ultimo confermato dalla Corte di Cassazione con sentenza del 14 ottobre 2024.

1.6 Il sistema sanzionatorio previsto dal MOG

Diverso dal sistema sanzionatorio previsto per l'Ente è il sistema sanzionatorio introdotto dal MOG. L'art. 6, comma 2, lett. e) del Decreto, nell'individuare il contenuto dei Modelli di Organizzazione, Gestione e Controllo, indica espressamente quale requisito del MOG la previsione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure nel medesimo indicate.

La norma in commento è stata recentemente modificata, attraverso il recepimento delle prescrizioni di cui alla L. 179/17 (recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato", c.d. *whistleblower*), che hanno introdotto all'interno dell'art. 2 del D.Lgs. 231/01 i commi 2 *bis*, 2 *ter* e 2 *quater*.

Attraverso l'integrazione del D.Lgs. 231/01 con le previsioni della L. 179/17 è stata introdotta nel Decreto la c.d. disciplina del *whistleblowing*, ovvero della segnalazione, da parte dei dipendenti, di condotte illecite rilevanti ai sensi del D.Lgs. 231/01 o di violazioni del Modello dell'Ente di cui siano venuti a conoscenza in ragione delle funzioni svolte.

Per effetto di un tanto il D. Lgs. 231/01 impone, quale criterio di idoneità del Modello di Organizzazione, Gestione e Controllo, la previsione di sanzioni anche nei confronti di chi viola le misure di tutela del segnalante (c.d. *whistleblower*), nonché di chi effettua, con dolo o colpa grave, segnalazioni che si rivelano infondate.

Successivamente, con l'emanazione del D.Lgs. 24/2023 il legislatore ha imposto che il sistema disciplinare adottato dall'Ente includa sanzioni anche nei confronti di coloro che accertano essere responsabili degli illeciti di cui all'art. 21, comma 1, del citato Decreto[4], come nel prosieguo meglio dettagliate.

Va premesso che il sistema disciplinare introdotto dal MOG è indipendente e non pregiudica qualsiasi

[4] Si riporta l'art. 1, comma 1, D.Lgs. 24/2023: "*Fermi restando gli altri profili di responsabilità, l'ANAC applica al responsabile le seguenti sanzioni amministrative pecuniarie:*
a) da 10.000 a 50.000 euro quando accerta che sono state commesse ritorsioni o quando accerta che la segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza di cui all'articolo 12;
b) da 10.000 a 50.000 euro quando accerta che non sono stati istituiti canali di segnalazione, che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero che l'adozione di tali procedure non è conforme a quelle di cui agli articoli 4 e 5, nonché quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute;
c) da 500 a 2.500 euro, nel caso di cui all'articolo 16, comma 3, salvo che la persona segnalante sia stata condannata, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile".

altra conseguenza (di carattere civilistico, amministrativo o penale) che possa derivare dal fatto stesso.

Le sanzioni disciplinari previste dal Modello si applicano in caso di violazione o elusione delle disposizioni del MOG, indipendentemente dalla commissione o meno del reato e dall'esito dell'eventuale procedimento penale avviato, nonché per le ipotesi di seguito meglio dettagliate afferenti alla violazione della disciplina *whistleblowing* di cui all'omonimo Decreto.

UCA prende atto e dichiara che la predisposizione di un adeguato sistema sanzionatorio per la violazione delle disposizioni contenute nel Modello di Organizzazione, Gestione e Controllo è condizione essenziale per garantire l'effettività del Modello stesso, posto che la violazione delle prescrizioni contenute nel medesimo ledono di per sé solo il rapporto di fiducia che deve necessariamente intercorrere con l'Ente, a prescindere che dalle stesse derivi la commissione di uno dei reati puniti dal Decreto.

Tutti i destinatari del MOG hanno l'obbligo di segnalare tempestivamente all'OdV le violazioni e le presunte violazioni del Modello delle quali sono a conoscenza.

Precisamente, le condotte che costituiscono il presupposto per l'applicazione del sistema sanzionatorio del MOG sono le seguenti:

- assunzione, nello svolgimento delle attività sensibili dell'Ente, di condotte non conformi alle prescrizioni del MOG e/o del Codice Etico, tali da esporre il medesimo al rischio di condanna ai sensi del Decreto;
- violazione di procedure interne previste dal MOG per lo svolgimento delle attività sensibili;
- violazione delle misure poste a tutela del segnalante (c.d. *whistleblower*), nonché degli ulteriori soggetti di cui all'art. 3, comma 5, del Decreto *whistleblowing*[5];
- trasmissione all'OdV di segnalazioni che si rivelano infondate, effettuate con dolo o colpa

[5] Si riporta il disposto di cui all'art. 3, comma 5: "*Fermo quanto previsto nell'articolo 17, commi 2 e 3, le misure di protezione di cui al capo III, si applicano anche:*
a) ai facilitatori;
b) alle persone del medesimo contesto lavorativo della persona segnalante, di colui che ha sporto una denuncia all'autorità giudiziaria o contabile o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
c) ai colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
d) agli enti di proprietà della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o che ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone".

grave da parte del segnalante;

- ostacolo o tentativo di ostacolo alla segnalazione;
- mancata adozione di procedure per l'effettuazione e la gestione delle segnalazioni o adozione di procedure non conformi al Decreto *whistleblowing*;
- mancata attività di verifica e analisi delle segnalazioni ricevute;
- violazione dell'obbligo di riservatezza di cui all'art. 12 del Decreto *whistleblowing*.

Le sanzioni disciplinari di cui al presente documento vengono altresì applicate alla persona segnalante che sia stata condannata, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziale o contabile.

Nell'individuazione del sistema sanzionatorio previsto per i propri dipendenti UCA richiama integralmente l'apparato sanzionatorio contemplato dal C.C.N.L. applicato ai medesimi in vigore (C.C.N.L. per il settore assicurativo, personale dipendente non dirigente, in vigore dal 22 febbraio 2017), di seguito indicate:

- rimprovero verbale;
- biasimo inflitto per iscritto;
- sospensione dal servizio e dal trattamento retributivo per un periodo non superiore a 10 giorni;
- risoluzione del rapporto di lavoro per giustificato motivo;
- risoluzione del rapporto di lavoro per giusta causa.

La sanzione dovrà essere irrogata al dipendente rispettando la procedura dettata dall'art. 7 dello Statuto dei Lavoratori (L. n. 300/1970) e le ulteriori ed eventuali prescrizioni previste dal C.C.N.L. applicato e sopra richiamato.

Di seguito si individuano, a titolo meramente esemplificativo, le condotte che possono condurre all'applicazione delle sanzioni disciplinari sopra elencate, graduando la gravità della sanzione da irrogare in funzione della natura della violazione (formale o sostanziale), dell'intensità del dolo o del grado della colpa e delle conseguenze potenzialmente pregiudizievoli per UCA:

- incorre nel provvedimento di "rimprovero verbale" il lavoratore che commetta una violazione meramente formale delle procedure interne previste dal Modello, o adotti, nell'espletamento delle attività sensibili, un comportamento non conforme alle prescrizioni del Modello stesso, ancorché da tali violazioni o irregolarità non derivi alcuna conseguenza pregiudizievole per la Società;

- incorre nel provvedimento di “biasimo inflitto per iscritto” il lavoratore che sia recidivo nel commettere una violazione meramente formale delle procedure previste dal Modello o nell’adottare, nell’espletamento delle attività sensibili, un comportamento negligente e non conforme alle prescrizioni del Modello, pur non arrecando danno o rischio concreto alla Società;
- incorre nel provvedimento della “sospensione dal servizio e dal trattamento retributivo per un periodo non superiore a 10 giorni” il lavoratore che nel commettere una violazione sostanziale delle procedure interne previste dal Modello o nell’adottare - nell’espletamento delle attività sensibili - un comportamento non conforme alle prescrizioni del Modello, arrechi danno o crei situazioni di potenziale pericolo alla Società, ovvero pregiudichi l’efficacia dei controlli interni posti a presidio delle aree “a rischio reato”, esponendo in tal guisa la Società al rischio di commissione di reati presupposto o, comunque, a danni di natura reputazionale e/o economica;
- incorre nel provvedimento della “risoluzione del rapporto di lavoro per giustificato motivo” il lavoratore che, con notevole inadempimento delle prescrizioni del Modello nell'espletamento delle attività sensibili, ponga in essere un contegno diretto in modo non equivoco alla commissione di un reato presupposto o che determini la concreta applicazione di sanzioni di qualsiasi natura a carico della Società;
- incorre nel provvedimento della “risoluzione del rapporto di lavoro per giusta causa” il lavoratore che, nell’espletamento delle attività sensibili, commetta una violazione sostanziale delle prescrizioni del Modello, di natura dolosa o gravemente colposa, con notevole scostamento dai canoni di diligenza, prudenza e perizia imposti dall’attività esercitata, tale da compromettere irrimediabilmente il rapporto fiduciario con la Società. In particolare, rientrano tra tali condotte: 1) l’adozione, nell’ambito delle attività sensibili, di comportamenti dolosi o gravemente colposi tali da determinare o agevolare la commissione di un reato presupposto in seno alla Società; 2) la commissione o l’agevolazione di condotte illecite da cui sia derivato un pregiudizio concreto per l’integrità aziendale; 3) la recidiva in violazioni sostanziali delle prescrizioni del Modello che abbiano già, in passato, comportato l’irrogazione di sanzioni disciplinari a carico dell’autore; 4) qualsiasi contegno che abbia determinato la concreta applicazione, a carico della Società, delle sanzioni previste dal Decreto.

L’individuazione della tipologia e dell’entità della sanzione da applicare sarà effettuata considerando i seguenti criteri generali:

- la gravità della violazione, valutata anche in relazione alla gravità del danno o del pericolo arrecato all’Ente;

- la potenzialità del danno derivante all'Ente;
- l'intensità dell'elemento soggettivo della condotta (dolo, colpa);
- la posizione ricoperta dal soggetto che ha commesso la violazione;
- il comportamento complessivo tenuto dal lavoratore nel corso del rapporto lavorativo, avuto altresì riguardo alla sussistenza o meno di precedenti provvedimenti disciplinari a carico del medesimo;
- l'eventuale concorso di altri soggetti nella violazione.

In caso di violazioni del MOG commesse dagli Amministratori e dal Direttore Generale le diposizioni di cui al C.C.N.L. applicato (C.C.N.L. per il settore assicurativo personale dirigente, in vigore dal 7 giugno 2013) si integrano con gli strumenti tipici previsti dal diritto societario (quali le azioni di responsabilità), nonché con quanto disciplinato dall'Autorità di Vigilanza (Regolamento IVASS 39/2018).

L'applicazione delle sanzioni ai destinatari avverrà previa deliberazione da parte del Consiglio di Amministrazione.

In ogni caso dovrà essere assicurato il contraddittorio tra le parti prima di procedere con l'applicazione della sanzione disciplinare.

I destinatari del Modello sono tenuti a comunicare all'Organismo di Vigilanza dell'Ente segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del D.Lgs. 231/01 e fondate su elementi di fatto precisi e concordanti, nonché violazioni del MOG di cui sono venuti a conoscenza in ragione delle funzioni svolte.

L'OdV garantisce la riservatezza dell'identità del segnalante sin dalla ricezione della segnalazione ed in ogni fase successiva. La garanzia di riservatezza presuppone che il segnalante renda nota la propria identità attraverso la segnalazione e impedisce che il medesimo possa subire conseguenze pregiudizievoli in ambito disciplinare. In ogni caso l'OdV prenderà in considerazione anche le segnalazioni anonime ricevute, purché adeguatamente circoscritte.

Sono vietati gli atti di ritorsione o discriminatori nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione.

In particolare, l'Ente non può procedere al licenziamento ritorsivo o discriminatorio del segnalante, ovvero al mutamento delle mansioni al medesimo già affidate (ai sensi dell'art. 2103 del codice civile) e, più in generale, qualsiasi altra misura ritorsiva o discriminatoria sarà considerata nulla.

Le segnalazioni infondate, poste in essere con dolo o colpa grave da parte del segnalante e la violazione delle misure poste a tutela del segnalante saranno punite attraverso l'irrogazione delle sanzioni previste dal C.C.N.L. applicato, sopra meglio descritte. La sanzione da applicare verrà individuata considerando il grado di gravità della segnalazione trasmessa, nonché l'elemento psicologico che ha assistito la condotta del segnalante (dolo o colpa grave), ovvero la gravità della misura di tutela del segnalante violata.

Tutte le segnalazioni devono essere trasmesse attraverso i canali di comunicazione indicati dall'Organismo di Vigilanza (a mezzo e-mail all'indirizzo di posta elettronica: **odv@ucaspa.com**; a mezzo posta ordinaria presso la sede legale della società, in Torino, Piazza San Carlo, 161).

1.7 I reati presupposto del D. Lgs. 231/01

La responsabilità introdotta dal Decreto nei confronti degli Enti segue il principio di legalità e, pertanto, si configura esclusivamente in presenza della commissione di uno o più dei reati tassativamente individuati dal Decreto medesimo.

L'elenco dei reati richiamato dal Decreto non è immutabile, essendo costantemente oggetto di aggiornamento e modifica in relazione alle diverse esigenze di prevenzione che emergono per effetto dell'attività svolta dall'Ente e delle nuove previsioni legislative.

In questa parte generale, ai soli fini identificativi, si procede ad una elencazione per classi dei reati puniti dal Decreto:

- reati commessi nei rapporti con la Pubblica Amministrazione e reati di peculato, concussione, induzione indebita a dare o promettere utilità e corruzione (artt. 24 e 25);
- delitti informatici e di trattamento illecito di dati (art. 24 *bis*);
- delitti di criminalità organizzata (art. 24 *ter*);
- reati transnazionali (introdotti dalla L. 146/2006);
- reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 *bis*);
- delitti contro l'industria e il commercio (art. 25 *bis*.1);
- reati societari e reato di corruzione tra privati (art. 25 *ter*);
- delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 *quater*);
- pratiche di mutilazione degli organi genitali femminili (art. 25 *quater*.1);
- delitti contro la personalità individuale (art. 25 *quinquies*);
- abusi di mercato (art. 25 *sexies*);

- omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro (art. 25 *septies*);
- reati in materia di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25 *octies*);
- delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25 *octies.1*);
- delitti in materia di violazione del diritto d'autore (art. 25 *novies*);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 *decies*);
- reati ambientali (art. 25 *undecies*);
- impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 25 *duodecies*);
- razzismo e xenofobia (art. 25 *terdecies*);
- frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25 *quaterdecies*);
- reati tributari (art. 25 *quinquiesdecies*);
- contrabbando (art. 25 *sexiesdecies*);
- delitti contro il patrimonio culturale (art. 25 *septiesdecies*);
- riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25 *duodevicies*);
- delitti contro gli animali (art. 25 *undevicies*).

Per una descrizione specifica di ogni singola figura di reato di rilievo per l'Ente si rinvia alla parte speciale del presente Modello.

CAPITOLO 2 IL MOG DI UCA ASSICURAZIONE SPESE LEGALI E PERITALI S.P.A.

2.1 Sistema di *Governance* e assetto organizzativo dell'Ente

La società UCA Assicurazione Spese Legali e Peritali S.p.A. (di seguito anche "Compagnia" o "Ente"), P.IVA - N. Iscr. Reg. Imprese 00903640019 - R.E.A. 115282 - Iscr. Sez. I Albo Imprese ISVAP N 1.00024 del 03/01/2008, in persona dei legali rappresentanti, Rag. Luigi Gilardi e Dott.ssa Adelaide Gilardi, ha sede in Torino, P.zza San Carlo, 161 - Palazzo Villa.

UCA (Ufficio Consulenza Assicurazioni) è una società fondata nel 1932, a Chieri, per fornire consulenza e assistenza per tutti i rischi assicurativi. Nel 1934 UCA si trasforma in Compagnia di

Assicurazioni delle spese legali e peritali, mutando denominazione in *Ubique Consilium Adiuvat* ("in ogni circostanza il consiglio di un esperto è di giovamento").

Nell'anno successivo, con decreto ministeriale, UCA viene autorizzata a esercitare il nuovo ramo assicurativo delle spese legali, giudiziarie e peritali relative a sinistri.

Nel 1967 ad UCA viene affiancata SALDA, assicurazione specializzata nella responsabilità civile rami elementari, che sarà venduta dopo circa un decennio.

Successivamente UCA si è specializzata nel ramo della tutela legale, e, a partire dal 1994, esercita anche il ramo perdite pecuniarie, divenendo l'unica società assicurativa indipendente a esercitare, sul territorio italiano e in modo esclusivo, il Ramo Assistenza Legale e Perdite Pecuniarie.

Il Codice delle assicurazioni private (di seguito, per brevità, c.p.a., D.Lgs. 209/05), agli artt. 163, 164, 173, 174 definisce la tutela legale come il contratto con il quale l'impresa di assicurazione, verso pagamento di un premio, si obbliga a prendere a carico le spese legali peritali o a fornire prestazioni di altra natura, occorrenti all'assicurato per la difesa dei suoi interessi in sede giudiziale, in ogni tipo di procedimento, o in sede extragiudiziale, soprattutto allo scopo di conseguire il risarcimento di danni subiti o per difendersi contro una domanda di risarcimento avanzata nei suoi confronti, purché non proposta dall'impresa che presta la copertura assicurativa di tutela legale.

La Compagnia opera sul mercato avvalendosi, per la vendita, della rete di intermediari.

La *mission* della Compagnia è quella di perseguire l'eccellenza nel mercato in cui opera, attraverso il rispetto dei valori fondanti sanciti nel Codice Etico, ottenere la soddisfazione ed assicurare valore aggiunto per gli azionisti, i dipendenti, gli intermediari, gli assicurati e, in generale, per l'intera comunità, nel breve come nel lungo termine.

I poteri di gestione dell'Ente sono affidati al Consiglio di Amministrazione, organo che si compone di cinque membri: due Amministratori Delegati, tre Consiglieri di cui due privi di deleghe, uno dei quali Indipendente, incaricato del monitoraggio dell'adeguatezza e del corretto funzionamento del sistema di gestione dei rischi.

L'organo amministrativo, nell'ottica di implementare la trasparenza e la tracciabilità dei processi decisionali, ha autoregolamentato il proprio funzionamento dotandosi di un proprio Regolamento.

L'organo amministrativo nell'ambito dei propri compiti di indirizzo strategico ed organizzativo ha la responsabilità ultima del sistema di governo societario, funzionale alla sana e prudente gestione delle attività e proporzionato alla natura, alla portata e alla complessità delle attività dell'Impresa.

Sono parte integrante del sistema di governo societario il sistema dei controlli interni e il sistema di gestione dei rischi, dei quali viene mantenuta nel tempo la costante completezza, funzionalità ed

efficacia.

L'attività di vigilanza è affidata al Collegio Sindacale composto da cinque sindaci, di cui tre effettivi e due supplenti.

L'Ente ha istituito nel suo organico anche la figura del Direttore Generale - Consigliere delegato, le cui deleghe sono più precisamente dettagliate nelle relative delibere consiliari e nel Documento di *Governance* di cui all'art. 5, comma 2, lett. i), Reg. IVASS n. 38/2018.

L'Ente si è affidato per l'attività di controllo contabile ad una società di revisione dei conti esterna.

Sono state esternalizzate anche le Funzioni di Verifica di Conformità alle Norme, di Gestione dei Rischi e Attuariale.

L'assetto organizzativo aziendale si riflette nell'Organigramma e nel Funzionigramma, che individuano con chiarezza ruoli e responsabilità delle unità organizzative e che vengono portati a conoscenza di tutti i collaboratori.

2.2 Il sistema di deleghe e di procure

Il sistema di deleghe e di procure è disciplinato nello Statuto della Compagnia, al quale il presente documento fa espressamente rinvio.

Per delega si intende un atto interno di attribuzione di funzioni e di compiti.

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,
- ciascuna delega deve definire in modo specifico ed inequivoco i poteri del delegato e il soggetto cui il delegato riporta gerarchicamente.

Il C.d.A. dell'Ente ha deliberato di affidare agli amministratori, attraverso attribuzione di specifiche deleghe, la supervisione e l'indirizzo delle quattro aree di organizzazione aziendale, l'Area AFC, l'Area Commerciale, l'Area Organizzazione/IT e l'Area Sinistri.

Tali deleghe sono più precisamente dettagliate nelle relative delibere consiliari, nonché nel Documento di *Governance* di cui all'art. 5, comma 2, lett. i), Reg. IVASS n. 38/2018.

La Compagnia ha conferito mandato ad una serie di collaboratori, per la promozione ed il collocamento di prodotti assicurativi e la gestione dei rapporti con gli assicurati, i quali devono informare la Compagnia previamente di ogni assunzione di rischio o di modifica dei rischi già assunti, nell'osservanza delle regole del mandato in corso.

Al fine di dare concreta attuazione al D.Lgs. 231/01 tutte le procedure aziendali ed il sistema di

deleghe sono sottoposti ad un costante processo di revisione che rappresenta l'elemento fondamentale per lo sviluppo di un sistema di monitoraggio continuo dei rischi. I poteri connessi alla delega ricevuta devono essere esercitati in maniera prudente, equilibrata ed obiettiva, valorizzando lo spirito innovativo di ciascuna risorsa, nel rispetto dei limiti delle responsabilità di ciascuno.

2.3 Il MOG di UCA ASSICURAZIONE SPESE LEGALI E PERITALI S.P.A.

In un sistema come quello assicurativo, caratterizzato da una sempre crescente complessità degli adempimenti normativi richiesti, UCA, in coerenza con i principi individuati nel Codice Etico, persegue l'obiettivo di rispettare la legalità e la correttezza nello svolgimento della propria attività, adottando adeguati strumenti operativi e di controllo.

In quest'ottica UCA promuove la cultura del controllo e sensibilizza tutto l'organico sull'importanza del rispetto della normativa introdotta in materia di controlli interni: l'esistenza all'interno dell'impresa di adeguati presidi organizzativi e procedurali che assicurino il rispetto delle norme costituisce non solo una modalità di prevenzione dei rischi legali e reputazionali, ma anche uno strumento volto a garantire una adeguata protezione degli interessi degli assicurati.

Il MOG definisce un sistema di controlli atto ad escludere condotte che comportino la responsabilità amministrativa della Società ai sensi del D.Lgs. 231/01 e, in quanto tale, costituisce pertanto parte integrante del sistema di governo societario aziendale. La sua adozione consente ad UCA di beneficiare dell'esimente di cui al medesimo Decreto e, al contempo, migliora il sistema di *Governance*.

I principi contenuti nel presente Modello che si ispirano alle Linee Guida dell'ANIA, oltre che al contenuto del Codice Etico della Compagnia, hanno lo scopo di prevenire la commissione dei reati garantendo la piena consapevolezza in capo ai destinatari delle condotte assunte in relazione ai rischi connessi al D.Lgs. 231/01.

Il MOG si propone di individuare le c.d. attività sensibili di UCA, ovvero quelle attività nelle quali risulta più elevato il rischio della commissione di uno dei reati puniti dal Decreto, e di enunciare procedure e principi di comportamento che dovranno essere osservati da parte dei destinatari.

In particolare, il MOG prevede la predisposizione di misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge, eliminando tempestivamente le situazioni di rischio.

Il MOG costituisce regolamento interno della Compagnia e deve essere osservato anche da tutti i collaboratori esterni e dai consulenti.

L'efficacia del Modello viene garantita attraverso il suo costante adeguamento alla struttura dell'Ente

e alla previsione di un sistema sanzionatorio disciplinare, più sopra esplicitato, applicabile a tutte le ipotesi di violazione o elusione delle prescrizioni in esso contenute.

Il Modello è portato a conoscenza del personale dell'Ente con cadenza annuale, e comunque in occasione di ogni aggiornamento dello stesso, attraverso appositi flussi informativi interni.

Il Modello si basa sui seguenti principi di un adeguato sistema di controllo interno:

- **tracciabilità delle operazioni rilevanti ai fini del Decreto:** le operazioni devono essere adeguatamente documentate in maniera tale che in qualsiasi momento sia possibile risalire al soggetto che le ha eseguite e al controllo che sulle medesime è stato effettuato. La salvaguardia di dati e procedure in ambito informatico è assicurata mediante l'adozione del Modello Organizzativo *Privacy* (MOP), il quale comprende i processi, le procedure e le attività che in concreto ha svolto l'Ente per garantire un livello di sicurezza e di protezione dei dati adeguato ai rischi provenienti da minacce esterne ed interne.

  Ulteriori e specifiche misure a tutela del patrimonio informativo aziendale sono descritte nella documentazione in materia di *cyber security* (e negli allegati richiamati che ne costituiscono parte integrante e sostanziale) cui il presente Modello fa espresso rinvio, il quale definisce le misure di sicurezza assunte dall'Ente al fine di tutelare la *cyber security* aziendale;
- **separatezza delle funzioni:** nessuno può gestire in autonomia un intero processo. Sulla base di detto principio si deve assicurare che l'autorizzazione ad effettuare una determinata operazione provenga da persona diversa da quella che ha eseguito operativamente o controllato l'operazione;
- **formalizzazione delle deleghe;**
- **comunicazione obbligatoria all'OdV di tutte le informazioni rilevanti per l'espletamento del suo incarico;**
- **documentazione dei controlli:** attraverso la previsione di un sistema di *reporting* atto a documentare lo svolgimento e l'esito dei controlli anzidetti.
- **sicurezza degli accessi e dei flussi finanziari.**

In conformità a quanto disposto dall'art. 6, comma 1), lett. b), del Decreto, il presente Modello dovrà essere aggiornato in occasione di:

- innovazioni normative;
- oscillazioni giurisprudenziali rilevanti;
- violazioni del Modello e/o esiti negativi di verifiche sull'efficacia del medesimo;
- modifiche della struttura organizzativa dell'Ente, derivanti, ad esempio, da operazioni di finanza

straordinaria ovvero da mutamenti nella strategia d'impresa che dipendono dallo svolgimento di nuove attività.

I principi di riferimento del presente Modello si integrano con quelli del Codice Etico dell'Ente anche se il MOG, dando attuazione alle disposizioni di cui al D.Lgs. 231/01, ha portata e finalità diverse rispetto al Codice Etico. Infatti, va precisato che il Codice Etico ha portata generale e contiene una serie di principi di etica aziendale che l'Ente riconosce come propri e sui quali intende richiamare l'osservanza di tutti coloro che cooperano al perseguimento dei fini aziendali. Il Modello soddisfa, invece, l'esigenza di predisporre un sistema di regole interne al fine di prevenire il rischio della commissione di particolari tipologie di reati.

2.4 Le fasi di formazione del MOG di UCA

La predisposizione del presente Modello di Organizzazione, Gestione e Controllo è stata preceduta dallo svolgimento di attività propedeutiche e preparatorie che possono essere suddivise in differenti fasi e che di seguito vengono indicate:

- l'individuazione delle c.d. attività sensibili, vale a dire delle attività a rischio reato che vengono realizzate dall'Ente. Si tratta delle attività o dei processi nello svolgimento dei quali vi è la possibilità di incorrere nella commissione di uno dei reati puniti dal D.Lgs. 231/01. Un tanto sia considerando l'oggetto sociale dell'Ente, sia a seguito di specifico *assessment* di UCA;
- l'individuazione dei sistemi di controllo interno già adottati dall'Ente in relazione allo svolgimento delle attività sensibili;
- l'implementazione dei sistemi di controllo interno già adottati dall'Ente per la programmazione dello svolgimento delle attività sensibili nell'ottica di ridurre al minimo il rischio di realizzazione di uno dei reati richiamati dal Decreto, ovvero l'istituzione di sistemi di controllo interno volti a disciplinare lo svolgimento delle attività sensibili dell'Ente, qualora non ancora previsti.

L'Ente ha istituito l'Organismo di Vigilanza ai sensi dell'art. 6, comma 1, lett. b), del Decreto, con il compito di vigilare sul funzionamento e sull'osservanza del Modello e di curarne le proposte per il suo aggiornamento. Allo scopo di garantire l'adempimento delle prescrizioni dettate dal MOG, l'Ente ha:

- definito un sistema di flussi informativi rivolti all'OdV, attraverso l'istituzione di almeno un canale informatico di comunicazione;

- definito le attività di diffusione e sensibilizzazione del MOG all'interno della sua struttura e anche all'esterno, nei confronti di tutti i soggetti che intrattengono rapporti con il medesimo;
- assicurato l'applicazione di sanzioni disciplinari nelle ipotesi di violazione o di elusione delle prescrizioni indicate nel MOG.

2.5 La procedura di adozione del MOG

Il presente Modello è stato ragionato tenendo conto dell'attività dell'Ente e ponendola a confronto con le prescrizioni contenute nel D.Lgs. 231/01, con l'evidente finalità di sottrarre il medesimo al rischio di una condanna per i reati posti in essere dalle figure apicali e dai soggetti sottoposti inseriti nella sua struttura organizzativa.

Il MOG viene adottato con approvazione da parte Consiglio di Amministrazione, in conformità alle prescrizioni contenute nell'art. 6, comma 1, lettera a) del D.Lgs. 231/01.

Al medesimo è demandato anche il compito di approvare gli aggiornamenti al presente Modello, che saranno suggeriti e presentati dall'Organismo di Vigilanza.

Il Modello sarà adeguato in relazione alle ulteriori disposizioni normative emanate di volta in volta nell'ambito di applicazione del D.Lgs. 231/2001, alle più importanti pronunzie giurisprudenziali, nonché in base alle modifiche che riguarderanno l'Ente e che verranno ritenute rilevanti ai fini dell'applicazione del presente Modello.

2.6 Conoscenza e diffusione del MOG di UCA

L'Ente deve comunicare il Modello organizzativo adottato (e quindi ogni successivo aggiornamento) allo scopo di assicurare che tutti i destinatari siano a piena conoscenza sia delle procedure da seguire per compiere correttamente le proprie mansioni, sia delle sanzioni che conseguono ad eventuali inosservanze.

I membri del C.d.A. e del Collegio Sindacale osservano il rispetto del presente documento e del Codice Etico.

Considerata la sensibilità dell'Ente al rispetto dei principi di onestà e correttezza, nonché della normativa nazionale e comunitaria, ai quali impronta tutta la sua attività, e la particolare importanza della materia introdotta dal D.Lgs. 231/01, oltre che alle conseguenze che dalla mancata osservanza della medesima potrebbero derivare all'Ente, UCA promuove la formazione e lo sviluppo delle proprie risorse, organizzando appositi incontri volti ad illustrare i contenuti del Codice Etico e i principi introdotti dal D.Lgs. 231/01.

2.7 Le attività sensibili di UCA

A seguito di specifica attività di *assessment* sono stati individuati i rischi presenti all'interno dell'Ente che sono connessi alla responsabilità introdotta dal D.Lgs. 231/01, i quali vengono riassunti nella seguente tabella:

REATO - CLASSI DI REATO	INDICE DI RISCHIO (*)	ELEMENTI DI RISCHIO - NOTE
Art. 24 - Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico	**B**	Richiesta di contributi e finanziamenti pubblici; esercizio dell'attività di intermediazione assicurativa con la pubblica amministrazione; erogazione di omaggi e/o benefici.
Art. 24 *bis* - Delitti informatici e trattamento illecito di dati	**M**	Raccolta, trattamento e conservazione di dati relativi a clienti, dipendenti, collaboratori, fornitori; gestione degli applicativi informatici.
Art. 24 *ter* - Delitti di criminalità organizzata	**T**	Selezione del personale e dei collaboratori, selezione delle controparti contrattuali, gestione della contabilità.
Art. 25 - Concussione, induzione indebita a dare o promettere utilità e corruzione	**B**	Relazioni con enti pubblici, in particolare con l'IVASS (Autorità di Vigilanza), erogazione di omaggi/benefici, presentazione di dichiarazioni a enti pubblici.
Art. 25 *bis* - Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento	**B**	Gestione delle comunicazioni esterne, commercializzazione dei prodotti assicurativi.
Art. 25 *bis*.1 - Delitti contro l'industria e il commercio	**B**	Modalità di vendita dei prodotti sul mercato.
Art. 25 *ter* - Reati societari	**B**	Tenuta della contabilità, predisposizione dei documenti societari, cessione di partecipazioni, attività finanziarie.
Art. 25 *quater* - Delitti con finalità di terrorismo o di eversione dell'ordine democratico	**T**	Il rischio è trascurabile non solo per il contesto di riferimento ma anche in considerazione del rispetto della normativa antiriciclaggio.

Art. 25 *quater*.1 - Pratiche di mutilazione degli organi genitali femminili	**T**	Il rischio è trascurabile.
Art. 25 *quinquies* - Delitti contro la personalità individuale	**B**	Il rischio è basso; può rilevare, astrattamente, nella gestione dei rapporti con fornitori di servizi (es. servizi di pulizie)
Art. 25 *sexies* - Abusi di mercato	**B**	Il rischio è basso; può rilevare, astrattamente, nella gestione di informazioni c.d. "price sensitive" di cui l'Ente possa venire in possesso.
Art. 25 *septies* - Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro	**B**	Il rischio è basso essendosi l'Ente uniformato alle prescrizioni di cui al D.lgs. 81/08.
Art. 25 *octies* - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio	**M**	Ricezione di pagamenti, acquisti di beni e servizi.
Art. 25- octies.1 – Delitti in matria di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	**B**	Gestione dei pagamenti.
Art. 25 *novies* - Delitti in materia di violazione del diritto d'autore	**B**	Utilizzo degli applicativi informatici, gestione del sito internet e dei *social network*, pianificazione dell'attività pubblicitaria.
Art. 25 *decies* - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	**B**	Gestione dei rapporti con l'autorità giudiziaria, con gli organi di polizia giudiziaria.
Art. 25 *undecies* - Reati ambientali	**B**	Attività di smaltimento dei toner.
Art. 25 *duodecies* - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	**T**	Assunzioni di cittadini extra UE con permesso di soggiorno irregolare, avvio di collaborazioni con tali soggetti.

Art. 25 *terdecies* - Razzismo e xenofobia	**T**	Gestione dei rapporti con gli interlocutori, utilizzo dei locali, gestione di eventuali finanziamenti erogati dall'Ente.
Art. 25 *quaterdecies* - Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati	**T**	Il rischio è trascurabile in considerazione dell'organizzazione e dell'attività svolta dall'Ente.
Art. 25 *quinquiesdecies* - Reati tributari	**M**	Redazione del bilancio, formalizzazione ordini e contratti, ritenute relative al personale e ai lavoratori autonomi, attività di emissione di documenti contabili attivi e il ricevimento di documenti contabili passivi
Art. 25 *sexiesdecies* - Contrabbando	**T**	Il rischio è trascurabile.
Art. 25 *septiesdecies* – delitti contro il patrimonio culturale	**T**	Il rischio è trascurabile.
Art. 25 *duodevicies* – riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici	**T**	Il rischio è trascurabile.
Art. 25 *undevicies* – delitti contro gli animali	T	Il rischio è trascurabile.

Legenda:
(*) Indice di rischio T = trascurabile
B = basso
M = medio
A = alto

In particolare, deve escludersi il rischio di realizzazione delle seguenti classi di reato:

a) delitti con finalità di terrorismo o di eversione dell'ordine democratico;
b) pratiche di mutilazione degli organi genitali femminili;
c) impiego di cittadini di paesi terzi il cui soggiorno è irregolare;
d) razzismo e xenofobia;
e) frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati;
f) contrabbando;

g) delitti contro il patrimonio culturale, riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici;
h) delitti di criminalità organizzata;;
i) delitti contro gli animali.

In ogni caso, pur potendosi considerare remoto il rischio di realizzazione dei reati sopra indicati, il presente Modello individua, per alcune classi di reato, una serie di principi generali che dovranno essere osservati dai destinatari nello svolgimento delle attività sensibili al fine di eliminare definitivamente il rischio.

L'Ente si impegna a tenere costantemente monitorata la propria attività sia in relazione ai suddetti reati sia in relazione a quelli ulteriori che dovessero essere recepiti dal D.Lgs. 231/01, attraverso l'implementazione del presente Modello.

CAPITOLO 3 L'ORGANISMO DI VIGILANZA DI UCA ASSICURAZIONE SPESE LEGALI E PERITALI S.P.A.

3.1 L'Organismo di Vigilanza di UCA

È istituito, in ottemperanza alle disposizioni di cui all'art. 6 del D.Lgs. n. 231/2001, presso la Compagnia, un Organismo con funzioni di vigilanza e controllo in ordine al funzionamento, all'efficacia e all'aggiornamento del presente MOG (brevemente OdV).

In considerazione della propria struttura e delle proprie dimensioni, UCA istituisce un Organismo di Vigilanza a composizione collegiale e mista.

I componenti dell'OdV sono nominati dal C.d.A. avendo cura di verificare il possesso da parte dei medesimi dei seguenti requisiti:

- autonomia: i membri dell'OdV godono di autonomia nei confronti degli organi di direzione ed amministrazione dell'Ente;
- indipendenza: i membri dell'OdV non si trovano in una posizione, neppure potenziale, di conflitto di interessi con l'Ente;
- professionalità;
- continuità d'azione: è previsto un presidio dell'attività dell'Ente da parte dell'OdV attraverso lo scambio di flussi informativi e con il coinvolgimento nel continuo nell'attività dell'Impresa;

- onorabilità: i membri dell'OdV a) non hanno subito condanne, neanche in primo grado o attraverso una sentenza di applicazione della pena su richiesta delle parti, per uno dei reati puniti dal Decreto; b) non sono stati interdetti, anche solo in via temporanea, o sospesi dai pubblici uffici o dagli uffici direttivi delle persone giuridiche; c) non hanno procedimenti penali pendenti per uno dei reati puniti dal Decreto.

L'OdV si riserva la facoltà di farsi coadiuvare da professionisti esterni in presenza di problematiche che richiedano per la loro soluzione competenze tecniche specifiche.

I membri dell'OdV vengono revocati in presenza di una giusta causa di revoca individuata:

- nell'interdizione o nell'inabilitazione, ovvero in una grave infermità che renda il membro dell'OdV inidoneo a svolgere le funzioni di vigilanza affidate all'Organismo;
- in un grave inadempimento del Modello;
- in una sentenza di condanna passata in giudicato per aver personalmente commesso uno dei reati di cui al D.Lgs. 231/01.

Nel caso in cui un componente intenda rinunciare all'incarico deve darne motivata comunicazione al C.d.A.

L'eventuale integrazione dell'Organismo, in caso di rinuncia o di decadenza di uno dei membri, può avvenire già nel primo C.d.A. successivo.

L'OdV si è autonomamente dotato di un proprio Regolamento, che individua le regole di funzionamento dell'Organismo e che è stato comunicato al C.d.A.

L'OdV dispone di autonomi poteri di spesa che esercita attraverso un *budget* approvato annualmente dall'Organo amministrativo dell'Ente.

La pronunzia di una sentenza di condanna o di patteggiamento per uno dei reati puniti dal Decreto emessa a carico dell'Ente a seguito di accertata inadeguatezza ovvero omissione dell'attività di vigilanza determina la decadenza immediata dell'OdV.

3.2 Funzioni e poteri dell'OdV

Il D.Lgs. 231/01 attribuisce le seguenti funzioni all'OdV:

a) vigilare sull'effettività e sull'osservanza del MOG da parte dei destinatari nella misura in cui è richiesta a ciascuno di loro;
b) vigilare sull'efficacia e sull'adeguatezza del MOG in relazione alla struttura aziendale e alla effettiva capacità di prevenire la commissione dei reati di cui al D.Lgs. 231/01;
c) curare l'aggiornamento del MOG attraverso la presentazione di proposte di modifica del

documento al C.d.A.

Per svolgere le funzioni che gli sono normativamente attribuite, l'OdV dispone dei seguenti poteri di iniziativa e controllo:

- svolge periodicamente ispezioni sull'attività posta in essere dall'Ente;
- ha accesso a tutte le informazioni e ai documenti riguardanti le attività a rischio;
- può rivolgersi, per problematiche di particolare complessità, a professionisti esterni;
- conduce indagini interne per verificare la sussistenza di eventuali violazioni delle prescrizioni contenute nel MOG, portate alla sua attenzione attraverso specifiche segnalazioni o delle quali viene a conoscenza nello svolgimento dell'attività di vigilanza;
- svolge ispezioni a campione sulle procedure operative relative alle aree a rischio di reato;
- può individuare ulteriori attività a rischio rispetto a quelle già contemplate dal MOG che potranno essere ricomprese nel novero delle attività sensibili;
- monitora le iniziative per la diffusione della conoscenza e dell'apprendimento del MOG e, ove necessario, contribuisce a predisporre la documentazione interna necessaria al fine del funzionamento del MOG, contenente istruzioni d'uso, chiarimenti o aggiornamenti dello stesso;
- è costantemente informato circa le modifiche strutturali e operative che riguardano l'Ente.

L'OdV non dispone di poteri coercitivi o di intervento modificativi della struttura aziendale o sanzionatori nei confronti dei destinatari del MOG, i quali restano affidati al C.d.A.

Ai fini di cui al Decreto *whistleblowing*, l'OdV ricopre altresì il ruolo di gestore dei canali di segnalazione interna.

3.3 Attività di *reporting* dell'OdV e flussi informativi all'OdV

Garanzia fondamentale per l'attuazione e l'efficacia del "Sistema 231" è l'instaurazione di flussi informativi tra l'OdV, le principali funzioni aziendali e gli organi societari.

L'OdV riferisce:

- su base continua al C.d.A.;
- all'inizio e alla chiusura di ciascun esercizio al C.d.A. ed al Collegio Sindacale;
- immediatamente al C.d.A. in presenza di situazioni straordinarie e in caso di segnalazioni che rivestono carattere dell'urgenza.

L'OdV potrà chiedere di essere sentito dal C.d.A. ogni qualvolta ritenga opportuno un esame o un

intervento di siffatto organo in materie inerenti il funzionamento e l'efficace attuazione del MOG.
L'OdV potrà, a sua volta, essere convocato in ogni momento dal C.d.A. e dagli altri organi sociali per riferire su particolari eventi o situazioni relative al funzionamento e al rispetto del MOG.
Tutti i soggetti inseriti nella struttura dell'Ente sono tenuti, in presenza di determinate situazioni, ad un obbligo di informazione nei confronti dell'OdV.
L'obbligo di informazione incombe principalmente sulle funzioni preposte allo svolgimento delle attività a rischio reato, e, più in generale, su tutti i dipendenti e i collaboratori dell'Ente, i quali sono tenuti a comunicare tempestivamente le seguenti segnalazioni:

- eventuali notizie relative alla commissione o alla ragionevole convinzione di commissione di reati presupposto;
- violazioni o presunte violazioni -in ogni caso non manifestamente infondate- del MOG da parte di altri destinatari o di violazioni del Codice Etico;
- la pendenza di procedimenti penali a carico di dipendenti dell'Ente ai quali sia contestata la commissione di uno dei reati puniti dal Decreto;
- l'irrogazione di sanzioni disciplinari a soggetti inseriti nell'organizzazione dell'Ente.

Le condotte illecite segnalate, comunque, devono riguardare situazioni di cui il soggetto sia venuto direttamente a conoscenza in ragione del rapporto di lavoro e, quindi, ricomprendono certamente quanto il soggetto ha appreso in virtù dell'ufficio rivestito ma anche le notizie acquisite in occasione e/o a causa dello svolgimento delle mansioni lavorative, seppure in modo casuale. L'OdV prende in considerazione le segnalazioni ricevute valutandone preventivamente la fondatezza e svolgendo una successiva attività di indagine per accertare le presunte violazioni delle prescrizioni contenute nel MOG.
Per la gestione delle segnalazioni come sopra richiamate, nonché di quelle disciplinate dal Decreto *whistleblowing*, la Compagnia ha adottato canali di segnalazione interna volti a consentire il flusso di segnalazioni e informazioni verso l'OdV, nonché una apposita procedura per la gestione dei canali e delle segnalazioni.
I citati canali garantiscono la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.
L'OdV garantisce inoltre il segnalante e gli altri aventi diritto da qualsiasi forma di ritorsione, discriminazione o penalizzazione, fermo restando gli obblighi di legge e la tutela dei diritti dei soggetti accusati erroneamente.

Le segnalazioni interne possono essere effettuate:

- in forma orale, richiedendo un incontro con l'OdV, che dovrà essere fissato entro un termine ragionevole;
- in forma scritta ad uno dei seguenti canali:
    - depositando la segnalazione in apposita cassetta postale posizionata all'ingresso della Compagnia;
    - inviate a mezzo posta raccomandata presso la sede legale della Compagnia in Torino, Piazza San Carlo, n. 161, all'attenzione dell'OdV opportunamente indicato in carattere maiuscolo sulla busta;
    - a mezzo e-mail all'indirizzo di posta elettronica: **odv@ucaspa.com**

La segnalazione interna presentata ad un soggetto diverso dall'OdV dovrà essere trasmessa all'OdV entro sette giorni dal suo ricevimento, senza possibilità di trattenerne copia. Al segnalante dovrà essere dato avviso della trasmissione della segnalazione all'OdV.Per la gestione della segnalazione l'OdV si attiene a quanto disciplinato nella procedura per la gestione delle segnalazioni interne adottata dalla Compagnia, a cui si fa espresso rinvio per quanto in questa sede non dettagliato.

A tal fine l'OdV:

- identifica correttamente il segnalante acquisendone, oltre all'identità, anche la qualifica e il ruolo;
- separa i dati identificativi del segnalante dal contenuto della segnalazione, prevedendo l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva associazione della segnalazione con l'identità del segnalante solo nei casi in cui risulti strettamente necessario;
- adotta idonee modalità di conservazione dei dati e di accesso ai medesimi.

Terminata l'istruzione, l'OdV informa tempestivamente il C.d.A. che assumerà i provvedimenti del caso.

PARTE SPECIALE

CAPITOLO 4 I REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

4.1 Inquadramento dei rapporti con la P.A.

I reati contro la Pubblica Amministrazione di rilievo ai fini del D.Lgs. 231/01 sono compiuti da soggetti che, in ragione delle loro cariche o funzioni, sono entrati in contatto con soggetti che svolgono funzioni pubbliche o servizi pubblici; il presupposto di tali reati è, dunque, l'instaurazione di rapporti con la P.A.

I delitti commessi nei confronti della P.A., ai quali rimandano gli artt. 24 e 25 del D.Lgs. 231/01 sono quelli disciplinati nel Libro II, Titolo II, Capo I del codice penale.

Il concetto di Pubblica Amministrazione comprende tutta l'attività dello Stato e degli altri enti pubblici. Si fornisce di seguito un'elencazione ampia, ma non esaustiva, degli Enti pubblici:

- le amministrazioni dello Stato, delle Regioni, degli Enti territoriali e locali, degli altri Enti pubblici non economici;
- gli Organi della Commissione Europea, la Pubblica Amministrazione di Stati esteri;
- le imprese pubbliche e i soggetti privati che adempiono una funzione pubblicistica;
- Banca d'Italia, Consob, IVASS, INAIL, INPS, Agenzia delle Entrate, ecc..

Taluni dei reati contro la P.A. sono reati propri, nel senso che possono essere commessi solo da specifiche categorie di soggetti: i pubblici ufficiali e gli incaricati di pubblico servizio.

Ai sensi dell'art. 357 c.p. sono pubblici ufficiali *"coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa"*, intendendosi per funzione amministrativa quella 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.

A titolo esemplificativo, sono tali coloro che ricoprono cariche di vertice all'interno dello Stato o di Enti territoriali e, più in generale, coloro i quali in base allo statuto e al sistema di deleghe adottato ne formano la volontà o la portano all'esterno attraverso l'esercizio del potere di rappresentanza.

Conseguentemente, si rileva che vengono definite come "*funzioni pubbliche*" quelle attività amministrative che costituiscono esercizio di poteri deliberativi, autoritativi o certificativi.

Sono, invece, incaricati di un pubblico servizio, ai sensi dell'art. 358 c.p. *"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, con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".

Per pubblico servizio il Legislatore intende quel servizio disciplinato da norme di diritto pubblico, ma privo dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione. Sono incaricati di un pubblico servizio gli impiegati di un ufficio pubblico, i dipendenti di Autorità di vigilanza privi di poteri autoritativi e i dipendenti di Enti che, pur essendo privati, svolgono servizi pubblici.

UCA intrattiene i seguenti rapporti con la P.A.:

- svolge attività di assicurazione, anche avvalendosi della rete distributiva;
- stipula specifici accordi di collaborazione con la P.A.;
- intrattiene rapporti occasionali con i pubblici ufficiali e gli incaricati di un pubblico servizio;
- gestisce rapporti con l'amministrazione finanziaria per gli adempimenti tributari e con gli enti previdenziali per gli adempimenti connessi al personale dipendente;
- gestisce i rapporti con le Autorità di Vigilanza.

4.2 Fattispecie di reato nei rapporti con la P.A.

L'art. 24 del Decreto richiama i seguenti reati:

- malversazione di erogazioni pubbliche (art. 316 *bis* c.p.);
- indebita percezione di erogazioni a danno dello Stato (art. 316 *ter* c.p.);
- truffa in danno dello Stato, di altro Ente Pubblico o dell'Unione Europea (art. 640, comma 2, n.1 c.p.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 *bis* c.p.);
- frode informatica ai danni dello Stato o di altro Ente pubblico (art. 640 *ter* c.p.);
- frode nelle pubbliche forniture (art. 356 c.p.).
- frode ai danni del Fondo Europeo Agricolo (art. 2 L. 898/86);
- turbata libertà degli incanti (art. 353 c.p.);
- turbata libertà del procedimento di scelta del contraente (art. 353 *bis* c.p.).

Si descrivono di seguito alcune delle fattispecie che potrebbero assumere rilevanza rispetto

all'attività svolta dalla Compagnia.

4.3 Malversazione di erogazioni pubbliche (art. 316 *bis* c.p.)

Commette tale fattispecie delittuosa il soggetto estraneo alla Pubblica Amministrazione che avendo ottenuto dallo Stato o da altro Ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati alla realizzazione di determinate finalità di pubblico interesse, non li destina alle predette finalità.

La condotta consiste nell'avere distratto, anche parzialmente, la somma ottenuta, a prescindere dal fatto che l'attività programmata si sia effettivamente svolta.

Il reato può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengono destinati alle finalità per cui erano stati richiesti.

Esempio

Utilizzo di fondi ricevuti da una pubblica amministrazione da destinare ad attività di formazione del personale per effettuare pagamenti a diverso titolo per conto dell'Ente.

4.4 Indebita percezione di erogazioni a danno dello Stato (art. 316 *ter* c.p.)

La fattispecie punita dall'art. 316 *ter* c.p. si configura quando, mediante uno dei seguenti comportamenti:

- utilizzo o presentazione di dichiarazioni o documenti falsi o attestanti cose non vere;
- omissione di informazioni dovute,

un soggetto consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri Enti pubblici o dalle Comunità europee.

In questa ipotesi, contrariamente a quanto visto nel paragrafo precedente, non ha rilevanza l'utilizzo che viene fatto delle erogazioni indebitamente ricevute; il momento consumativo del reato coincide con l'ottenimento dei finanziamenti. Per la commissione del reato si richiede che le somme ricevute a titolo di contributo o di finanziamento non siano dovute in quanto mancano i presupposti per poterle ottenere e, di conseguenza, manca la giustificazione di un pubblico interesse.

La fattispecie di cui all'art. 316 *ter* c.p. è residuale rispetto all'ipotesi della truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 *bis* c.p.), nel senso che si configura solo nei casi in

cui la condotta non integri gli estremi del più grave reato di cui all'art. 640 *bis* c.p.

Esempio

Presentazione di una richiesta di finanziamento per attività di ristrutturazione di un immobile di proprietà della Compagnia mediante dichiarazione di presupposti falsi.

4.5 Truffa in danno dello Stato, di altro Ente Pubblico o dell'Unione Europea (art. 640, comma 2, n. 1 c.p.)

La norma punisce chi, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno. Nel caso di specie il fatto deve essere commesso in danno dello Stato o di altro ente pubblico o dell'Unione Europea.

Esempio

Nella predisposizione di documenti per la partecipazione a procedure di gara ad evidenza pubblica un membro del Consiglio di Amministrazione fornisce alla P.A. informazioni non veritiere (ad esempio, supportate da documentazione artefatta) al fine di ottenere l'aggiudicazione della gara stessa.

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

La fattispecie si configura quando gli artifizi e i raggiri tipici del reato di cui all'art. 640 c.p. (truffa) sono posti in essere per ottenere erogazioni pubbliche. A differenza della fattispecie di indebita percezione di erogazioni pubbliche, in questo caso la condotta in esame - per potersi configurare - non può prescindere dall'induzione in errore del soggetto passivo del reato (ad esempio, manca l'induzione in errore del soggetto passivo e, pertanto, il fatto potrà integrare il reato di cui all'art. 316-ter c.p. e non quello di truffa aggravata, nel caso in cui l'ente erogatore del finanziamento – ricevuta la falsa autodichiarazione – si limiti ad attestare la sussistenza dei requisiti per la spettanza del beneficio economico richiesto, senza compiere autonoma attività valutativa sul contenuto dell'autodichiarazione mendace; in tal caso, infatti, mancherebbe l'induzione in errore dell'ente che ha erogato il beneficio).

Esempio

Un membro del Consiglio di Amministrazione pone in essere condotte fraudolente, consistenti in artifici (ad esempio documentazione artefatta), traendo in inganno l'ente erogatore al fine di ottenere un contributo pubblico.

4.7 Frode informatica ai danni dello Stato o di altro Ente pubblico (art. 640 *ter* c.p.)

La fattispecie punisce il soggetto che alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo, senza diritto, con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.

Ai sensi dell'art. 24 del D.Lgs. 231/01, la frode informatica rileva se commessa in danno dello Stato o di altro ente pubblico, ossia nel caso in cui il soggetto, con la condotta di alterazione, manipolazione o intervento senza diritto sul sistema informatico o sui dati in esso contenuti, ottenga, per sé o per altri, un profitto ingiusto, cagionando in tal modo un danno allo Stato o ad altro ente pubblico.

Esempio

Dopo aver ottenuto un finanziamento, una risorsa dell'area informatica viola il sistema informatico dell'Ente pubblico erogatore, modificando i dati ed inserendo un importo relativo ai finanziamenti maggiore di quello ottenuto in modo legittimo.

4.8 Turbata libertà degli incanti (art. 353 c.p.)

La fattispecie punisce il soggetto che 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.

4.9 Turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.)

Salvo che il fatto costituisca più grave reato, la fattispecie punisce il soggetto che 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.

4.10 Frode nelle pubbliche forniture (art. 356 c.p.)

La fattispecie punisce chiunque commette frode nell'esecuzione di contratti di fornitura conclusi con lo Stato, con un ente pubblico, o con un'impresa esercente servizi pubblici o di pubblica necessità. Per contratto di fornitura si intende ogni strumento contrattuale destinato a fornire alla PA beni o servizi. Affinché si verifichi il reato in oggetto è necessaria la malafede contrattuale, ossia la presenza di un espediente malizioso o di un inganno, tali da far apparire l'esecuzione del contratto conforme agli obblighi assunti. La condotta del privato fornitore si caratterizza per non essere conforme ai doveri di lealtà e moralità commerciale e di buona fede contrattuale: in questo consiste l'elemento della frode.

4.11 Attività sensibili di UCA

Nei rapporti che l'Ente intrattiene con la P.A. sono sensibili le seguenti attività:

- gestione in generale dei rapporti con la P.A. (ad esempio gestione dei rapporti con l'Autorità di Vigilanza per scambi di comunicazioni, gestione dei rapporti con l'Autorità di Vigilanza nel corso di verifiche e ispezioni, gestione dei rapporti con l'amministrazione finanziaria per gli adempimenti tributari e fiscali, gestione dei rapporti con i pubblici ufficiali e gli incaricati di pubblico servizio in generale, gestione dei rapporti con gli enti previdenziali e assistenziali per gli adempimenti retributivi e previdenziali connessi al personale dipendente e ai collaboratori esterni);
- attività di assicurazione con la P.A.;
- conferimento di deleghe o procure per l'attività di rappresentanza nei confronti della P.A.; partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti agevolati da parte di organismi pubblici italiani o comunitari ed il loro concreto impiego;
- gestione dei rapporti con i dipendenti;
- partecipazione a gare pubbliche;
- stipula di specifici accordi di collaborazione con la P.A.;
- gestione degli affari legali e di attività giudiziali e stragiudiziali;
- ottenimento di permessi, licenze e autorizzazioni (ad esempio richiesta di concessioni edilizie, autorizzazioni comunali e certificati) per l'esercizio dell'attività aziendale;
- gestione dei flussi monetari e finanziari (ad esempio gestione della contabilità e dei pagamenti);

- gestione di erogazioni liberali (ad esempio gestione di omaggi, liberalità, sponsorizzazioni e donazioni) a rappresentanti della P.A.;
- incassi e pagamenti.

4.12 Comportamenti vietati ai destinatari del MOG

In generale è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente le fattispecie di reato considerate dal Decreto (art. 24 del D.Lgs. 231/01); sono altresì proibite le violazioni dei principi e delle procedure di cui alla Parte Speciale del MOG.

In un'ottica di prevenzione l'Ente si astiene dal porre in essere comportamenti che, sebbene non siano così gravi da realizzare le fattispecie di reato ai sensi dell'art. 24 del Decreto, possono potenzialmente diventarlo o favorirne la commissione.

In particolare, ai Destinatari è fatto divieto di:

- effettuare regali[6] che, in generale, possano anche solo essere interpretati come eccedenti le normali pratiche commerciali o di cortesia o rivolti ad acquisire trattamenti di favore nella conduzione di qualsiasi attività riconducibile all'Ente;
- effettuare qualsiasi forma di regalo a funzionari pubblici o dipendenti della P.A., a revisori, sindaci o a loro familiari che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio all'Ente;
- eseguire prestazioni e riconoscere compensi in favore dei collaboratori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- presentare dichiarazioni non veritiere, artefatte, incomplete o lacunose ad organismi pubblici al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- porre in essere contegni truffaldini od omettere informazioni dovute al fine di trarre in inganno la P.A. ed orientare a favore di UCA le decisioni che l'ente pubblico è chiamato ad assumere nei riguardi della Società;destinare eventuali somme ricevute da organismi pubblici a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli per cui erano destinate;erogare contributi ad associazioni o enti di qualsiasi tipo se per finalità estranee al raggiungimento della missione aziendale e dell'oggetto sociale di UCA;
- in sede di selezione ed assunzione del personale è vietata qualsiasi forma di nepotismo, di

[6] Per regalo si intende qualsiasi tipo di beneficio, quale a titolo esemplificativo: oggetti, biglietti per eventi sportivi, culturali o di qualunque tipo, viaggi, partecipazione gratuita a convegni, pranzi o cene che non siano strettamente necessari e motivati.

favoritismo e di clientelismo. Nell'ipotesi di assunzione di un soggetto in precedenza legato da un rapporto di lavoro con una P.A., UCA si asterrà dall'avviare trattative economiche con quest'ultima per i trentasei mesi successivi all'assunzione;

- nei rapporti economici con la P.A. gli amministratori e i collaboratori dell'Ente devono astenersi dal porre in essere comportamenti che possano indurre l'Ente pubblico a decidere in violazione di leggi, regolamenti e bandi di gara.

È pertanto vietato ai destinatari di influenzare impropriamente le decisioni delle Pubbliche Amministrazioni mediante offerta o promessa, diretta o indiretta, di beni, altre utilità o favori, al fine di ottenere il compimento di atti non conformi o contrari ai doveri d'ufficio.

4.13 Principi specifici per le procedure

Nello svolgimento delle attività sensibili di cui al presente capitolo si applicano i seguenti principi:

- la gestione di qualsiasi rapporto con la P.A. deve essere improntata al rispetto dei principi di correttezza, di trasparenza e di rispetto delle leggi vigenti;
- la gestione di trattative, l'assunzione di impegni e l'esecuzione di rapporti, di qualsiasi genere, con la P.A. e con Enti che svolgono attività di pubblica utilità o di pubblico interesse o comunque di rapporti aventi carattere pubblicistico sono riservati esclusivamente alle Funzioni aziendali a ciò preposte e/o autorizzate;
- nell'ipotesi di partecipazioni a gare pubbliche le Funzioni aziendali interessate si impegnano e verificano il rispetto della procedura di partecipazione alle gare pubbliche, nonché la normativa di riferimento;
- in presenza di una situazione di conflitto di interesse il destinatario deve informare con tempestività la Funzione aziendale di riferimento e l'OdV;
- le dichiarazioni rese alla P.A. ai fini dell'ottenimento di concessioni, autorizzazioni o licenze, nonché contributi, finanziamenti o erogazioni devono essere sempre rese da soggetti preventivamente autorizzati e devono contenere elementi assolutamente veritieri; inoltre, tutta la documentazione prodotta alla P.A. dev'essere accuratamente archiviata e conservata, al fine di garantire tracciabilità e controllo sulle attività svolte e sulle interlocuzioni intercorse;
- le somme eventualmente ricevute dalla P.A. per la realizzazione di finalità meritevoli di

interesse devono essere esclusivamente destinate all'attuazione degli scopi per i quali sono state erogate;

- i verbali relativi a ispezioni giudiziarie, tributarie o amministrative poste in essere dalle Autorità di Vigilanza di settore devono essere trasmessi all'OdV, il quale deve essere informato dell'esito di ogni controllo o ispezione;
- sono ammessi regali di modesto valore a clienti e consulenti purché siano effettuati in occasione di particolari festività (Natale e Pasqua). I regali effettuati hanno l'obiettivo di promuovere l'immagine dell'Ente sul mercato di riferimento. Detti regali devono essere sempre documentati ed autorizzati dall'Amministratore Delegato e dagli ulteriori soggetti muniti del relativo potere di firma;
- la selezione e l'assunzione del personale e dei collaboratori devono avvenire nel rispetto del criterio della trasparenza, privilegiando la professionalità. Il personale deve essere selezionato considerando la corrispondenza del profilo professionale con le competenze e le attitudini richieste da UCA, nel rispetto del principio delle pari opportunità per tutti i soggetti interessati. Qualora la persona da selezionare provenga da una P.A., l'Ufficio Gestione del Personale e il Responsabile dell'area interessata dalla nuova assunzione verificano che il soggetto non provenga da una P.A. con la quale l'Ente intrattiene dei rapporti commerciali.

  UCA non procede all'assunzione di soggetti che negli ultimi tre anni di servizio, hanno esercitato poteri autoritativi o negoziali per conto delle pubbliche amministrazioni, in aderenza a quanto sancito dall'art. 53, D.Lgs. 165/01. Detta norma prevede il divieto per i dipendenti che negli ultimi tre anni di servizio hanno esercitato poteri autoritativi o negoziali per conto delle pubbliche amministrazioni di svolgere, nei tre anni successivi alla cessazione del rapporto di pubblico impiego, attività lavorativa o professionale presso i soggetti privati destinatari dell'attività della pubblica amministrazione svolta attraverso i medesimi poteri;
- i flussi di denaro in entrata e in uscita sono costantemente monitorati. In particolare, l'Ente accerta che tutti gli incassi e tutti i pagamenti siano correlati ad attività poste in essere per il raggiungimento della missione sociale. Con specifico riferimento ai pagamenti effettuati alla P.A. è necessario procedere alla tracciabilità e verificabilità *ex post* delle transazioni tramite adeguati supporti documentali/informativi;
- il pagamento delle fatture è effettuato solo previa verifica della sussistenza della documentazione giustificativa del pagamento.

Chiunque venga a conoscenza di violazioni o presunte violazioni rilevanti ai fini della responsabilità dell'Ente è tenuto ad informare, mediante apposita segnalazione, l'OdV.

CAPITOLO 5 REATI DI CONCUSSIONE, INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ E CORRUZIONE

5.1 Le fattispecie di reato punite dall'art. 25 del Decreto

L'art. 25 del Decreto richiama i seguenti reati:

- concussione (art. 317 c.p.);
- corruzione per l'esercizio di una funzione (artt. 318, 321 c.p.);
- corruzione per un atto contrario ai doveri d'ufficio (artt. 319, 321 c.p.);
- traffico di influenze illecite (art. 346 *bis* c.p.);
- corruzione in atti giudiziari (artt. 319 *ter*, 321 c.p.);
- induzione indebita a dare o promettere utilità (art. 319 *quater* c.p.);
- corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.);
- istigazione alla corruzione (art. 322 c.p.);
- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e ai funzionari delle Comunità europee e degli Stati esteri (art. 322 *bis* c.p.);
- peculato (art. 314, comma 1, c.p.);
- peculato mediante profitto dell'errore altrui (art. 316 c.p.);
- indebita destinazione di denaro o cose mobili (art. 314 *bis* c.p.).

Si descrivono di seguito alcune delle fattispecie che potrebbero assumere rilevanza rispetto all'attività svolta dalla Compagnia.

5.2 Concussione (art. 317 c.p.)

La norma punisce il pubblico ufficiale o l'incaricato di un pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Esempio

Un dipendente in concorso con un pubblico ufficiale costringe un terzo a dare o promettere un pagamento non dovuto.

5.3 Corruzione per l'esercizio di una funzione (art. 318 c.p.)

La fattispecie si verifica quando il pubblico ufficiale, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa. L'art. 321 c.p. estende la punibilità anche al privato corruttore, ossia il soggetto che indebitamente offre o promette al funzionario pubblico il denaro o l'utilità non dovuta per sollecitare l'esercizio delle sue funzioni.

Esempio

Un componente del Consiglio di Amministrazione offre ad un pubblico ufficiale una somma di denaro per velocizzare la pratica di rilascio di una concessione o di un'autorizzazione.

5.4 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 riceva, per sé o per altri, denaro o altri vantaggi o ne accetti la promessa per omettere o ritardare o aver omesso o ritardato atti del suo ufficio, oppure per compiere o aver compiuto un atto contrario ai doveri del suo ufficio (determinando un vantaggio in favore dell'offerente). L'attività del pubblico ufficiale potrà estrinsecarsi in un atto contrario ai suoi doveri, illecito in quanto contrario a norme imperative o illegittimo poiché in contrasto con uno specifico dovere dell'ufficio.

Questa fattispecie di reato si differenzia dalla concussione in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre dalla concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio. Ne consegue che, mentre nel caso della concussione, il privato è relegato a mera vittima del reato, nell'ipotesi di corruzione c.d. "propria" anche il privato corruttore soggiace alla stessa pena prevista per il funzionario pubblico.

Esempio

Il pubblico ufficiale che accetta denaro da un componente del Consiglio di Amministrazione per garantire l'aggiudicazione di una gara all'Ente, violando il dovere di imparzialità. Oppure, si pensi al contegno del componente del Consiglio di Amministrazione che offre ad un pubblico ufficiale una

somma di denaro perché questi si impegni ad informarlo di eventuali controlli fiscali organizzati dal proprio comando sull'Ente e ad intervenire positivamente per impedire accertamenti sfavorevoli al medesimo.

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

La norma, che costituisce una fattispecie residuale rispetto a quelle disciplinate dagli artt. 318, 319, 319 *ter* e 322 *bis* c.p., punisce il soggetto che 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, per remunerare un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322 *bis*, relazione all'esercizio delle sue funzioni, ovvero per realizzare un'altra mediazione illecita. La norma precisa che per "*altra mediazione illecita*" si intende la mediazione per indurre il funzionario pubblico a compiere un atto contrario ai doveri d'ufficio costituente reato dal quale possa derivare un vantaggio indebito.
La norma punisce anche il soggetto che dà indebitamente o promette denaro o altra utilità economica.

La fattispecie, introdotta dalla Legge n. 190/2012, ha subito negli ultimi anni diverse modifiche; da ultimo ad opera della Legge n. 114/2024 che, rispetto alla formulazione introdotta dalla Legge n. 3/2019 (c.d, "Spazzacorrotti"), ha reso penalmente irrilevante la mera vanteria delle relazioni asserite con il funzionario pubblico, richiedendo che il mediatore utilizzi relazioni esistenti con il funzionario pubblico, non più soltanto asserite. Inoltre, per effetto dell'attuale formulazione, è priva di rilevanza penale la mediazione finalizzata ad indurre il pubblico ufficiale al compimento di un atto contrario ai doveri d'ufficio che non costituisca reato: poiché, nella stragrande maggioranza delle ipotesi, l'atto contrario ai doveri d'ufficio cui si dirige la mediazione è costituito da un abuso d'ufficio del funzionario pubblico, per effetto della sua abrogazione (ad opera della stessa L. 114/2024), il campo applicativo del traffico di influenze illecite risulterà di molto ristretto.

Esempio
Il Consigliere promette denaro ad un terzo che vanta una relazione realmente esistente con un funzionario IVASS al fine di remunerarlo per eludere l'avvio di controlli sull'Ente.

5.6 Corruzione in atti giudiziari (art. 319 *ter* c.p.)

Tale fattispecie delittuosa si configura nel caso in cui, per favorire o danneggiare una parte in un procedimento giudiziario (civile, penale o amministrativo), l'Ente corrompa un pubblico ufficiale (non solo un magistrato ma anche un cancelliere, un perito, un consulente tecnico o un altro funzionario) commettendo le condotte di cui agli artt. 318 e 319 c.p. Questa ipotesi di reato si realizza al fine di ottenere un vantaggio anche per l'Ente che non necessariamente deve essere parte del procedimento.

Esempio
Un componente del Consiglio di Amministrazione versa denaro ad un cancelliere del Tribunale affinché accetti, seppur fuori termine, il deposito di memorie o di produzioni documentali.

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

Questa fattispecie criminosa si configura nei casi in cui, salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a sé o a un terzo, denaro o altra utilità. La punibilità, oltre che per il pubblico ufficiale e l'incaricato di pubblico servizio, è prevista anche per il privato che, a differenza dell'ipotesi di concussione, non è obbligato, ma solamente indotto da parte del funzionario pubblico alla promessa o dazione e, pertanto, non può essere considerato una mera vittima del reato; in altri termini, nell'ipotesi di induzione indebita, il privato conserva una possibilità di scelta e, a fronte della pressione morale esercitata dal pubblico ufficiale, finisce per prestare acquiescenza alla richiesta della prestazione non dovuta, in quanto motivato dalla prospettiva di conseguire un indebito tornaconto personale: il che giustifica l'applicazione di una pena anche al soggetto privato.

Esempio
Il responsabile delle risorse umane, nel corso di una visita ispettiva da parte di un funzionario della competente Autorità di Vigilanza, viene indotto dal medesimo ad assumere il proprio figlio, al fine di scongiurare l'irrogazione alla Società di una sanzione (purché legittima; infatti, se la minaccia di sanzione da parte dell'autorità di Vigilanza fosse illegittima, non si verserebbe nell'ipotesi di

induzione indebita, bensì di concussione e, pertanto, il soggetto costretto ad assumere sarebbe una mera vittima del reato, come tale non punibile).

5.8 Istigazione alla corruzione (art. 322 c.p.)

Si tratta di una forma anticipata di "corruzione" che ricorre quando, in presenza di un comportamento finalizzato alla corruzione, questa non si perfeziona in quanto il pubblico ufficiale rifiuta l'offerta o la promessa non dovuta e illecitamente avanzatagli per l'esercizio delle sue funzioni o dei suoi poteri o per il compimento di un atto contrario ai doveri d'ufficio.

Esempio

Un componente del Consiglio di Amministrazione offre ad un pubblico ufficiale una somma di denaro per velocizzare la pratica di rilascio di una concessione o di un'autorizzazione; il pubblico ufficiale, tuttavia, rifiuta l'offerta..

5.9 Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e ai funzionari delle Comunità europee e degli Stati esteri (art. 322 bis c.p.)

Questo articolo non fa altro che estendere ai membri della Corte penale internazionale o degli organi delle Comunità europee ed ai funzionari delle Comunità europee e degli Stati esteri i reati di concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione. È un reato che si concretizza nelle fattispecie sopra descritte, nelle quali però il "corrotto" è un membro della Corte penale internazionale o degli organi delle Comunità europee ovvero un funzionario delle Comunità europee e degli Stati esteri.

Esempio

Si rinvia agli esempi sopra indicati riferendo a soggetti della Corte penale internazionale o degli organi delle Comunità europee e ai funzionari delle Comunità europee e degli Stati esteri.

5.10 Attività sensibili di UCA

Le fattispecie di reati sopra analizzate potrebbero verificarsi nei rapporti con la P.A. finalizzati alla:

- negoziazione/stipulazione e/o esecuzione di contratti/convenzioni ai quali si perviene mediante procedure ad evidenza pubblica;
- gestione dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni, licenze, provvedimenti amministrativi occasionali/*ad hoc* necessari allo svolgimento di attività tipiche aziendali ed attività strumentali, e per la cura di adempimenti quali comunicazioni, dichiarazioni, deposito atti e documenti, pratiche, ecc. e per le verifiche/accertamenti/procedimenti sanzionatori che ne derivano;
- gestione dei rapporti con i soggetti pubblici per gli aspetti che riguardano la sicurezza e l'igiene sul lavoro (ad esempio il D.Lgs. 81/08);
- gestione di trattamenti previdenziali del personale e/o gestione dei relativi accertamenti/ispezioni e gestione dei rapporti con i soggetti pubblici relativi all'assunzione di personale appartenente a categorie protette o la cui assunzione è agevolata;
- gestione dei rapporti con i fornitori;
- gestione delle attività di acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici;
- predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere;
- gestione di visite ispettive, verifiche, accertamenti, procedimenti giudiziali o arbitrali;
- gestione dei rapporti con le Autorità di Vigilanza (richieste di informazioni, chiarimenti, scambi di corrispondenza, comunicazioni, ecc.);
- gestione delle risorse finanziarie;
- gestione del patrimonio immobiliare.

5.11 Comportamenti vietati ai destinatari del MOG

In generale è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente le fattispecie di reato considerate dal Decreto (art. 25 del D.Lgs. 231/01); sono altresì proibite le violazioni dei principi e delle procedure dell'Ente individuate nella presente Parte Speciale.

In un'ottica di prevenzione l'Ente è altresì tenuto ad astenersi dal porre in essere comportamenti che, sebbene non siano così gravi da realizzare le fattispecie di reato ai sensi dell'art. 25 del Decreto, possano potenzialmente diventarlo o favorirne la commissione.

UCA vieta ogni forma di corruzione nei confronti di soggetti che lavorano nella P.A.; rifiuta ogni forma di induzione indebita da parte di rappresentanti della P.A., siano essi pubblici ufficiali o soggetti incaricati di un pubblico servizio.

UCA vieta altresì ogni forma di corruzione nei confronti di soggetti che lavorano in aziende private.

Nell'ambito dei suddetti divieti è in particolare fatto divieto di:

- elargire o promettere somme di denaro o qualsiasi utilità comunque non riconducibili alla propria prestazione professionale a funzionari della P.A. o a loro familiari, a funzionari di Enti erogatori di fondi pubblici senza giustificativi, ovvero a soggetti che vantano relazioni (esistenti o asserite) con un pubblico ufficiale;
- effettuare qualsiasi forma di regalo a funzionari pubblici o dipendenti della P.A., a revisori, sindaci o a loro familiari, a soggetti che vantano relazioni (esistenti o asserite) con un pubblico ufficiale, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio a UCA;
- accordare altri vantaggi di qualsiasi natura in favore di rappresentanti della P.A., nonché a soggetti che vantano relazioni (esistenti o asserite) con un pubblico ufficiale, che possano determinare le stesse conseguenze previste al precedente punto, ad esempio, mediante assunzione di persone che non possiedono i requisiti necessari per la mansione offerta;
- eseguire prestazioni e riconoscere compensi in favore dei rappresentanti della P.A. che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- effettuare pagamenti a funzionari pubblici, nonché a soggetti che vantano relazioni (esistenti o asserite) con un pubblico ufficiale, con denaro contante o altre utilità non dovute (e ciò vale anche se si è indotti da un pubblico ufficiale o da un incaricato di pubblico servizio);
- nei rapporti economici con la P.A., porre in essere comportamenti che possano indurre l'Ente pubblico a decidere in violazione di leggi, regolamenti e bandi di gara;
- in occasione di richieste o rapporti con la P.A., tenere qualsiasi comportamento diretto ad influenzare impropriamente le decisioni della controparte, comprese quelle dei funzionari che trattano o prendono decisioni per conto della P.A.

5.12 Principi specifici per le procedure

Nello svolgimento delle attività sensibili di cui al presente capitolo si osservano le seguenti procedure:

- la gestione di qualsiasi rapporto con la P.A. deve essere improntata al rispetto dei principi di correttezza, di trasparenza e di rispetto delle leggi vigenti;
- la gestione di trattative, l'assunzione di impegni e l'esecuzione di rapporti, di qualsiasi genere, con la P.A. e con Enti che svolgono attività di pubblica utilità o di pubblico interesse o comunque di rapporti aventi carattere pubblicistico sono riservati esclusivamente alle Funzioni aziendali a ciò preposte e/o autorizzate;
- tutte le comunicazioni e gli adempimenti previsti dalla legge e dai regolamenti nei confronti della PA e delle Autorità di Vigilanza devono essere eseguiti con tempestività, correttezza e buona fede, diligenza e professionalità, in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere, evitando e comunque segnalando nella forma e nei modi idonei, situazioni di conflitto di interesse; inoltre, in occasione di tali comunicazioni, occorre utilizzare canali di comunicazione che permettono la successiva tracciabilità delle informazioni inviate o ricevute; inoltre, nel caso in cui la documentazione da inviare alla P.A. sia prodotta – anche solo in parte – con il supporto di soggetti terzi (consulenti, ecc.), è necessario selezionare gli stessi in base a requisiti di professionalità, indipendenza e competenza;
- alle Aree e agli Uffici a qualsiasi titolo coinvolti nella gestione dei rapporti con i funzionari delle Autorità nell'ambito di sopralluoghi / visite ispettive, è fatto divieto, a titolo esemplificativo e non esaustivo, di fornire dati, informazioni, documenti o dichiarazioni incompleti, falsi o alterati; chiedere o indurre i funzionari delle Autorità a trattamenti di favore ovvero omettere informazioni dovute al fine ostacolare l'esercizio delle stesse nell'ambito di sopralluoghi e ispezioni; tenere una condotta ingannevole che possa indurre i funzionari delle Autorità in errore; ostacolare/ritardare la produzione e/o l'invio dei riscontri alle richieste/istanze pervenute dalle stesse Autorità; influenzare il giudizio, il parere, il rapporto o le conclusioni delle Autorità di Vigilanza;

in tutti i casi in cui è possibile e compatibile con le tempistiche accordate si richiede di adottare soluzioni che prevedano la predisposizione del documento da consegnare alla P.A. o all'Autorità di Vigilanza da parte di più soggetti competenti in materia (meccanismo di

maker/checker); inoltre, nel corso degli incontri con le Autorità, ove possibile, è richiesta la presenza di almeno due persone della Compagnia tra i quali, ove possibile, un Responsabile di Area/Ufficio, così come previsto dalla Procedura Rapporti con le Autorità;

- tutta la documentazione prodotta e consegnata alla P.A. e alle Autorità di Vigilanza dev'essere debitamente archiviata e conservata, al fine di garantire la tracciabilità e la trasparenza del processo;
- nel caso di contenziosi giudiziali/stragiudiziali/arbitrati che coinvolgono UCA, i professionisti esterni ai quali viene affidata la relativa gestione sono selezionati sulla base di criteri di esperienza, requisiti soggettivi di professionalità e onorabilità; l'operato di tali professionisti è oggetto di costante monitoraggio, al fine di garantire che i rapporti con l'Autorità Giudiziaria nell'ambito del contenzioso siano improntati ai principi di correttezza, trasparenza e tracciabilità, anche quando gestiti per il tramite di un legale esterno; inoltre, l'OdV deve essere tempestivamente informato dell'avvio di procedimenti giudiziali/stragiudiziali e di arbitrati che coinvolgono UCA;
- sono ammessi regali di modesto valore a clienti e consulenti purché siano effettuati in occasione di particolari festività (Natale/Pasqua). I regali effettuati hanno l'obiettivo di promuovere l'immagine dell'Ente sul mercato. Detti regali devono essere sempre documentati ed autorizzati dall'Amministratore Delegato e dagli ulteriori soggetti muniti del relativo potere di firma;
- i dipendenti e i collaboratori dell'Ente sono autorizzati a ricevere regali di modesto valore in occasione di particolari festività. Gli omaggi e le utilità ricevute, aventi caratteristiche in contrasto con i principi di cui sopra, verranno devolute a fini di beneficenza o utilità sociale;
- deve essere garantita l'applicazione del principio di separazione delle funzioni tra chi autorizza, chi esegue e chi controlla, anche nei pagamenti;
- dev'essere garantita l'osservanza, da parte di tutti i richiedenti l'esecuzione di flussi finanziari, dei budget di spesa assegnati; nel caso di superamento di tali limiti di spesa, il processo dev'essere accompagnato da specifica autorizzazione che espliciti le ragioni della deroga;
- i flussi di denaro in entrata e in uscita sono costantemente monitorati. In particolare, l'Ente accerta che tutti gli incassi e tutti i pagamenti siano correlati ad attività poste in essere per il raggiungimento della missione aziendale. Con specifico riferimento ai pagamenti effettuati

- alla P.A. è necessario procedere alla tracciabilità e verificabilità *ex post* delle transazioni tramite adeguati supporti documentali/informativi; a tal fine, dev'essere garantita la conservazione, per ogni operazione, di adeguata documentazione a supporto dell'attività svolta, in modo da consentire l'individuazione del percorso decisionale e dei diversi livelli di responsabilità, nonché l'agevole ricostruzione dell'operazione;
- i fornitori sono selezionati seguendo il principio dell'imparzialità e dell'equità e sulla base di dati oggettivi e documentabili, verificando che non sussista una situazione di conflitto di interessi con l'Ente;
- in conformità a quanto previsto dalla Procedura Ufficio Contratti, occorre garantire evidenza documentale e la corretta archiviazione: degli ordini di acquisto o di altri documenti (contratti, accordi) sulla base dei quali vengono effettuati gli acquisti di beni e servizi; delle comunicazioni inoltrate ai fornitori a seguito di problemi e/o inefficienze riscontrate in fase di approvvigionamento (relative a tematiche di qualità, quantità, tempistiche di approvvigionamento difformi dalle condizioni contrattuali, ecc.); di autorizzazioni a eventuali deroghe alle condizioni standard concesse ai fornitori (ad esempio rispetto ai termini di pagamento, ad eventuali anticipi, ecc.);
- nell'ambito dell'attività di selezione del personale, la scelta dei candidati avviene esclusivamente sulla base di criteri di merito, volti a privilegiare le competenze e le capacità dei candidati rispetto al ruolo da ricoprire; prima di procedere all'instaurazione del rapporto di lavoro, viene accertato il possesso dei requisiti di onorabilità e di affidabilità in capo al candidato; l'intero processo di selezione ed assunzione è debitamente tracciato, onde garantire massima trasparenza; sono in ogni caso vietate pratiche discriminatorie o assunzioni per motivi di favore, finalizzate ad influenzare l'indipendenza di operato di funzionari pubblici;
- nell'ambito della gestione del personale, compensi, *benefit*, premi devono essere attribuiti sulla base di criteri obiettivi, definiti previamente dalla Società e non allo scopo di consentire favoritismi di alcun genere; i rimborsi spesa sono effettuati solo per spese adeguatamente documentate e per costi effettivamente anticipati da UCA;
- il patrimonio immobiliare è gestito in ottemperanza alle direttive impartite dal C.d.A., nonché alle indicazioni del Presidente del C.d.A., elaborate in applicazione della Politica di Gestione del Patrimonio Immobiliare, alla quale il presente documento fa espresso rinvio, ovvero delle istruzioni ricevute dall'Ufficio *Property* (Area Amministrazione, Finanza e Controllo).

Chiunque venga a conoscenza di violazioni o presunte violazioni rilevanti ai fini della responsabilità

dell'Ente è tenuto ad informare, mediante apposita segnalazione, l'OdV.

5.13 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai reati contro la Pubblica Amministrazione (capitoli 4 e 5)

Di seguito sono riportate le procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai reati contro la P.A.

Tali procedure sono parte integrante del Modello e s'intendono integralmente richiamate:

- Politica sull'Informativa al Pubblico e Politica sulle Informazioni da Fornire all'IVASS
- Politica delle Informazioni Statistiche
- Procedura Segreteria Societaria
- Procedura Rapporti con le Autorità
- Procedura sui Processi e Responsabilità nelle procedure di Trasmissione dei Dati Anagrafici e Societari
- Procedura Ufficio Contratti
- Procedura Ufficio Gestione Tecnico – Legale
- Politica relativa al Sistema di Controllo Interno
- Procedura di Gestione del Personale
- Procedura di Gestione dei Processi e delle Procedure
- Procedura Comunicati Stampa
- Politica relativa alla Gestione dei Rischi
- Politica di Gestione del Rischio Operativo
- Politica relativa alla Funzione di Verifica di Conformità alle Norme
- Politica relativa alla Funzione di Revisione Interna
- Politica di Formazione dell'Organo Amministrativo, di Controllo e del Personale Rilevante
- Procedura di Gestione dei Progetti Rilevanti
- Politica di Esternalizzazione e Scelta dei Fornitori e sull'utilizzo dei Servizi ICT, compresi quelli a Supporto di Funzioni Essenziali o Importanti, prestati da Fornitori Terzi di Servizi ICT.

CAPITOLO 6 REATI SOCIETARI

6.1 Le fattispecie dei reati societari (art. 25 *ter* D. Lgs. 231/01)

Il D.Lgs. n. 61/2002 ha previsto l'inserimento nel D.Lgs. 231/01 di specifiche sanzioni a carico dell'Ente *"in relazione a reati in materia societaria previsti dal codice civile, se commessi nell'interesse della società da amministratori, direttori generali, liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si sarebbe realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica"*.

I reati societari possono qualificarsi come propri perché soggetti attivi possono essere solo *"amministratori, direttori generali, liquidatori o da persone sottoposte alla loro vigilanza"*. Tuttavia, l'art. 2639 c.c. equipara al soggetto formalmente investito della qualifica richiesta ai fini dell'integrazione della fattispecie di reato anche *"chi è tenuto a svolgere la stessa funzione, diversamente qualificata, sia chi esercita in modo continuativo e significativo i poteri tipici inerenti alla qualifica o alla funzione"*, pertanto anche tali soggetti potrebbero essere ritenuti responsabili dei reati in esame.

L'art. 25 *ter* del Decreto richiama i seguenti reati:

- false comunicazioni sociali (artt. 2621, 2621 *bis* c.c.);
- false comunicazioni sociali delle società quotate (art. 2622 c.c.);
- impedito controllo (art. 2625 c.c.);
- indebita restituzione dei conferimenti (art. 2626 c.c.);
- formazione fittizia del capitale (art. 2632 c.c.);
- illegale ripartizione degli utili o delle riserve (art. 2627 c.c.);
- illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- omessa comunicazione del conflitto di interesse (art. 2629 *bis* c.c.);
- indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- corruzione tra privati (art. 2635, comma 3, c.c.);
- istigazione alla corruzione tra privati (art. 2635 *bis* c.c.);
- illecita influenza sull'Assemblea (art. 2636 c.c.);

- aggiotaggio (art. 2637 c.c.);
- ostacolo all'esercizio delle funzioni delle Autorità pubbliche di Vigilanza (art. 2638, commi 1 e 2, c.c.);
- false o omesse dichiarazioni per il rilascio del certificato preliminare

(art. 54 D.Lgs. 19/23).

Si descrivono brevemente le sole fattispecie di reato di interesse per l'Ente.

6.2 False comunicazioni sociali (artt. 2621, 2621 *bis* c.c.)

La fattispecie si realizza attraverso l'esposizione consapevole nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero, idonei concretamente ad indurre in errore i destinatari sulla reale situazione economica, patrimoniale o finanziaria della società, con l'intenzione di ingannare i soci o il pubblico, ovvero attraverso l'omissione, con la stessa intenzione, di fatti materiali rilevanti sulla situazione medesima la cui comunicazione è imposta dalla legge. La comunicazione mendace o l'omissione rilevante dev'essere tale da indurre, in concreto, in errore i destinatari della stessa (il mercato, il pubblico, i soci, i creditori, ecc.).

La fattispecie di cui all'art. 2621 c.c. costituisce reato proprio, in quanto soggetti agenti possono essere l'organo amministrativo, i direttori preposti alla redazione dei documenti societari, i sindaci e i liquidatori.

Il Decreto richiama anche l'art. 2621 *bis* c.c. che punisce sempre il delitto di false comunicazioni sociali, ma in una forma più lieve, nel caso in cui i comportamenti posti in essere siano di lieve entità, in relazione alla natura e alle dimensioni della società, nonché delle modalità e degli effetti della condotta, ovvero qualora si tratti di società che non superano i limiti indicati dal secondo comma dell'art. 1 del Regio Decreto 16 marzo 1942, n. 267 (legge fallimentare).

Esempio

Redazione del bilancio con un attivo superiore rispetto alla situazione reale al fine di non far emergere una perdita che determinerebbe l'assunzione di provvedimenti sul capitale sociale.

6.3 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 legalmente attribuite ai soci, ad altri organi sociali. Anche questo, al pari delle false comunicazioni sociali, è reato proprio e soggetto attivo è l'organo amministrativo della società.

- Per quanto riguarda le attività di controllo il cui impedimento concretizza la fattispecie in esame, il riferimento è all'art. 2403 c.c., che nell'ambito dei controlli demandati ai sindaci individua, in generale, il controllo sul rispetto dei principi di corretta amministrazione, sull'osservanza della legge e dell'atto costitutivo, sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dall'Ente. Va considerato che, poiché i sindaci possono avvalersi di dipendenti ed ausiliari (art. 2403 *bis* c.c.), assume rilievo penale anche l'impedimento recato allo svolgimento delle funzioni demandate ad eventuali coadiutori.

La fattispecie a carico dell'ente, tuttavia, risulta integrata solo se dalla condotta derivi un danno ai soci.
Quanto all'elemento soggettivo del reato, l'illecito in esame postula la coscienza e volontà di impedire od ostacolare il controllo della gestione per effetto della condotta di occultamento (dolo generico) con la consapevolezza e la volontà di cagionare con tale condotta un danno ai soci (nella forma del dolo eventuale, essendo sufficiente in capo al soggetto attivo la rappresentazione della ragionevole possibilità di cagionare tale danno).

Esempio

L'amministratore che ponga in essere operazioni volte ad occultare documenti richiesti per lo svolgimento di attività di controllo da parte dei soci, ovvero che alteri fraudolentemente il contenuto dei libri contabili o dei verbali assembleari impedendo in tal guisa un controllo sugli stessi.

6.4 Indebita restituzione dei conferimenti (art. 2626 c.c.)

La fattispecie punisce gli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli. La fattispecie in esame sanziona una condotta idonea a determinare un pregiudizio per la società, risolvendosi in una forma di aggressione al capitale sociale, a vantaggio dei soci.

Esempio

Un amministratore restituisce a un socio l'importo del denaro che il socio aveva conferito alla società al momento della costituzione.

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

La fattispecie punisce l'organo amministrativo che ripartisce utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartisce riserve, anche non costituite con utili, che non possono per legge essere distribuite.

Esempio

Su proposta del C.d.A. avviene la distribuzione di utili che costituiscono fondi non distribuibili.

6.6 Operazioni in pregiudizio dei creditori (art. 2629 c.c.)

La fattispecie punisce l'organo amministrativo che, violando le disposizioni di legge a tutela dei creditori, effettua riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.

La norma tutela i creditori sociali assicurando l'effettività e l'integrità del capitale sociale in relazione ad alcune operazioni di finanza straordinaria. La condotta tipica si concretizza nell'effettuare operazioni sul capitale (fusione, scissione, riduzione) in violazione delle norme poste a tutela dei creditori.

Per la configurazione della fattispecie di reato è necessario che la condotta dell'organo amministrativo cagioni un danno ai creditori. Il reato si consuma al momento del verificarsi di tale danno. Il reato si estingue se prima del giudizio il danno cagionato viene risarcito.

Esempio

Esposizione di dati non veritieri nella situazione patrimoniale di fusione/scissione.

6.7 Omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.)

La fattispecie sanziona la condotta dell'amministratore o del 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 ai sensi dell'articolo 116 del T.U.F., ovvero di un soggetto sottoposto a vigilanza della Banca d'Italia, della Consob o dell'IVASS che viola gli obblighi previsti dall'articolo 2391, primo comma, c.c. se dalla violazione siano derivati danni alla società o a terzi. In particolare, l'art. 2391 c.c. stabilisce: per l'amministratore, l'obbligo di dare notizia agli altri membri del CdA e al collegio sindacale di ogni interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società; per l'amministratore delegato, l'obbligo di astenersi dal

compiere l'operazione in conflitto; per l'amministratore unico, l'obbligo di dare notizia dell'esistenza dell'interesse, oltre che al collegio sindacale, anche alla prima assemblea utile.
Perché si configuri il reato, tuttavia, non basta la mera violazione degli obblighi civilistici, occorrendo altresì che, da tale condotta, sia derivato un danno alla società o a terzi.

Esempio
Nella maggior parte dei casi, la Società è il soggetto danneggiato. Pertanto, un'ipotesi in cui anche l'Ente può esser chiamato a rispondere è quella in cui la condotta omissiva dell'amministratore abbia causato danni non alla propria Società, bensì a terzi che siano venuti in contatto e abbiano concluso con la Società rapporti giuridici.
Si pensi ad un componente del Consiglio di Amministrazione della Società X che risulti essere, al contempo, socio occulto della Società Y; in occasione dell'affidamento di una fornitura, la Società X, influenzata dall'amministratore che omette di comunicare agli altri membri dell'organo amministrativo il proprio interesse personale nell'operazione, decide di assegnare il contratto alla Società Y, anziché allo storico fornitore Z; quest'ultimo, pertanto, subisce un danno economico consistente nella perdita di un appalto che, in condizioni di trasparenza, avrebbe verosimilmente ottenuto.

6.8 Formazione fittizia del capitale (art. 2632 c.c.)
Si puniscono l'organo amministrativo e i soci conferenti che, anche in parte, formano o aumentano fittiziamente il capitale sociale mediante attribuzione di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravalutazione rilevante dei conferimenti di beni in natura o di crediti, ovvero del patrimonio della società nel caso di trasformazione.
Soggetti attivi sono l'organo amministrativo e i soci conferenti.
Tre sono le condotte che possono integrare il reato:

- la prima condotta consiste nell'attribuire azioni o quote sociali per una somma inferiore al loro valore nominale, in tal guisa creando titoli rappresentativi di un capitale inesistente;
- la seconda condotta è descritta come sottoscrizione reciproca di azioni o quote. Il requisito della reciprocità richiede l'esistenza di uno specifico accordo avente di mira lo scambio di azioni o quote; non si presuppone, invece, la contestualità o la connessione delle due

operazioni;

- la terza condotta concerne la sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società in caso di trasformazione.

In tutti e tre i casi il reato si consuma nel momento di effettiva formazione del capitale sociale, ossia, nel momento della formale dichiarazione, effettuata attraverso l'iscrizione nel registro delle imprese dell'atto costitutivo della società o degli atti che attestano l'effettuazione di un aumento di capitale.

Esempio

Il Presidente del C.d.A. espone dati non veritieri nella situazione patrimoniale relativa all'Ente, sopravvalutando i conferimenti in natura, così aumentando fittiziamente il capitale sociale.

6.9 Illecita influenza sull'Assemblea (art. 2636 c.c.)

La fattispecie si verifica quando un soggetto, con atti simulati o con frode, determina la maggioranza in Assemblea allo scopo di procurare a sé o ad altri un ingiusto profitto.

Esempio

L'organo amministrativo predispone documenti alterati al fine di ottenere una delibera autorizzativa favorevole per un'operazione dalla quale ricavare un indebito profitto.

6.10 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 ostacolare l'esercizio delle funzioni di vigilanza, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza;
- l'occultamento, in tutto o in parte, con altri mezzi fraudolenti, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima.

Esempio

L'organo amministrativo non comunica all'Autorità di Vigilanza una segnalazione prevista, così da eludere possibili controlli da parte dell'organismo medesimo.

6.11 Attività sensibili dell'Ente

Il rischio di incorrere nella commissione di uno dei reati societari sopra descritti si verifica, in particolare, nello svolgimento delle attività demandate all'Area Amministrazione, Finanza e Controllo dell'Ente. Trattasi delle attività aventi ad oggetto:

- la tenuta della contabilità generale (a mero titolo esemplificativo, chiusura registri IVA, controllo schede contabili, tenuta del registro delle attività a copertura delle riserve tecniche, del registro dei beni ammortizzabili), la redazione del bilancio di esercizio (a mero titolo esemplificativo, la predisposizione del bilancio di verifica, la predisposizione e l'invio dei dati al fiscalista per il calcolo delle imposte, la condivisione della documentazione con la società di revisione), la predisposizione delle comunicazioni relative alla situazione economica, patrimoniale e finanziaria della società e, più in generale, di qualunque documento giuridicamente rilevante nel quale si evidenzino elementi economici, patrimoniali e finanziari dell'azienda;
- le comunicazioni esterne: gestione di dati e notizie verso l'esterno relativi alla società (comunicazioni con il pubblico e con l'Autorità di Vigilanza);
- la gestione dei rapporti con gli organi sociali e con l'assemblea (a mero titolo esemplificativo, redazione dei verbali del Consiglio di Amministrazione e/o del Collegio Sindacale; gestione dei conflitti di interessi; flussi informativi agli organi sociali da parte dell'Area Amministrazione, Finanza e Controllo dell'Ente; convocazione e conduzione delle assemblee; presentazione di documentazione con dati rilevanti; svolgimento delle assemblee e verbalizzazione delle delibere);
- le operazioni sul capitale sociale;
- i conferimenti di beni/crediti;
- i processi di ristrutturazione o riorganizzazione aziendale;
- i rapporti con le Autorità di Vigilanza.

6.12 Comportamenti vietati ai destinatari del MOG

I destinatari del presente MOG devono astenersi dal porre in essere comportamenti tali da integrare una delle fattispecie di reato individuate dall'art. 25 *ter* del Decreto, ovvero dal porre in essere comportamenti che, sebbene non siano così gravi da costituire una delle fattispecie di reato

anzidette, possono potenzialmente diventarlo.

Nello specifico, è fatto divieto di:

- predisporre o comunicare dati non veritieri sulla situazione economico-patrimoniale della società;
- omettere di comunicare dati la cui trasmissione è imposta dalla normativa in vigore;
- alterare o comunque inserire dati non veritieri nel bilancio societario e nelle altre comunicazioni sociali;
- occultare documenti al fine di impedire lo svolgimento delle attività di controllo;
- trasmettere comunicazioni non veritiere alle Autorità di Vigilanza;
- occultare, in tutto o in parte la comunicazione di fatti alle Autorità di Vigilanza;
- comunicare agli organi sociali informazioni o dati incompleti o mendaci.

6.13 Principi specifici per le procedure

UCA assicura la tracciabilità di tutte le operazioni eseguite e la documentazione di qualunque operazione rilevante ai fini della redazione del bilancio.

Nella gestione di tutte le operazioni sociali, i destinatari sono tenuti ad osservare le prescrizioni contenute nel Codice Etico e, quindi, sono tenuti ad osservare le regole di corretta, completa e trasparente contabilizzazione nel rispetto dei criteri normativi e dei principi contabili adottati da UCA, assicurando il rispetto del principio dell'integrità nella tenuta della contabilità.

Ulteriormente, ai destinatari è richiesto di:

- predisporre e redigere tutta la documentazione societaria in modo chiaro, completo, preciso e veritiero, nel rispetto delle previsioni civilistiche e delle procedure amministrative e contabili adottate da UCA; a tal fine, per consentire la corretta predisposizione del bilancio e di ogni altra comunicazione di carattere economico o finanziario, ciascuna funzione o unità organizzativa deve collaborare al processo trasmettendo alla funzione responsabile, nel rispetto della tempistica prevista, i dati e le notizie richiesti;
- operare, nei rapporti con gli organi sociali, con trasparenza, correttezza e lealtà;
- fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;
- la valutazione degli immobili di proprietà della Compagnia avviene in conformità a quanto previsto dalla Procedura Valutazione Immobili che disciplina la nomina dell'Esperto Indipendente per la

valutazione, la fase di valutazione e la verifica della stessa; in particolare, la Compagnia verifica l'idoneità della valutazione a rappresentare in modo coerente e completo le modalità di formazione dei valori degli immobili e degli altri beni oggetto di stima, nonché il rispetto dei principi valutativi sanciti dalle Politiche della Compagnia e dalla normativa vigente;

- 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;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate; la documentazione da inviare e le comunicazioni da effettuare alle Autorità di Vigilanza devono essere predisposte dalle Funzioni competenti in materia; in ogni caso, prima di procedere alla trasmissione all'Autorità di Vigilanza è necessario effettuare un controllo circa la completezza e correttezza del materiale raccolto e predisposto per l'invio; nel caso in cui la documentazione da trasmettere alle Autorità di Vigilanza sia prodotta – in tutto o in parte – con il supporto di soggetti terzi (consulenti, periti, tecnici, …), questi ultimi dovranno essere selezionati in base ai requisiti di professionalità, indipendenza, competenza; tutta la documentazione prodotta o consegnata alle Autorità di Vigilanza dev'essere conservata al fine di assicurare la tracciabilità delle attività;
- osservare la Procedura sui Flussi Informativi all'Alta Direzione, al fine di garantire la ricezione da parte della stessa delle informazioni relative alle diverse attività svolte dalle Aree / Uffici, assicurando la trasparenza della gestione dell'impresa e le condizioni per un'efficace ed effettiva azione di indirizzo e controllo sull'attività della Società e sull'esercizio dell'Impresa da parte dell'Alta Direzione.

L'OdV deve essere tempestivamente informato dell'inizio delle operazioni ispettive e deve conservare copia dei verbali delle ispezioni.

6.14 Reato di corruzione tra privati (art. 25 *ter*, comma 1, lett. S-*bis*, D. Lgs. 231/01)

Il reato di corruzione tra privati è stato introdotto nel novero dei reati presupposto dalla L. n. 190/12, che ha modificato l'art. 2635 c.c., ed è stato successivamente modificato dal D.Lgs. 38/17.

L'art. 2635 c.c. è una fattispecie residuale che punisce, 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, che sollecitano, ricevono o accettano la promessa di denaro o altra utilità non dovuti, per sé o per altri, per compiere od omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.

Il fatto può essere commesso anche da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

La norma punisce anche il corruttore che dà o promette denaro o altra utilità alle persone anzidette.

L'art. 25 *ter*, comma 1, lett. S-*bis* del D.Lgs. 231/01 richiama solo il terzo comma dell'art. 2635 c.c. che punisce il soggetto che dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma, quindi, il corruttore. Affinché sorga una responsabilità in capo all'Ente è necessario che dalla condotta derivi, da un lato, un qualche vantaggio per il medesimo e, dall'altro, un nocumento nei confronti della società di appartenenza del corrotto.

Esempio

Un componente del Consiglio di Amministrazione promette denaro o altra utilità ad un esponente di altro Ente al fine di avvantaggiare l'Ente per il quale lavora.

6.15 Attività sensibili di UCA

Il reato sopra descritto è solo astrattamente ipotizzabile in capo all'Ente.

Tuttavia, devono essere segnalate alcune attività sensibili che potrebbero porsi come attività strumentali o propedeutiche al reato di corruzione tra privati. Si tratta delle seguenti attività:

- acquisti di beni o servizi;
- selezione ed assunzione del personale;
- gestione omaggistica ed erogazioni liberali;
- partecipazione a gare di appalto: tale attività rileva in relazione alla partecipazione a gare d'appalto indette da privati, nelle quali è possibile immaginare la corruzione dell'amministratore di una società concorrente affinché accetti di ritirare la candidatura;
- la negoziazione e la gestione di contratti attivi con società, consorzi, fondazioni associazioni e altri enti privati, anche privi di personalità giuridica, che svolgono attività professionale e di impresa, dal cui mancato svolgimento possa derivare un vantaggio per la società o per le quali la stessa possa avere un interesse (per esempio, analisti finanziari, *mass media*, agenzie di *rating*, organismi di certificazione e di valutazione di conformità, etc.);
- la gestione dei flussi finanziari;

- la liquidazione dei sinistri.

6.16 Comportamenti vietati ai destinatari del MOG

I destinatari del Modello devono astenersi dal porre in essere comportamenti tali da integrare la fattispecie di reato individuata dall'art. 25 *ter* comma 1, lett. S-*bis* del Decreto, ovvero dal porre in essere comportamenti che, sebbene non siano così gravi da costituire la fattispecie di reato anzidetta, possono potenzialmente diventarlo.

Nello specifico si richiede al personale di osservare i seguenti divieti:

- non adottare comportamenti che vengano meno agli obblighi di fedeltà verso l'Ente;
- non adottare comportamenti (che si traducono in promesse di danaro o altra utilità) che possano indurre terzi a compiere atti a vantaggio dell'Ente ma a danno della società per cui lavorano o che rappresentano.

In generale, ciò che si richiede ai dipendenti e ai collaboratori è di perseguire la *mission* aziendale mediante comportamenti eticamente corretti e leali nei confronti di tutti i soggetti con i quali si intrattengono rapporti commerciali.

6.17 Principi specifici per le procedure

Relativamente alle attività sensibili identificate si invitano i destinatari del presente Modello al rispetto dei principi sanciti nel Codice Etico e, ulteriormente, si individuano i seguenti principi/procedure:

- l'Ente verifica l'attendibilità e l'onorabilità personale dei dipendenti e dei collaboratori prima della sottoscrizione del rapporto di lavoro e in costanza di rapporto, attraverso la richiesta di produzione del certificato dei carichi pendenti/di una autocertificazione resa ai sensi del D.P.R. 445/00 al momento dell'assunzione, ovvero dell'avvio della collaborazione e, successivamente, in caso di variazioni che il dipendente o collaboratore sarà tenuto a comunicare tempestivamente, attraverso il rilascio di un'autodichiarazione;
- i dipendenti e i collaboratori sono tenuti a segnalare tempestivamente ai superiori e all'Organismo di Vigilanza aziendale ogni richiesta di denaro o di regali non giustificata dai normali rapporti amministrativi, ricevuta da soggetti appartenenti ad altre aziende, ovvero sono tenuti a segnalare ogni omaggio o utilità ricevuta che non sia di modico valore e che sia tale da indurre a tenere comportamenti in contrasto con gli interessi dell'Ente;
- nella conduzione di qualsiasi trattativa, sono evitate situazioni nelle quali i soggetti coinvolti siano

o possano apparire in conflitto di interesse;

- in conformità a quanto previsto dalla Procedura Ufficio Contratti, occorre garantire evidenza documentale e la corretta archiviazione degli ordini di acquisto o di altri documenti (contratti, accordi) sulla base dei quali vengono effettuati gli acquisti di beni e servizi; delle comunicazioni inoltrate ai fornitori a seguito di problemi e/o inefficienze riscontrate in fase di approvvigionamento (relative a tematiche di qualità, quantità, tempistiche di approvvigionamento difformi dalle condizioni contrattuali, ecc.); di autorizzazioni a eventuali deroghe alle condizioni standard concesse ai fornitori (rispetto agli ordinari termini di pagamento o alla concessione di anticipi);
- è vietato effettuare prestazioni o pagamenti in favore di fornitori/professionisti/consulenti che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- sulle fatture passive emesse da fornitori/professionisti/consulenti viene svolto un controllo e viene verificata la congruità rispetto all'ordine di acquisto;
- i pagamenti ai professionisti/consulenti/fornitori devono essere effettuati sul conto intestato agli stessi e mai su conti cifrati, o in contanti, o in favore di un soggetto diverso.

6.18 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai reati societari

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai reati contro la P.A.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Politica per la Valutazione delle Attività e delle Passività diverse dalle riserve tecniche
- Politica di Gestione delle Attività e delle Passività
- Politica di Gestione del Capitale
- Procedura Asset And Liability Management
- Politica di Gestione del Patrimonio Immobiliare
- Procedura di Valutazione degli Immobili
- Procedura Ufficio Contenzioso
- Politica di Operatività Infragruppo
- Politica sui Conflitti di Interesse

- Politica di Remunerazione e Incentivazione degli Amministratori, Organi di Controllo, Personale Rilevante, Funzioni Fondamentali ed Altri Dipendenti
- Politica di Remunerazione e Incentivazione degli Intermediari Assicurativi
- Politica relativa al Sistema di Controllo Interno
- Procedura Segreteria Societaria
- Procedura sui Flussi Informativi verso l'Alta Direzione
- Politica sulle Informazioni Statistiche
- Procedura Rapporti con le Autorità
- Procedura Ufficio Gestione Tecnico – Legale
- Politica di Esternalizzazione e Scelta dei Fornitori e sull'utilizzo dei Servizi ICT, compresi quelli a Supporto di Funzioni Essenziali o Importanti, prestati da Fornitori Terzi di Servizi ICT
- Procedura Gara di Produzione
- Procedura di Gestione del Personale
- Procedura Ufficio Contratti
- Procedura di Gestione dei Processi e delle Procedure
- Politica relativa alla Funzione di Verifica di Conformità alle Norme
- Politica relativa alla Funzione di Revisione Interna
- Politica relativa alla Funzione Attuariale.

CAPITOLO 7 REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO. DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E TRASFERIMENTO FRAUDOLENTO DI VALORI (ARTT. 25 OCTIES, 25 OCTIES- 1 D.LGS. 231/01)

7.1 Le fattispecie dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

I reati di riciclaggio sono stati introdotti nel D.Lgs. 231/01, all'art. 25 *octies*, attraverso il richiamo al D.Lgs. 231/07 (c.d. Decreto Antiriciclaggio).

Si tratta delle seguenti fattispecie di reato:

- ricettazione;
- riciclaggio;
- impiego di denaro, beni o utilità di provenienza illecita;
- autoriciclaggio.

7.2 Ricettazione (art. 648 c.p.)

Punisce il soggetto che fuori dei casi di concorso nel reato (art. 110 c.p.), al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi reato, o comunque si intromette nel farli acquistare, ricevere od occultare.

Vanno considerate tutte le singole tipologie di condotte incluse nel concetto di ricettazione, intendendosi:

- per acquisto: il conseguimento del possesso del bene proveniente da reato, anche se solo temporaneo, avvenuto a seguito di un'attività negoziale, onerosa o a titolo gratuito;
- per ricezione: ogni forma di conseguimento del possesso del bene proveniente da reato;
- per occultamento: l'attività preordinata a nascondere il bene ricevuto e proveniente da reato.

La condizione sufficiente a configurare la ricettazione è la consapevolezza da parte del soggetto attivo della provenienza delittuosa del bene. Le cose oggetto delle condotte punite dall'art. 648 c.p. possono avere una provenienza illecita tanto immediata quanto mediata, non reputandosi, cioè, necessario che la cosa acquistata, ricevuta od occultata costituisca il diretto ed immediato provento del reato principale, ben potendo essa giungere al soggetto attivo anche attraverso una catena di intermediari.

Esempio

Un componente del Consiglio di Amministrazione autorizza l'acquisto di arredi che sa provenire da attività illecita, pagandoli ad un prezzo inferiore rispetto al loro valore di mercato.

7.3 Riciclaggio (art. 648 *bis* c.p.)

La condotta si verifica quando, fuori dei casi di concorso nel reato, un soggetto sostituisce o trasferisce denaro, beni o altre utilità provenienti da reato, ovvero compie in relazione ad essi altre operazioni in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Anche il reato di riciclaggio può configurarsi attraverso la realizzazione di diverse condotte:

- di sostituzione, ovvero di scambio del denaro, dei beni o delle altre utilità di provenienza illecita con valori diversi; si pensi, ad esempio, al cambio di denaro contante con altre banconote, finalizzato a "ripulire" il provento illecito, per separarlo da ogni possibile collegamento con il reato;
- di trasferimento, ovvero di spostamento del denaro, dei beni o delle altre utilità di provenienza illecita attraverso attività negoziali; si pensi, ad esempio, allo spostamento di valori illeciti da un luogo ad un altro, come in un conto estero;
- altre operazioni atte ad ostacolare l'identificazione della provenienza delittuosa del denaro, dei beni o delle altre utilità; il legislatore, infine, per evitare vuoti di tutela, ha introdotto una formula di chiusura ("*altre operazioni*") idonea a ricomprendere nel reato tutte le nuove tecniche di riciclaggio.

Affinché si configuri il reato disciplinato dall'art. 648 *bis* c.p. è necessario che il soggetto agente ponga in essere un *quid pluris* rispetto alla condotta di ricettazione, ovvero il compimento di atti o fatti diretti alla sostituzione del denaro di provenienza delittuosa.

Esempio

L'ufficio Assunzione Rischi, omettendo i controlli richiesti dalla normativa antiriciclaggio sull'obbligo di adeguata verifica della clientela (D. Lgs. 231/07), stipula una serie di polizze assicurative con soggetti coinvolti in traffici illeciti, consentendo ai contraenti di ripulire il denaro ottenuto dall'attività illecita.

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

La disposizione in commento punisce il soggetto che, fuori dei casi di concorso nel reato e dei casi

previsti dagli articoli 648 e 648 *bis* c.p., impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

Si tratta di una norma residuale volta a punire solo coloro i quali non sono già compartecipi nel reato principale o non sono già imputabili per ricettazione o riciclaggio. Il legislatore ha voluto così sanzionare l'"anello terminale" dell'attività illecita, sfociante nell'investimento produttivo (in attività economiche o finanziarie) dei proventi illeciti.

Esempio

L'Ufficio Contenzioso riceve consapevolmente in pagamento denaro di provenienza illecita da parte di un cliente che ha già provveduto autonomamente alla sua sostituzione e lo investe in attività economiche o finanziarie.

7.5 Autoriciclaggio (art. 648 ter 1 c.p.)[7]

Il reato di autoriciclaggio è stato introdotto nel codice penale dalla L. n. 186/2014 ed è stato inserito tra i reati presupposto della responsabilità amministrativa degli Enti ai sensi del D.Lgs. n. 231/01 (art. 25 *octies*).

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

L'autoriciclaggio consiste nell'attività di occultamento dei proventi derivanti da crimini propri e si riscontra soprattutto a seguito di particolari reati, quali l'evasione fiscale, la corruzione e l'appropriazione di beni sociali.

Tuttavia non è sufficiente un arricchimento dal reato base, con conseguente reimpiego per ricadere nella fattispecie di cui all'art. 648 *ter* 1 c.p.; devono essere messe in atto azioni volte ad ostacolare concretamente l'identificazione della provenienza delittuosa del denaro.

Le condotte attraverso le quali si commette il reato di autoriciclaggio sono:

- l'impiego: vale a dire la re-immissione in qualsiasi forma, in un'attività economica o finanziaria, del denaro, dei beni o delle altre utilità provenienti dalla commissione del delitto;

[7] È stato introdotto con l'art. 3 della L. 15.12.2014, n. 186, pubblicata in G.U. n. 292 del 17.12.2014.

- la sostituzione: intesa come qualsiasi mutazione del bene o dell'utilità illecita in altro bene/utilità, tesa ad ostacolare l'individuazione della provenienza illecita del primo;
- il trasferimento: lo spostamento del bene o dell'utilità illecita.

In linea con quanto fino ad ora detto si ricorda la causa di esclusione della punibilità prevista dall'art. 648 *ter* 1, comma quarto, c.p., che si verifica quando, attraverso le condotte poste in essere, il denaro, i beni e le altre utilità vengono destinate alla mera utilizzazione o al godimento personale (ad esempio, non sarebbe punibile a titolo di autoriciclaggio l'amministratore che, ricevuta un'utilità non dovuta per compiere un atto in violazione degli obblighi del proprio ufficio, la utilizzi per andare a fare la spesa al supermercato).

Il problema che si pone con riferimento alla fattispecie dell'autoriciclaggio riguarda la determinazione del reato presupposto, ovvero se la ricerca di questo debba essere limitata ai soli reati tassativamente indicati dal D.Lgs. 231/01 o, piuttosto, possa trattarsi di qualsiasi reato. Sul punto vi sono diversi orientamenti: un primo filone sostiene la prima teoria, ovvero che i reati presupposto dell'autoriciclaggio possano essere solo quelli già ricompresi nel D.Lgs. 231/01[8]. Secondo un diverso pensiero, invece, non vi sarebbe limite alla determinazione dei reati presupposto dell'autoriciclaggio, in quanto l'art. 25 *octies* non individua alcuna restrizione[9]. Sul punto la giurisprudenza non è ancora intervenuta per fare chiarezza. Privilegiando l'ultima tesi, se da un lato è vero che viene rafforzata la funzione di strumento di prevenzione del MOG, dall'altro va preso atto della completa vanificazione del principio di tassatività dei reati previsto dal Decreto.

Volendo assumere una posizione intermedia, rispettosa sia del principio di tassatività che dell'esigenza di prevenzione, va preso atto dell'esistenza di una classe di reati espressamente richiamati all'art. 25 *quaterdecies* del Decreto che molto spesso costituiscono il reato presupposto dell'autoriciclaggio; si tratta dei reati tributari, disciplinati dal D.Lgs. 74/2000 e di seguito elencati:

- la dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
- la dichiarazione fraudolenta mediante artifici;
- la dichiarazione infedele;
- l'omessa dichiarazione;
- l'emissione di fatture o di altri documenti per operazioni inesistenti;

[8] In questa direzione si veda la Circolare di Confindustria, n. 19867 del 12.06.2015.
[9] In questo senso pare essersi orientata l'Associazione Bancaria Italiana (ABI), con Circolare 1.12.2015, n. 6.

- l'occultamento e la distruzione di documenti contabili;
- l'omesso versamento di ritenute dovute o certificate;
- l'omesso versamento di IVA;
- l'indebita compensazione;
- la sottrazione fraudolenta al pagamento di imposte.

Esempio

Utilizzo dei proventi ottenuti dalla commissione di un reato tributario per creare dei fondi neri su un conto corrente aperto all'estero, così da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

7.6 Le fattispecie di delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori

L'art. 3 del D.lgs.184/2021, introducendo nel Decreto 231 l'art. 25-*octies*.1, ha esteso la responsabilità amministrativa degli enti ai delitti in materia di strumenti di pagamento diversi dai contanti, strettamente collegati ai reati di riciclaggio di cui all'art. 25-*octies*.

Si tratta delle seguenti fattispecie di reato:

- indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti;
- detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti;
- frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale;
- trasferimento fraudolento di valori.

Si descrivono brevemente le fattispecie di reato di interesse per l'Ente.

7.7 Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.)

La fattispecie si realizza quando un soggetto, 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. La fattispecie si realizza altresì quando un soggetto, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i

documenti sopra citati, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

7.8 Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.)

La fattispecie punisce chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. La pena è aumentata se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.

Esempio

Un dirigente della Compagnia, con accesso ai sistemi interni, manipola il *software* di gestione dei sinistri inserendo dati falsi sui sinistri per far risultare un aumento del rischio, con conseguente incremento dei premi delle polizze.

7.9 Trasferimento fraudolento di valori (art. 512-bis c.p.)

La fattispecie sanziona chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero al fine di agevolare la commissione dei delitti di ricettazione (art. 648 c.p.) o riciclaggio (art. 648-bis c.p.) o impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.). La disposizione punisce altresì chi, al fine di eludere le disposizioni in materia di documentazione antimafia, attribuisce fittiziamente ad altri la titolarità di imprese, quote societarie o azioni ovvero di cariche sociali, qualora l'imprenditore o la società partecipi a procedure di aggiudicazione o di esecuzione di appalti o di concessioni.

Con tale norma il legislatore ha inteso sanzionare l'attività finale della commissione di illeciti di natura patrimoniale, concretantesi nell'investimento produttivo dei proventi illeciti. Si rappresenta tuttavia che la fattispecie in esame trova applicazione solo se il fatto non costituisce un reato più grave; pertanto, stante la clausola di sussidiarietà, l’art. 512-bis c.p. appare destinata ad avere uno spazio applicativo piuttosto ristretto, riservato alle sole condotte di impiego di proventi illeciti realizzato tramite operazioni non idonee ad ostacolare l'identificazione della provenienza illecita.

Si rappresenta tuttavia che, per la giurisprudenza di legittimità dominante[10], il reato in parola – la cui condotta consiste precipuamente nell'intestare intestare fittiziamente un bene a un prestanome – integra un illecito distinto rispetto ai reati in materia di riciclaggio, potendo dunque concorrere con tali reati; ciò in quanto le operazioni di intestazione fittizia non rappresentano solo un passaggio intermedio del riciclaggio, bensì integrano una fattispecie autonoma che agevola la successiva ripulitura del denaro "sporco".

Esempio

L'amministratore delegato – agendo quale intermediario di un membro di un'organizzazione criminale dedita ad attività di evasione fiscale e riciclaggio – in cambio di investimenti e apporti finanziari diretti alla propria Società – pone in essere una serie di operazioni volte a schermare la reale proprietà di capitali di provenienza delittuosa (trasferendo fittiziamente la proprietà di alcuni immobili ai propri familiari).

7.10 Attività sensibili di UCA

Il rischio che i destinatari del Modello commettano uno dei reati appena descritti è in linea di principio maggiore nello svolgimento delle seguenti attività:

- rapporti con i fornitori;
- attività di sponsorizzazione;
- gestione dei flussi finanziari;
- in relazione alla condanna per il reato di autoriciclaggio, costituiscono attività sensibili dell'Ente tutte le attività per le quali l'Ente risulta esposto alla commissione degli illeciti di cui al Decreto, che possono costituire il reato presupposto della fattispecie dell'autoriciclaggio;
- gestione di carte di credito e di tutti gli altri mezzi di pagamento diversi dal contante;
- utilizzo di strumenti informatici e telematici.

7.11 Comportamenti vietati ai destinatari del MOG

I destinatari del Modello devono astenersi dal porre in essere comportamenti tali da integrare una delle fattispecie di reato individuate dagli artt. 25 *octies* e 25 *octies.1* del Decreto, ovvero dal porre in

[10] In tal senso, Cass Pen., Sez. II, n. 23440/2025.

essere comportamenti che, sebbene non siano così gravi da costituire una delle fattispecie di reato anzidette, possono potenzialmente diventarlo.

Nello svolgimento delle attività sensibili i destinatari del presente documento:

- non accettano dai fornitori o da soggetti a loro collegati, omaggi o utilità in genere; nei casi in cui si rendano necessarie eccezioni, è fatto comunque divieto ai destinatari di accettare omaggi ed utilità che, in ragione della natura o del valore, possano indurre a tenere comportamenti in contrasto con gli interessi degli altri fornitori. Gli omaggi e le utilità ricevute, aventi caratteristiche in contrasto con i principi di cui sopra, verranno devolute a fini di beneficenza o utilità sociale. Nei casi critici, il destinatario deve darne tempestiva notizia all'OdV. Il medesimo principio viene applicato anche nei confronti dei fornitori gestiti in *outsourcing*;
- non stringono relazioni commerciali con soggetti di nota o sospetta appartenenza o riconducibilità ad organizzazioni criminali;
- selezionano i fornitori e/o professionisti solo in presenza di caratteristiche di sicura affidabilità, correttezza e onestà;
- non utilizzano strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
- garantiscono la tracciabilità e la trasparenza dei flussi finanziari;
- utilizzano carte di credito e altri mezzi di pagamento elettronici di titolarità aziendale solo previa specifica autorizzazione e soltanto in conformità alle istruzioni e direttive eventualmente ricevute;
- non accedono abusivamente a sistemi informatici e telematici, banche dati o software, né intervengono sui sistemi stessi senza diritto;
- utilizzano la connessione Internet solo per gli scopi e il tempo strettamente necessario per

l'espletamento delle proprie mansioni o incarichi;

- compiere qualsiasi operazione negoziale di natura apparente o fittizia (a titolo esemplificativo, operazioni straordinarie, trasferimento di quote/azioni, attribuzione di cariche amministrative, trasferimento di denaro, beni o proprietà immobiliari, ecc.), qualsiasi sia la finalità perseguita;
- non pongono in essere o agevolano operazioni o attività che non siano rispettose delle norme del Codice Etico.

7.12 Principi specifici per le procedure

Ai destinatari del Modello è richiesto, in linea con quanto sancito dal Codice Etico, di mantenere una condotta improntata ai principi di onestà e correttezza, agendo con trasparenza e buona fede nello svolgimento delle proprie attività.

I destinatari sono tenuti a rispettare tutte le norme e disposizioni, sia nazionali che internazionali, in tema di antiriciclaggio ed antiterrorismo.

Il presente documento individua i seguenti principi/procedure da rispettare al fine di eliminare il rischio per l'Ente di incorrere in uno dei reati considerati nei superiori paragrafi:

- i flussi di denaro in entrata e in uscita sono costantemente monitorati. In particolare, l'Ente accerta che tutti gli incassi e tutti i pagamenti siano correlati ad attività poste in essere per il raggiungimento della missione sociale. L'Ente, attraverso l'Ufficio Contabilità Agenzie, garantisce un puntuale controllo contabile anche sulla rete commerciale, mediante quadratura analitica delle singole agenzie, controlli delle rimesse non pervenute alla Compagnia e verifica dell'emissione del sollecito, nonché della segnalazione all'ispettore di zona, verifica degli incassi sul gestionale PassCompagnia;
- i dipendenti addetti alle relazioni con i fornitori devono procedere alla selezione dei medesimi nell'osservanza dei requisiti di qualità, prezzo, convenienza, capacità ed efficienza, o altri purché predefiniti e valutabili in termini oggettivi, imparziali e trasparenti, evitando qualunque logica motivata da favoritismi o dettata dalla certezza o dalla speranza di ottenere vantaggi, anche con riferimento a situazioni estranee al rapporto di fornitura, per sé o per l'Ente;
- l'Ufficio Contratti sottopone periodicamente a revisione l'elenco dei fornitori;
- l'Ufficio Amministrazione e Gestione Reti effettua una serie di controlli preventivi atti a verificare l'onorabilità degli intermediari (Agenzie, Broker e Banche) da inserire nella rete

- commerciale della Compagnia; in particolare, preliminarmente all'apertura di nuova collaborazione, l'Ufficio Amministrazione e Gestione Reti verifica l'esistenza dell'iscrizione dell'Intermediario al RUI e l'operatività dell'intermediario; richiede il casellario giudiziale o, in alternativa, il rilascio di autocertificazione ai sensi dell'art. 47 D.P.R. 445/2000 attestante l'onorabilità, professionalità e l'assenza di condanne penali in capo all'intermediario;l'Area Amministrazione, Finanza e Controllo verifica mensilmente l'andamento degli investimenti e del rispetto dei limiti connessi agli investimenti, attraverso la produzione di report riepilogativi che vengono trasmessi al Responsabile dell'Area Amministrazione, Finanza e Controllo e all'Alta Direzione. Con riferimento agli investimenti immobiliari, l'Area Amministrazione, Finanza e Controllo concorderà con un Esperto Indipendente, selezionato e nominato dal C.d.A., la documentazione necessaria per l'attività di valutazione, provvedendo ad archiviare tutto il flusso documentale intervenuto, sì da garantire la tracciabilità del processo. L'Esperto Indipendente procederà alla redazione della Relazione di stima del patrimonio immobiliare nei tempi definiti, in coerenza con la normativa applicabile.

7.13 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai reati in materia di riciclaggio, in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai reati in materia di riciclaggio, di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Politica per la Valutazione delle Attività e delle Passività diverse dalle riserve tecniche
- Politica di Gestione delle Attività e delle Passività
- Politica di Gestione del Capitale
- Procedura Asset And Liability Management
- Procedura Ufficio Antifrode
- Politica degli Investimenti
- Politica di Gestione del Patrimonio Immobiliare
- Procedura di Valutazione degli Immobili

- Procedura Ufficio Contenzioso
- Politica di Operatività Infragruppo
- Politica relativa al Sistema di Controllo Interno
- Procedura Ufficio Gestione Tecnico – Legale
- Politica di Esternalizzazione e Scelta dei Fornitori e sull'utilizzo dei Servizi ICT, compresi quelli a Supporto di Funzioni Essenziali o Importanti, prestati da Fornitori Terzi di Servizi ICT
- Procedura di Gestione del Personale
- Procedura di Gestione dei Processi e delle Procedure
- Politica relativa alla Funzione di Verifica di Conformità alle Norme
- Politica relativa alla Funzione di Revisione Interna
- Politica relativa alla Funzione Attuariale
- Procedura sui Flussi Informativi verso l'Alta Direzione
- Politica di Gestione degli Accessi
- Procedura per la Gestione delle Identità e dei Diritti di Accesso Fisici e Logici
- Politica di Gestione delle Identità.

CAPITOLO 8 REATI DI OMICIDIO COLPOSO E LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E DELLA SICUREZZA SUL LAVORO

8.1 Le fattispecie di reato di omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro (art. 25 *septies* D. Lgs. 231/01)

L'articolo 9 della L. 3 agosto 2007 n. 123, poi sostituito dall'art. 300 del D.Lgs. 9 aprile 2008 n. 81, ha introdotto nel Decreto l'art. 25 *septies*, inserendo nel novero dei reati presupposto le fattispecie di omicidio colposo (art. 589 c.p.) e di lesioni personali colpose (art. 590 c.p.) avvenuti in violazione delle norme in materia di tutela della salute e della sicurezza sul lavoro.

Il Testo Unico sulla Salute e Sicurezza sul Lavoro è contenuto nel D.Lgs. 81/08, coordinato con il D.Lgs. 106/09.

Il datore di lavoro è destinatario di uno specifico obbligo legale di garanzia, in virtù del quale deve adottare tutte le cautele necessarie ad assicurare la sicurezza dei lavoratori e, in generale, di tutti coloro che si trovano in una situazione analoga ai medesimi e che sono presenti sul luogo di lavoro per qualsiasi ragione, purché a questo connessa (ad esempio stagisti).

La responsabilità dell'Ente non consegue ad una colpa "generica" (vale a dire per imprudenza, imperizia, negligenza), bensì ad una colpa "specifica": l'inosservanza delle norme per la prevenzione degli infortuni sul lavoro.

Il Testo Unico sulla Salute e Sicurezza sul Lavoro all'art. 30, comma 1, prevede:

- il rispetto degli standard tecnico-strutturali di legge previsti per attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- lo svolgimento dell'attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- l'attività di sorveglianza sanitaria;
- l'attività di informazione e formazione dei lavoratori;
- l'attività di vigilanza sul rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- l'acquisizione di documentazione e certificazioni obbligatorie di legge;
- le verifiche periodiche dell'applicazione e dell'efficacia delle procedure adottate.

L'art. 30 del D.Lgs. 81/08 prevede l'adozione di un Modello di Organizzazione e Gestione (il MOG di cui al D.Lgs. 231/01) che venga efficacemente attuato al fine di assicurare il corretto adempimento di tutti gli obblighi imposti dal Testo Unico sulla Salute e Sicurezza sul Lavoro.

Inoltre, a mente del Testo Unico richiamato, il MOG *"deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1. Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello. Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico"*[11].

L'art. 25 *septies* del Decreto richiama quindi i seguenti reati:

- omicidio colposo,
- lesioni personali colpose gravi o gravissime

dettagliati nel prosieguo.

8.2 Omicidio colposo (art. 589 c.p.)

La fattispecie delittuosa in esame si configura quando, a causa della mancata osservanza delle norme antinfortunistiche e di quelle sulla tutela dell'igiene e della salute sul lavoro, si verifica la morte di un lavoratore, ovvero quando ciò accade per la mancata adozione di tali accorgimenti e misure.

Il datore di lavoro è sempre responsabile dell'infortunio occorso al lavoratore, sia quando ometta di apportare idonee misure protettive, sia quando non accerti e vigili che di queste misure il dipendente faccia effettivamente uso.

8.3 Lesioni personali colpose gravi o gravissime (art. 590, comma 3 c.p.)

La fattispecie si verifica quando un soggetto, violando le norme per la prevenzione degli infortuni sul lavoro, cagiona ad altro soggetto lesioni gravi o gravissime.

[11] D.Lgs. n. 81/08, art. 30, commi 2, 3 e 4.

Ai sensi dell'art. 583 c.p., la lesione personale è grave:

a) se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;
b) se il fatto produce l'indebolimento permanente di un senso o di un organo.

La lesione personale è gravissima se dal fatto deriva:

a) una malattia certamente o probabilmente insanabile;
b) la perdita di un senso;
c) la perdita di un arto o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella.

8.4 Attività sensibili di UCA

La Compagnia eleva la tutela della salute e della sicurezza dei propri collaboratori e dipendenti a valore fondamentale attraverso il rispetto puntuale delle disposizioni di cui al D.Lgs. 81/08.

In questo senso l'Ente si è dotato del Documento di Valutazione dei Rischi (DVR), che aggiorna periodicamente e ha definito i ruoli e provveduto alle nomine delle figure coinvolte nella sicurezza aziendale.

Posta questa premessa, si possono individuare le seguenti attività sensibili:

- valutazione dei rischi;
- sorveglianza sanitaria;
- affidamento di lavori a terzi all'interno dei locali aziendali;
- gestione delle emergenze;
- formazione/informazione del personale.

8.5 Comportamenti vietati ai destinatari del MOG

I destinatari del MOG devono astenersi dal porre in essere comportamenti tali da integrare una delle fattispecie di reato individuate dall'art. 25 *septies* del Decreto, ovvero dal porre in essere comportamenti che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle descritte nel presente capitolo.

8.6 Principi specifici per le procedure

L'Ente ha attribuito al Consigliere Delegato, Alfredo Penna, i poteri e i doveri del "datore di lavoro" e del "committente" nelle materie afferenti la tutela dell'ambiente, la sicurezza e l'igiene del lavoro e la prevenzione incendi, ai sensi del D.Lgs. 81/08, il quale ha provveduto a dare corso agli adempimenti connessi all'attuazione del presente Decreto (a titolo esemplificativo, designazione del Responsabile del Servizio di Prevenzione e Protezione, designazione dei lavoratori incaricati dell'attuazione delle misure di prevenzione incendi, individuazione e designazione del Medico Competente, verifica e controllo della formazione del personale dipendente, …).

L'Ente rispetta tutte le prescrizioni contenute nel Testo Unico sulla Salute e Sicurezza sul lavoro, di cui al D.Lgs. 81/08.

A tal fine l'Ente si è dotato del Documento di Valutazione dei Rischi (DVR), il quale individua i rischi per la salute e la sicurezza dei lavoratori; predispone una serie di strumenti e di criteri di prevenzione al fine di fornire mezzi di protezione e misure di informazione al personale e assicura il costante aggiornamento dei dispositivi di sicurezza.

In relazione all'individuazione dei principi specifici da osservare nello svolgimento delle attività sensibili connesse al rischio di realizzazione dei reati di cui agli artt. 589 e 590, comma 3, c.p., il presente Modello fa espresso rinvio alle disposizioni contenute nel DVR adottato dall'Ente.

8.7 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai reati in materia di omicidio colposo e lesioni personali colpose avvenuti in violazione delle norme in materia di tutela della salute e della sicurezza sul lavoro

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai reati in materia di omicidio colposo e lesioni personali colpose avvenuti in violazione delle norme in materia di tutela della salute e della sicurezza sul lavoro.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Politica di Sicurezza Fisica e Ambientale
- Politica di Gestione del Capitale
- Politica di Esternalizzazione e Scelta dei Fornitori e sull'utilizzo dei Servizi ICT, compresi quelli a Supporto di Funzioni Essenziali o Importanti, prestati da Fornitori Terzi di Servizi ICT
- Procedura di Gestione del Personale

- Procedura di Gestione dei Processi e delle Procedure
- Procedura sui Flussi Informativi verso l'Alta Direzione
- Politica di Gestione degli Accessi
- Procedura per la Gestione delle Identità e dei Diritti di Accesso Fisici e Logici
- Politica di Gestione delle Identità.

CAPITOLO 9 RAZZISMO E XENOFOBIA

9.1 Le fattispecie di reato (art. 25 *terdecies* D.Lgs. 231/01)

L'art. 25 *terdecies* è stato inserito recentemente nel D.Lgs. 231/01 attraverso il recepimento della L. 20 novembre 2017, n. 167 (recante "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017").

L'art. 25 *terdecies* richiama i delitti puniti dall'articolo 3, comma 3 *bis*, della legge 13 ottobre 1975, n. 654, ovvero la condotta dei partecipanti ad organizzazioni, associazioni, movimenti o gruppi aventi tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi, nonché la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, fondati 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.

Va tuttavia rilevato che il D.Lgs. 21/2018, entrato in vigore il 6 aprile 2018, ha abrogato l'art. 3, comma 3 *bis*, della l. 654/75, senza intervenire direttamente sul D.Lgs. 231/01.

Per effetto di un tanto si potrebbe supporre un'abrogazione tacita del reato presupposto di cui all'art. 25 *terdecies*; tuttavia, va rilevata la contestuale introduzione del reato di propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa all'art. 604 *bis* del codice penale. Pertanto, al fine di armonizzare i contenuti delle normative analizzate sarebbe necessario un intervento sul D.Lgs. 231/01.

9.2 Attività sensibili e comportamenti vietati ai destinatari del MOG

UCA considera l'individuo, i suoi principi, i suoi diritti, valori intangibili da tutelare.

Ai dipendenti e ai collaboratori, nello svolgimento delle proprie mansioni, viene riconosciuta la più ampia libertà di espressione delle proprie idee e convinzioni, nel rispetto delle normative aziendali, dei diritti e delle dignità altrui.

La Compagnia contrasta e sanziona qualunque atteggiamento, anche solo apparentemente discriminatorio, con riguardo a nazionalità, stato di salute, età, sesso, religione, orientamenti religiosi, morali o filosofici, preferenze o attitudini sessuali ed opinioni politiche.

In forza dei principi osservati dall'Ente, il rischio di realizzazione dei reati in esame è trascurabile.

In ogni caso vanno considerate quali attività sensibili:

- la gestione dei rapporti con gli interlocutori (clienti, fornitori, rete commerciale);

- l’utilizzo dei locali presenti presso la sede dell’Ente e, più in generale, di tutte le proprietà immobiliari riconducibili all’Ente;
- la gestione dei finanziamenti.

I destinatari del presente Modello non devono in alcun modo prendere parte ad associazioni o comunque a gruppi che sono stati istituiti con lo scopo di fare propaganda, incitamento o istigazione fondato, 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.

La condotta anzidetta è vietata nel corso di qualsiasi rapporto con i terzi, a prescindere dalla modalità di svolgimento dell’incontro (di persona, telefonico, attraverso l’utilizzo di sistemi informatici).

L’Ente non deve mettere a disposizione i propri locali a soggetti che, anche solo astrattamente, sono sospettati di essere membri di gruppi o associazioni che hanno quale finalità la realizzazione di uno dei delitti di razzismo e xenofobia.

Infine, l’Ente non deve erogare finanziamenti a favore di organizzazioni che hanno quale finalità la propaganda, l’incitamento o l’istigazione fondati, in tutto o in parte, su ragioni discriminatorie.

Ogni finanziamento predisposto dall’Ente a favore di terzi deve essere debitamente documentato ed effettuato attraverso canali che ne assicurino la tracciabilità.

Prima di deliberare sull’erogazione del finanziamento il C.d.A. effettua adeguate ricerche sul destinatario del contributo e informa di un tanto l’OdV.

CAPITOLO 10 PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI E DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE (ARTT. 25 QUATER.1 E 25 QUINQUIES D.LGS. 231/01)

10.1 Pratiche di mutilazione degli organi genitali femminili (art. 25 *quater*.1 D.Lgs. 231/01)

La fattispecie, contemplata dall'art. 583-bis c.p., punisce le condotte di chi, in assenza di esigenze terapeutiche, determini la mutilazione degli organi genitali femminili o la lesione dei medesimi, qualora dalla lesione derivi una malattia nel corpo e nella mente.

10.2 Fattispecie di delitti contro la personalità individuale (art. 25 quinquies, D.Lgs. 231/01)

L'art. 25 *quinquies* D.Lgs. 231/01 richiama i delitti contro la personalità dell'individuo, vale a dire le fattispecie contemplate dagli artt. 600 e seguenti del c.p.:

- riduzione o mantenimento in schiavitù (art. 600 c.p.);
- prostituzione minorile (art. 600 *bis* c.p.);
- pornografia minorile (art. 600 *ter* c.p.);
- detenzione o accesso a materiale pornografico (art. 600 *quater* c.p.);
- pornografia virtuale (art. 600 *quater* 1 c.p.);
- iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 *quinquies* c.p.);
- tratta di persone (art. 601 c.p.);
- alienazione e acquisto di schiavi (art. 602 c.p.);
- intermediazione illecita e sfruttamento del lavoro (art. 603-*bis* c.p.);
- adescamento di minorenni (art. 609-*undecies* c.p.).

La classe di reati sopra indicata non presenta alcuna correlazione con le attività normalmente svolte dall'Ente, conseguentemente il rischio per il medesimo di incorrere nei reati contro la personalità individuale è trascurabile, eccezion fatta per la fattispecie di intermediazione illecita e sfruttamento del lavoro che - anche in considerazione del recente orientamento assunto dal Tribunale di Milano in materia[12] - la Società ha ritenuto opportuno, in ottica prudenziale, tenere in considerazione.

[12] Negli ultimi anni, infatti, numerose società, operanti nei settori più svariati (moda, logistica, vigilanza privata) sono state colpite da provvedimenti cautelari per caporalato, sfruttamento del lavoro e intermediazione illecita di manodopera. Maggiormente d'interesse in questa sede appare la vicenda che ha riguardato alcune aziende che sono state chiamate a rispondere penalmente per il fatto che applicavano ai propri dipendenti le tariffe retributive (sia pur minime) previste dal CCNL di settore, sottoscritto dalle associazioni di categoria maggiormente rappresentative.

10.3 Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)

Il reato si configura nei casi in cui taluno ponga in essere una delle seguenti condotte:

1) recluti manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;
2) utilizzi, assuma o impieghi 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.

La fattispecie precisa che 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.

10.4 Attività sensibili di UCA

Pur essendo basso il rischio di realizzazione dei reati contro la personalità individuale, è comunque possibile, in un'ottica di prevenzione, qualificare alcune attività svolte dall'Ente alla stregua di attività sensibili. In particolare, si tratta:

- della gestione dei rapporti con i dipendenti/collaboratori;
- dell'affidamento a terzi di servizi (es. esternalizzazione del servizio di pulizia dei locali);
- dell'utilizzo della rete internet.

10.5 Comportamenti vietati ai destinatari del MOG e principi specifici per le procedure

I Destinatari del Modello non devono:

- ricorrere, direttamente o indirettamente, a forme di sfruttamento del lavoro o intermediazione illecita di manodopera;

- stringere relazioni commerciali con soggetti di nota o sospetta appartenenza ad organizzazioni criminali e/o coinvolti in traffici illeciti legati al caporalato e alla intermediazione illecita
- instaurare rapporti con fornitori o appaltatori che non garantiscano il rispetto della normativa giuslavoristica (in materia di sicurezza, igiene, retribuzione, ecc.).

I Destinatari del Modello devono:

- definire il livello di retribuzione del personale (impiegato, funzionario e dirigente) in base all'inquadramento del lavoratore e facendo riferimento a quanto previsto dai Contratti Collettivi Nazionali di settore, così come previsto dalla Procedura Gestione del Personale, appurando in ogni caso che si tratti di retribuzione adeguata alla quantità e qualità della prestazione lavorativa richiesta, onde garantire la dignità del lavoratore e del servizio;
- osservare tutte le normative in materia di orario di lavoro, straordinari, ferie, riposi, permessi e congedi, tutela dei minori in età non lavorativa, ecc.;
- garantire situazioni lavorative, anche sotto il profilo igienico-sanitario, dignitose;
- selezionare fornitori e appaltatori previa adeguata attività di verifica in ordine alla sussistenza delle caratteristiche tecniche, professionali del fornitore, nonché rispetto alla sua onorabilità, eticità, conformità normativa e regolamentare, con particolare attenzione alla disciplina sulla tutela dei diritti umani ed alla normativa giuslavoristica (in materia di sicurezza, igiene, retribuzione, regolarità contributiva, ecc.).

L'Ente, in conformità ai principi sanciti nel Codice Etico, considera le risorse umane un patrimonio strategico ed essenziale per il conseguimento dei propri obiettivi e persegue una politica volta ad assicurare il riconoscimento dei meriti e a favorire la crescita professionale. Ne consegue che ogni valutazione di carattere economico ha valore recessivo rispetto alle esigenze di tutela dei diritti delle risorse umane. L'Ente tutela l'integrità morale e fisica dei dipendenti garantendo un ambiente di lavoro sano e sicuro, promuovendo la cultura della salute e della sicurezza, nonché il rispetto dei diritti e della personalità dei colleghi, dei collaboratori e dei terzi.

L'Ente si oppone a qualsiasi forma di lavoro irregolare; tutte le assunzioni/collaborazioni vengono regolamentate attraverso l'intervento dell'Ufficio di Gestione del Personale e lo Studio Professionale di Consulenza del Lavoro.

Nel corso del rapporto di lavoro, l'Ufficio Gestione del Personale si occupa della gestione della posizione contrattuale di ciascun dipendente. I dipendenti e i collaboratori devono utilizzare gli

strumenti informatici ed aziendali esclusivamente per finalità connesse allo svolgimento dell'attività lavorativa, rispettando le specifiche politiche di sicurezza impartite dalla Compagnia. I programmi non strettamente disposti dall'Ente sono vietati e viene punita l'eventuale installazione ed il successivo utilizzo.

10.6 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai reati contro la personalità individuale

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai reati contro la personalità individuale.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Politica di Sicurezza Fisica e Ambientale
- Politica di Gestione del Capitale
- Politica di Esternalizzazione e Scelta dei Fornitori e sull'utilizzo dei Servizi ICT, compresi quelli a Supporto di Funzioni Essenziali o Importanti, prestati da Fornitori Terzi di Servizi ICT
- Procedura di Gestione del Personale
- Procedura Ufficio Contratti
- Procedura di Gestione dei Processi e delle Procedure
- Procedura sui Flussi Informativi verso l'Alta Direzione
- Politica relativa alle Risorse Umane per la sicurezza delle informazioni
- Procedura per la Gestione delle Identità e dei Diritti di Accesso Fisici e Logici
- Politica di Gestione delle Identità
- Politica di Formazione dell'Organo Amministrativo, di Controllo e del Personale Rilevante
- Politica relativa alla Funzione di Verifica di Conformità alle Norme
- Politica relativa al Sistema di Controllo Interno.

CAPITOLO 11 REATI CONNESSI ALL'IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

11.1 Le fattispecie dei reati connessi all'impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 *duodecies* D. Lgs. N. 231/01)

Il D. Lgs. 109/12[13] ha introdotto nel D.Lgs. 231/01 l'art. 25 *duodecies*, che individua la responsabilità dell'Ente per il delitto punito dall'art. 22, comma 12 *bis*, D. Lgs. 286/1998.

L'art. 22, ai commi 12 e 12 *bis* prevede che *"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 5.000 euro per ogni lavoratore impiegato.*

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 particolare sfruttamento di cui al terzo comma dell'articolo 603 bis del codice penale."

Si rappresenta che, stante il richiamo da parte dell'art. 25 *duodecies* al solo comma 12 *bis*, la responsabilità dell'ente è prevista per la sola ipotesi in cui ricorrano le sopraccitate aggravanti speciali e, dunque, laddove l'ente che 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, 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 sfruttamento previste all'art. 603-bis, comma 3, c.p. (tali condizioni ricorrono nel caso di 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; ovvero nel caso di reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie; ovvero nel caso

[13] Il decreto in esame dà attuazione alla direttiva europea 18 giugno 2009 n. 2009/52/CE, recante norme minime relative a sanzioni e provvedimenti nei confronti di datori di lavoro che impiegano cittadini di paesi terzi il cui soggiorno è irregolare nel territorio dello Stato membro.

di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro; ovvero nel caso di sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti).

11.2 Attività sensibili di UCA

Il rischio che si configuri il reato sopra descritto è trascurabile.

Tuttavia, in un'ottica preventiva, si individuano le attività sensibili e i principi da seguire nello svolgimento delle medesime.

Le attività sensibili della Compagnia nelle quali vi è la possibilità di incorrere nella commissione dei reati di impiego di cittadini di paesi terzi con soggiorno irregolare, consistono principalmente nella selezione ed assunzione del personale e dei collaboratori e nella gestione degli appalti.

11.3 Comportamenti vietati ai destinatari del MOG e principi specifici per le procedure

L'Ente dichiara di non assumere dipendenti stranieri privi di regolare permesso di soggiorno e di non instaurare, o mantenere, rapporti di collaborazione con cittadini stranieri rientranti nella casistica individuata, nonché di non conferire incarichi ad appaltatori e/o subappaltatori che, al contrario, se ne avvalgono.

Così facendo l'Ente aderisce ai principi sanciti dalla Dichiarazione universale dei diritti dell'uomo, nonché a quanto previsto dalla normativa applicabile in materia di diritto del lavoro.In caso di assunzione di persone straniere residenti in Paesi terzi, l'Ente si rivolge alle Autorità competenti al fine di ottenere tutta la documentazione necessaria a consentire il regolare ingresso in Italia dello straniero e l'instaurazione di un rapporto di lavoro o di collaborazione regolare.

Per i cittadini stranieri già presenti in Italia l'Ente, prima di procedere all'assunzione o all'instaurazione del rapporto di collaborazione, verifica il possesso di un permesso di soggiorno regolare; inoltre, in costanza di rapporto, s'impegna a controllare che in occasione della scadenza dei permessi di soggiorno dei dipendenti stranieri, questi ultimi abbiamo provveduto ad avviare le relative pratiche di rinnovo, assicurando loro collaborazione nel rilascio della documentazione attestante l'impiego regolare presso la Società.

In ogni caso, la Società tutela prioritariamente i diritti delle persone e dei lavoratori rispetto a qualsiasi considerazione economica. A tal fine, osserva in modo puntuale tutte le normative in materia di orario di lavoro, straordinari, ferie, riposi, permessi e congedi, tutela dei minori in età non lavorativa e

assicura situazioni lavorative, anche sotto il profilo igienico-sanitario, dignitose e non degradanti.

11.4 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai reati connessi all'impiego di cittadini di paesi terzi il cui soggiorno è irregolare

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai reati connessi all'impiego di cittadini di paesi terzi il cui soggiorno è irregolare.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Politica di Sicurezza Fisica e Ambientale
- Politica di Gestione del Capitale
- Politica di Esternalizzazione e Scelta dei Fornitori e sull'utilizzo dei Servizi ICT, compresi quelli a Supporto di Funzioni Essenziali o Importanti, prestati da Fornitori Terzi di Servizi ICT
- Procedura di Gestione del Personale
- Procedura Ufficio Contratti
- Procedura di Gestione dei Processi e delle Procedure
- Procedura sui Flussi Informativi verso l'Alta Direzione
- Politica relativa alle Risorse Umane per la sicurezza delle informazioni
- Procedura per la Gestione delle Identità e dei Diritti di Accesso Fisici e Logici
- Politica di Gestione delle Identità
- Politica di Formazione dell'Organo Amministrativo, di Controllo e del Personale Rilevante
- Politica relativa alla Funzione di Verifica di Conformità alle Norme
- Politica relativa al Sistema di Controllo Interno.

CAPITOLO 12 REATI AMBIENTALI

12.1 Le fattispecie dei reati ambientali (art. 25 *undecies* D. Lgs. 231/01)

Il D. Lgs. 121/07[14] ha esteso la responsabilità amministrativa delle società e degli Enti ad una serie di reati ambientali.

Successivamente, la Legge n. 68/15, entrata in vigore il 29.05.2015, ha inserito nel Libro II del codice penale il titolo VI *bis* - "Delitti contro l'ambiente" - modificando l'art. 25 *undecies* del D. Lgs. 231/01, con la previsione di ulteriori reati ambientali che, se posti in essere, determinano una responsabilità amministrativa in capo all'Ente. Da ultimo, l'art. 25 *undecies* del D.Lgs. 231/01 è stato modificato dalla Legge n. 147/25, entrata in vigore in data 08.10.2025.

Di seguito si elencano i reati ambientali rilevanti ai sensi del D. Lgs. 231/01:

- inquinamento ambientale (art. 452 *bis* c.p.);
- disastro ambientale (art. 452 *quater* c.p.);
- delitti colposi contro l'ambiente (art. 452 *quinquies* c.p.);
- traffico ed abbandono di materiale ad alta radioattività (art. 452 *sexies* c.p.);
- impedimento del controllo (art. 452 *septies* c.p.);
- omessa bonifica (art. 452 *terdecies* c.p.);
- attività organizzate per il traffico illecito di rifiuti (art. 452 *quaterdecies* c.p.);
- uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727 *bis* c.p.);
- distruzione o deterioramento di *habitat* all'interno di un sito protetto (art. 733 *bis* c.p.);
- scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi e aeromobili (art. 137 Codice dell'Ambiente);
- abbandono di rifiuti non pericolosi in casi particolari (art. 255 *bis* Codice dell'Ambiente);
- abbandono di rifiuti pericolosi (art. 255 *ter* Codice dell'Ambiente);
- attività di gestione di rifiuti non autorizzata (art. 256 Codice dell'Ambiente);

[14] Attuazione della Direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della Direttiva 2009/123/CE che modifica la Direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni.

- combustione illecita di rifiuti (art. 256 *bis* Codice dell'Ambiente);
- inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (art. 257 Codice dell'Ambiente);
- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 Codice dell'Ambiente);
- spedizione illegale di rifiuti (art. 259, comma 1, Codice dell'Ambiente);
- delitti colposi in materia di rifiuti (art. 259-*ter* D.Lgs. 152/06);
- false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI – area movimentazione del trasporto di rifiuti (art. 260 *bis* commi 6 e 7, secondo e terzo periodo, e comma 8, primo periodo, Codice dell'Ambiente);
- violazione dei valori limite di emissione e delle prescrizioni stabilite dalle disposizioni normative o dalle Autorità competenti (art. 279, comma 5, Codice dell'Ambiente);
- importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (art. 1, commi 1 e 2; art. 2, commi 1 e 2; art. 6, comma 4 e art. 3 *bis*, comma 1, L. 150/92);
- cessazione e riduzione dell'impiego di sostanze lesive (art. 3, comma 6, L. 549/93);
- inquinamento doloso o colposo provocato dalle navi (art. 8, commi 1 e 2; art. 9, commi 1 e 2, D. Lgs. 202/07).

Il rischio di realizzazione di uno dei reati ambientali puniti dal Decreto è solo astrattamente ipotizzabile nella realtà aziendale di riferimento, in considerazione della tipologia di attività svolta dalla medesima. Di seguito sarà analizzata le sole fattispecie di reato ambientale punite dal Decreto che potrebbero essere commesse nel contesto aziendale considerato.

12.2 Abbandono di rifiuti non pericolosi in casi particolari (art. 255-*bis* D.Lgs. 152/06)[15]

Il delitto punisce l'abbandono o il deposito di rifiuti non pericolosi qualora: a) dal fatto derivi un pericolo per la vita o l'incolumità delle persone ovvero un pericolo di compromissione o deterioramento di acqua, aria, porzioni estese o significative del suolo o sottosuolo, ecosistema o biodiversità, anche agraria, di flora o fauna; b) il fatto sia commesso in siti contaminati o

15 Gli artt. 255-bis e 255-ter del D.Lgs. 152/2006 sono stati introdotti dalla Legge n. 147/2025, in vigore dall'8.10.2025.

potenzialmente contaminati (nonché su strade di accesso ai predetti siti e relative pertinenze).

12.3 Abbandono di rifiuti pericolosi (art. 255-*ter* D.Lgs. 152/06)

Il delitto punisce la mera condotta di abbandono o deposito di rifiuti pericolosi; è previsto un aggravamento di pena nell'ipotesi in cui: a) dal fatto derivi un pericolo per la vita o l'incolumità delle persone ovvero un pericolo di compromissione o deterioramento di acqua, aria, porzioni estese o significative del suolo o sottosuolo, ecosistema o biodiversità, anche agraria, di flora o fauna; b) il fatto sia commesso in siti contaminati o potenzialmente contaminati (nonché su strade di accesso ai predetti siti e relative pertinenze). Sono pericolosi i rifiuti esplosivi, comburenti, infiammabili, irritanti, tossici, cancerogeni, corrosivi, infettivi, mutageni, sensibilizzanti, ecotossici.

12.4 Attività di gestione di rifiuti non autorizzata (art. 256 D.Lgs. 152/06)

Fino alla Legge n. 147/2025, la norma puniva, al primo comma, l'attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza di specifica autorizzazione, mentre al terzo comma la realizzazione o gestione di una discarica non autorizzata. Entrambe le fattispecie erano di natura contravvenzionale.

Il legislatore nel 2025 modifica l'art. 256, "spacchettando" la fattispecie in due diverse ipotesi e prevedendo:

- nell'ipotesi base, una fattispecie contravvenzionale (punita con arresto o ammenda) volta a sanzionare la mera attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza di specifica autorizzazione; una fattispecie delittuosa (punita con la reclusione), nel caso in cui la gestione non autorizzata riguardi rifiuti pericolosi;
- nell'ipotesi aggravata, due fattispecie delittuose, a seconda che il fatto abbia ad oggetto rifiuti non pericolosi o pericolosi, qualora dalla gestione non autorizzata dei rifiuti derivi il pericolo per la vita o l'incolumità delle persone ovvero un pericolo di compromissione o deterioramento di acqua, aria, porzioni estese o significative del suolo o sottosuolo, ecosistema o biodiversità, anche agraria, di flora o fauna; ovvero qualora il fatto sia commesso in siti contaminati o potenzialmente contaminati (nonché su strade di accesso ai predetti siti e relative pertinenze).

12.5 Delitti colposi in materia di rifiuti (art. 259-*ter* D.Lgs. 152/06)

La fattispecie prevede una diminuzione delle sanzioni previste da un terzo a due terzi (anche per

l'ente) nel caso in cui taluno dei fatti di cui agli articoli 255-*bis*, 255-*ter*, 256 sia commesso per colpa.

12.6 Attività sensibili di UCA

Come sopra specificato, l'ipotesi di commissione di uno dei reati ambientali è, in linea di principio, scarsamente ipotizzabile all'interno della realtà aziendale considerata.

Tuttavia, con riferimento alla gestione non autorizzata di rifiuti, va comunque indicata come attività sensibile, nello svolgimento della quale potrebbe presentarsi il rischio di incorrere nella commissione del reato ambientale, la gestione dei rifiuti tossici (si pensi, a titolo esemplificativo, allo smaltimento dei toner).

Un'ulteriore attività sensibile per UCA, in materia di reati ambientali, va individuata nella gestione degli immobili di proprietà della Compagnia per quanto attiene alla violazione delle norme a tutela dell'ambiente in fase di ristrutturazione o di locazione dei medesimi.

12.7 Principi specifici per le procedure

Allo scopo di prevenire la commissione di reati ambientali, in via generale UCA promuove tra tutti i componenti un senso di responsabilità verso l'ambiente, la riduzione della produzione dei rifiuti e il rispetto della normativa vigente.

Per quanto concerne lo smaltimento dei rifiuti tossici, l'Ente aderisce al sistema di controllo della tracciabilità dei rifiuti tossici e affida la raccolta, il trasporto e lo smaltimento dei medesimi ad una società terza. In particolare, la società terza è responsabile del servizio di raccolta, trasporto e smaltimento dei toner delle macchine stampanti in dotazione agli uffici della Compagnia, attività che viene svolta secondo modalità coerenti con la normativa di riferimento.

Quanto alla procedura, il responsabile dell'Ufficio Servizi Generali provvede allo stoccaggio dei toner esausti negli idonei contenitori "ecobox", situati in apposito locale adibito a deposito/magazzino. Indicativamente ogni tre mesi, il medesimo Ufficio richiede via mail o telefono alla società terza il ritiro dei toner esausti. Questa, al ritiro, rilascia regolare copia del formulario identificativo del rifiuto (FIR), controfirmata e datata, che viene conservata dall'Ufficio Servizi Generali per 3 anni. Tutta la relativa documentazione cartacea viene conservata in apposito armadio presso l'Ufficio IT e la relativa scansione, effettuata dall'Ufficio Servizi Generali, viene archiviata in apposita cartella del server.

La gestione del patrimonio immobiliare è affidata all'Ufficio *Property*, inserito all'interno dell'Area Amministrazione, Finanza e Controllo, il quale dà materiale attuazione alle direttive del C.d.A. e alle

indicazioni provenienti direttamente dal suo Presidente. In particolare, in relazione alle attività di valorizzazione degli immobili (ad esempio, attraverso opere di ristrutturazione/cambio destinazione d'uso), nella scelta tra le diverse ipotesi di intervento, l'Ente si impegna ad adottare quella con minore impatto ambientale.

12.8 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai reati ambientali

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai reati ambientali.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Procedura in materia di Gestione Toner
- Politica di Sicurezza Fisica e Ambientale;
- Procedura Gestione Investimenti Immobiliari.

CAPITOLO 13 DELITTI DI CRIMINALITÀ ORGANIZZATA

13.1 Le fattispecie dei delitti di criminalità organizzata (art. 24 *ter* D.Lgs. 231/01)

L'art. 24 *ter* richiama le seguenti fattispecie di reato:

- associazione per delinquere (art. 416 c.p.);
- associazioni di tipo mafioso anche straniere (art. 416 *bis* c.p.);
- scambio elettorale politico - mafioso (art. 416 *ter* c.p.);
- sequestro di persona a scopo di estorsione (art. 630 c.p.);
- associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. n. 309/90);
- tutti i delitti se commessi avvalendosi delle condizioni previste dall'art. 416-bis c.p. ovvero per agevolare l'attività delle associazioni previste dallo stesso articolo;
- illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra, di esplosivi e armi clandestine nonché di più armi comuni da sparo escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110 (art. 407, comma 2, lett. a) n. 5 c.p.p.).

Il rischio per l'Ente di incorrere in responsabilità ai sensi del D. Lgs. 231/01 per la commissione di uno di tali reati è ipotizzabile solo in astratto. Di seguito si analizza l'unica fattispecie punita dal Decreto che potrebbe essere commessa nel contesto aziendale considerato.

13.2 Associazione per delinquere (art. 416 c.p.)

Fra tutti i reati indicati al superiore paragrafo merita di essere considerato il delitto di associazione per delinquere (art. 416 c.p.), che si realizza quando tre o più persone si associano allo scopo di commettere più delitti.

Con riferimento alla fattispecie dell'associazione per delinquere, la sanzione penale è ricollegata al solo fatto della promozione, costituzione, partecipazione ad una associazione criminosa formata da tre o più persone, indipendentemente dall'effettiva commissione (e distinta punizione) dei reati che costituiscono il fine dell'associazione.

Ciò significa che la sola cosciente partecipazione ad un'associazione criminosa da parte di un esponente o di un dipendente dell'Ente potrebbe determinare la responsabilità amministrativa dell'Ente stesso, sempre che la partecipazione o il concorso all'associazione risultasse strumentale al perseguimento anche dell'interesse o del vantaggio dell'Ente medesimo.

È inoltre richiesto che il vincolo associativo si esplichi attraverso un minimo di organizzazione a carattere stabile nel tempo e la condivisione di un programma di realizzazione di una serie indeterminata di delitti. Non basta, cioè, l'occasionale accordo per la commissione di uno o più delitti determinati: infatti, nel caso di accordo tra più soggetti per la commissione di uno o più delitti determinati, si verserà nell'ipotesi di concorso nel reato-fine e non nella più grave fattispecie di cui all'art. 416 c.p. L'Ente sarà responsabile anche nell'ipotesi in cui il reato sia commesso a livello "transnazionale" ai sensi dell'art. 10 della L. n. 146/06[16].

Si configura la fattispecie di associazione per delinquere a livello "transnazionale" quando è coinvolto un gruppo criminale organizzato, nonché il reato:

- è commesso in più di uno Stato;
- ovvero è commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avviene in un altro Stato;
- ovvero è commesso in uno Stato, ma in esso è implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- ovvero è commesso in uno Stato ma ha effetti sostanziali in un altro Stato.

13.3 Attività sensibili di UCA

Come sopra premesso, il rischio che l'Ente subisca una condanna ai sensi del D. Lgs. 231/01 per uno dei delitti di criminalità organizzata è trascurabile. Ciononostante, è opportuno il rispetto dei principi comportamentali che verranno descritti a seguire nello svolgimento delle attività di:

- selezione del personale;
- selezione dei rapporti di collaborazione;
- gestione della contabilità e degli adempimenti fiscali;
- selezione delle controparti contrattuali;
- omaggi, donazioni e sponsorizzazioni;
- utilizzo dei locali di proprietà dell'Ente.

13.4 Comportamenti vietati ai destinatari del MOG

I destinatari del presente Modello devono astenersi dal porre in essere, collaborare o dare causa alla

[16] Legge di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale.

realizzazione di comportamenti tali da integrare la fattispecie di reato di cui al presente capitolo, ovvero dal porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientrante fra quella sopra indicata, possono potenzialmente diventarlo. A tal fine:

- i fornitori devono essere selezionati verificando il rispetto degli standard aziendali (qualità, costo, puntualità delle consegne, disponibilità, tecnologia, innovazione, sostenibilità, conformità legale);
- i professionisti e i consulenti esterni ai quali si rivolge la Società devono contraddistinguersi per affidabilità, capacità ed onestà, conformità alle leggi, ai regolamenti e ai contratti vigenti;
- i pagamenti conseguenti agli ordini di acquisto devono essere effettuati con mezzi che garantiscono la tracciabilità, esclusivamente sul conto intestato al professionista/fornitore e mai in favore di soggetti diversi;
- è vietato utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
- è vietato intrattenere rapporti commerciali con soggetti dei quali sia nota o sospettata l'appartenenza ad organizzazioni criminali;
- gli immobili e i locali di proprietà della Società non possono essere concessi in locazione o comunque in uso ad associazioni che perseguono obiettivi criminali;
- in fase di selezione e di assunzione del personale (dipendenti, collaboratori, stagisti ecc.) occorre constatare la sussistenza di requisiti di onorabilità e affidabilità; parimenti, agenti, broker, partner di qualsiasi tipo vengono selezionati previa verifica del possesso dei requisiti di onorabilità e di affidabilità.

13.5 Principi specifici per le procedure

L'Ente:

- non assume personale senza avere verificato la sussistenza dei requisiti di onorabilità e affidabilità attraverso la produzione del certificato dei carichi pendenti/una autocertificazione resa ai sensi del D.P.R. 445/00;
- non instaura rapporti di collaborazione senza aver verificato la sussistenza dei requisiti di onorabilità e affidabilità attraverso la produzione del certificato dei carichi pendenti/una autocertificazione resa ai sensi del D.P.R. 445/00, richiesta contestualmente all'avvio della collaborazione;
- assicura la custodia in modo corretto e ordinato delle scritture contabili e degli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali e l'attuazione di un periodico monitoraggio del rispetto dei principi che regolano la compilazione, tenuta e conservazione delle dichiarazioni di natura contabile;
- nell'ambito dei rapporti contrattuali con i clienti, adotta regole che assicurino la massima trasparenza e chiarezza delle condizioni contrattuali applicate;
- attraverso l'Ufficio Assunzione Rischi fornisce adeguata consulenza alla rete commerciale, stabilendo i criteri di assumibilità dei rischi, i parametri tariffari e provvisionali ed esamina le richieste di assunzione di polizze collettive; in particolare, a titolo esemplificativo: 1) l'assunzione di massimali superiori agli importi standard di prodotto è riservata alla Compagnia e deve essere sempre posta al vaglio della Referente dell'Ufficio Assunzione Rischi che valuterà se esporle alla Direzione Commerciale per l'approvazione finale a seguito di una valutazione dell'andamento tecnico dell'Intermediario tramite lo strumento di PassAnalitycs; 2) clausole a testo libero con richieste integrative e/o derogatorie delle condizioni di polizza dovranno essere sottoposte alla Referente dell'Ufficio Assunzione Rischi che provvederà ad esporle, in base alla sostenibilità del rischio, alla Direzione Commerciale per l'approvazione; 3) sconti che superino il 20% dovranno essere posti al vaglio della Referente dell'Ufficio Assunzione Rischi;
- verifica che la rete distributiva adempia agli obblighi di adeguata verifica della clientela;
- assicura che le contribuzioni a titolo di liberalità, le donazioni o altre iniziative a carattere caritatevole siano effettuate solo in favore di enti di comprovata affidabilità, onestà e correttezza; garantisce in ogni caso la piena trasparenza del processo relativo alle sponsorizzazioni (quanto a budget destinato, enti beneficiari, finalità sottese); tutti i pagamenti

eseguiti in conseguenza di sponsorizzazioni devono essere effettuati esclusivamente sui conti intestati al beneficiario della sponsorizzazione.

13.6 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai delitti di criminalità organizzata

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai reati delitti di criminalità organizzata.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Procedura Ufficio Assunzione Rischi
- Politica sui Conflitti di Interesse
- Politica di Organizzazione, Gestione e Controllo della Distribuzione
- Politica di Esternalizzazione e Scelta dei Fornitori e sull'utilizzo dei Servizi ICT, compresi quelli a Supporto di Funzioni Essenziali o Importanti, prestati da Fornitori Terzi di Servizi ICT
- Politica relativa alla Funzione Attuariale
- Politica di Formazione dell'Organo Amministrativo, di Controllo e del Personale Rilevante
- Politica relativa alla Funzione di Verifica di Conformità alle Norme
- Politica relativa alla Funzione di Revisione Interna
- Politica di Remunerazione e Incentivazione degli Amministratori, Organi di Controllo, Personale Rilevante, Funzioni Fondamentali ed Altri Dipendenti
- Politica di Remunerazione e Incentivazione degli Intermediari Assicurativi
- Procedura Ufficio Antifrode
- Politica degli Investimenti
- Politica relativa al Sistema di Controllo Interno
- Procedura di Gestione del Personale
- Procedura Ufficio Contratti
- Procedura di Gestione dei Progetti Rilevanti
- Procedura di Gestione dei Processi e delle Procedure
- Procedura sui Flussi Informativi verso l'Alta Direzione
- Procedura Segreteria Societaria
- Procedura Rapporti con le Autorità.

CAPITOLO 14 DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

14.1 Fattispecie dei delitti contro l'industria e il commercio (art. 25 *bis.*1 D. Lgs. 231/01)

Il D. Lgs. 231/01 contempla le seguenti fattispecie delittuose:

- turbata libertà dell'industria o del commercio (art. 513 c.p.);
- illecita concorrenza con minaccia o violenza (art. 513 *bis* c.p.);
- frodi contro le industrie nazionali (art. 514 c.p.);
- frode nell'esercizio del commercio (art. 515 c.p.);
- vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517 *ter* c.p.);
- contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517 *quater* c.p.).

Di seguito si esaminano le sole fattispecie delittuose nelle quali potrebbe incorrere la Compagnia, trascurando le altre, la cui probabilità di realizzazione non è nemmeno astrattamente ipotizzabile.

14.2 Turbata libertà dell'industria o del commercio (art. 513 c.p.)

L'art. 513 c.p. punisce, a querela della persona offesa, chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio, vale a dire di un'attività produttiva e della rivendita dei beni a scopo di lucro.

La condotta può essere compiuta, alternativamente, mediante l'uso di violenza sulle cose, che implica il danneggiamento, la trasformazione o il mutamento di destinazione della cosa, ovvero mediante mezzi fraudolenti, vale a dire tutti i mezzi che sono idonei a trarre in inganno la vittima.

Nella prassi, generalmente, la condotta si realizza mediante il compimento di uno degli atti di concorrenza sleale di cui all'art. 2598 c.c.

Esempio

La società fa uso di mezzi fraudolenti nei confronti di un intermediario assicurativo che collabora con un competitor per indurlo a cessare l'attività di promozione di prodotti assicurativi del concorrente, con l'obiettivo di conquistare la relativa quota di mercato.

14.3 Illecita concorrenza con minaccia o con violenza (art. 513 *bis* c.p.)

La norma in esame punisce chiunque nell'esercizio di un'attività commerciale, industriale o comunque produttiva, compie atti di concorrenza con violenza o minaccia.

Non vengono puniti gli atti di concorrenza, che di per sé sono leciti, ma gli atti di concorrenza commessi con violenza sulla persona o sulle cose, ovvero con minaccia, prospettando al soggetto un male ingiusto e futuro.

Esempio

Il direttore commerciale minaccia alcuni ex collaboratori, prospettando loro un danno ingiusto per l'ipotesi in cui continuino ad intrattenere rapporti commerciali con un competitor.

14.4 Frode nell'esercizio del commercio (art. 515 c.p.)

La norma di cui sopra punisce il soggetto che, nell'esercizio di un'attività commerciale, ovvero in uno spaccio aperto al pubblico, consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità diversa da quella dichiarata o pattuita.

14.5 Attività sensibili di UCA

I reati contro l'industria e il commercio si inseriscono nell'ambito delle comunicazioni che la Compagnia intrattiene con l'esterno. È nel corso dello svolgimento di tale attività comunicativa che maggiore è il rischio di screditare un concorrente o i suoi prodotti, ovvero di esprimere apprezzamenti anche solo potenzialmente idonei a determinare un tanto o, ancora, di denigrare un concorrente o convincere, mediante l'inganno, un appaltatore a preferire la propria Compagnia al posto di altra.

Di seguito sono elencate le principali attività sensibili di UCA:

- gestione delle comunicazioni esterne, in considerazione dei profili di rischiosità connessi alla creazione, mediante artifici, di turbative all'esercizio dell'attività di altri;
- inserimento di contenuti nei vari *social network*;
- partecipazioni a gare, in considerazione dei profili di rischiosità connessi alla possibilità che vengano posti in essere comportamenti illeciti al fine di ottenere vantaggi nei confronti di un concorrente;
- gestione dei nuovi prodotti collocati dalla società;
- attività connesse alla stipula di nuovi accordi commerciali con altre società;
- approvvigionamento o utilizzo di prodotti, *software*, banche dati ed altre opere dell'ingegno, strumentali all'attività dell'Ente o destinati ad omaggi per la clientela.

14.6 Comportamenti vietati ai destinatari del MOG

I destinatari del presente Modello devono astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato elencate nel presente capitolo, ovvero dal porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti fra quelle sopra indicate, possono potenzialmente diventarlo.

In particolare, è fatto divieto di:

- usare nella commercializzazione dei prodotti assicurativi nomi o segni distintivi che possano produrre confusione con nomi o segni distintivi legittimamente usati da altri; in ogni caso, effettuare descrizioni dei prodotti commercializzati che non rispecchino le loro reali caratteristiche;
- diffondere notizie e apprezzamenti sui prodotti e sulle attività di un concorrente che possano determinare discredito o, in generale, attuare forme di concorrenza non corrette e trasparenti;
- concludere accordi con altre imprese o associazioni di imprese tali da pregiudicare il commercio o da impedire, restringere o falsare la concorrenza all'interno del mercato in cui l'Ente opera;
- ottenere segreti commerciali che appartengano ad altre aziende attraverso pratiche illegali;
- rivelare a terzi informazioni riguardanti le conoscenze tecniche, tecnologiche e commerciali della società, se non nei casi in cui tale rivelazione sia richiesta dall'Autorità Giudiziaria, da leggi o da altre disposizioni regolamentari o laddove sia espressamente prevista da specifici accordi contrattuali con cui le controparti si siano impegnate a utilizzarle esclusivamente per i fini per i quali dette informazioni sono trasmesse e a mantenerne la confidenzialità;
- assumere dipendenti di società concorrenti allo scopo di ottenere informazioni riservate o al fine di creare danno ai concorrenti.

14.7 Principi specifici per le procedure

UCA uniforma le proprie azioni improntando i rapporti con le altre Compagnie *competitors* al rispetto delle regole di concorrenza e di mercato, secondo libera e leale concorrenza.

I destinatari del presente documento si impegnano a non porre in essere comportamenti in contrasto con le disposizioni comunitarie e nazionali a tutela della libera concorrenza.

In particolare, vengono rispettati i seguenti principi:

- l'Ufficio Controllo Reti effettua dei controlli sulle comunicazioni pubblicitarie e sui siti degli

intermediari che contengono riferimenti ad UCA e accorda il benestare della Compagnia alla pubblicazione, ovvero indica all'intermediario le eventuali correzioni da apportare. In base al tenore della comunicazione riprodotta dall'intermediario l'Ufficio Controllo Reti verifica l'opportunità di richiedere il parere dell'Amministratore Delegato e dell'Ufficio Gestione Tecnico-Legale;

- il Responsabile dell'Ufficio Gestione Tecnico-Legale e la Funzione di Verifica di Conformità alle Norme verificano il contenuto dei testi pubblicitari predisposti dall'Ufficio *Marketing* (es. brochure, lettere offerta, …);
- la pubblicazione e l'utilizzo del marchio della Compagnia soggiace alla preventiva autorizzazione da parte dell'Ufficio Controllo Reti;
- l'Ufficio Stampa, costituito all'interno dell'Ufficio Incentive e Comunicazione, è responsabile della elaborazione dei Comunicati, secondo le indicazioni fornite dall'Alta Direzione e con l'eventuale supporto di consulenti/risorse esterne;
- l'Ufficio *Incentive* e Comunicazione valuta i contenuti inseriti nei vari *social network* ai quali l'Ente ha effettuato l'iscrizione (*Facebook*, *Twitter*, *Linkedin*, *Youtube*);
- l'Ufficio Assunzione Rischi assicura un'adeguata consulenza alla rete esterna in relazione alle soluzioni assicurative offerte e supporta la rete agenziale nella gestione delle proposte assicurative formulate tramite il portale Pass Compagnia;
- nell'ambito del controllo della Rete commerciale, l'Ente pone in essere dei controlli volti a monitorare l'utilizzo dei segni distintivi della Compagnia evitando che i medesimi vengano utilizzati in modo non conforme alle *policy* di UCA.

14.8 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai delitti contro l'industria e il commercio

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai delitti contro l'industria e il commercio.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Procedura Ufficio Antifrode
- Procedura Comunicati Stampa
- Politica sui Conflitti di Interesse
- Politica di Organizzazione, Gestione e Controllo della Distribuzione

- Politica di Gestione dei Reclami
- Politica di Remunerazione e Incentivazione degli Amministratori, Organi di Controllo, Personale Rilevante, Funzioni Fondamentali ed Altri Dipendenti
- Politica di Remunerazione e Incentivazione degli Intermediari Assicurativi
- Procedura di Gestione dei Progetti Rilevanti
- Procedura Ufficio Relazioni con la Clientela
- Procedura Ufficio Gestione Tecnico – Legale
- Procedura Ufficio Contenzioso
- Procedura Formazione Rete Distributiva.

CAPITOLO 15 FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO

15.1 Fattispecie di reato di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 *bis* D. Lgs. 231/01)

L'art. 25 *bis* D. Lgs. 231/01 richiama i seguenti reati:

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

Le fattispecie delittuose di cui sopra sono difficilmente compatibili con l'attività assicurativa svolta dalla Compagnia.

Fra di esse, le sole fattispecie che potrebbero avere una, sia pur remota, probabilità di verificazione sono quelle previste dagli artt. 457 e 473 c.p.

15.2 Spendita di monete falsificate in buona fede (art. 457 c.p.)

La fattispecie punisce il soggetto che spende o mette altrimenti in circolazione monete contraffatte o alterate, da lui ricevute in buona fede. Il reato è integrato nel caso in cui la spendita della moneta avvenga con la consapevolezza della sua falsità, consapevolezza acquisita in un momento successivo alla ricezione della stessa. Nel caso in cui la consapevolezza della falsità sia acquisita contestualmente alla ricezione della moneta, la spendita integrerà il diverso reato di cui all'art. 455 c.p.

15.3 Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)

La norma considerata punisce il soggetto che, potendo conoscere dell'esistenza del titolo di proprietà industriale, contraffà o altera marchi o segni distintivi, nazionali o esteri, di prodotti industriali, ovvero il soggetto che, senza essere concorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati.

Le condotte vietate sono identificate nella contraffazione e nell'alterazione di segni distintivi o prodotti industriali dei quali si conosce l'esistenza, ovvero nel semplice uso dei medesimi.

Attraverso la contraffazione il soggetto agente crea una cosa simile a quella già esistente, così da ingenerare confusione circa la sua essenza, mentre mediante l'alterazione modifica l'aspetto di una cosa.

Esempio

Al fine di promuovere un prodotto assicurativo, l'Ufficio Assunzione Rischi si avvale di un segno distintivo già registrato da un *competitor*.

15.4 Attività sensibili di UCA

Il rischio di commettere uno dei delitti di contraffazione richiamati dall'art. 25 *bis* D. Lgs. 231/01 è presente nello svolgimento delle seguenti attività:

- gestione delle transazioni finanziarie (incassi e pagamenti) e della cassa;
- commercializzazione dei prodotti assicurativi;
- gestione delle comunicazioni con l'esterno;
  abilitazione a sistema informatico della rete commerciale.

15.5 Comportamenti vietati ai destinatari del MOG

I destinatari del presente Modello devono astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare la fattispecie di reato sopra elencata, ovvero dal porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientrante fra quella sopra indicata, possono potenzialmente diventarlo.

Al fine di evitare che ciò si verifichi, si fa divieto di usare nomi o segni distintivi per la commercializzazione dei prodotti assicurativi che siano in grado di creare confusione con nomi o

segni usati da altri e di discostarsi nella descrizione di un prodotto assicurativo, dalle sue reali caratteristiche. Nello specifico, ai Destinatari è vietato:

- utilizzare marchi, loghi di compagnie assicurative in assenza di specifica autorizzazione;
- diffondere materiali pubblicitari contraffatti o di contenuto ambiguo, tali da trarre in inganno la clientela sull'identità dell'intermediario o della compagnia assicurativa.

La società si astiene dall'avviare collaborazioni con intermediari che fanno un uso distorto dei marchi e dei segni distintivi presenti sul mercato, in assenza di autorizzazione e che non garantiscono la trasparenza e la correttezza riguardo ai prodotti intermediati.

Nella gestione delle comunicazioni con l'esterno è vietato riportare nel contenuto della comunicazione il riferimento a caratteristiche che non appartengono al prodotto assicurativo commercializzato da UCA e che invece si riferiscono a prodotti offerti dai competitor.

Nella gestione della cassa e delle transazioni finanziarie, le operazioni eseguite mediante l'utilizzo del denaro contante devono essere tutte giustificate e tempestivamente registrate. Devono essere in ogni caso rispettati i limiti di utilizzo del denaro contante previsti dalla legge.

15.6 Principi specifici per le procedure

In conformità ai principi sanciti nel Codice Etico UCA opera sul mercato assicurando il rispetto dei principi di correttezza e di lealtà, respingendo ogni attività di contraffazione, alterazione o uso non concordato di segni distintivi.

A tal fine, si richiamano tutti i principi enunciati al paragrafo 14.7 del presente Modello.

CAPITOLO 16 DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

16.1 Fattispecie di delitti informatici e trattamento illecito di dati (art. 24 *bis* D. Lgs. 231/01)

L'articolo in esame è stato aggiunto dall'articolo 7 della L. 48/08[17].

Di seguito l'elenco dei delitti informatici richiamati dal D. Lgs. 231/01:

- documenti informatici (art. 491-*bis* c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.);
- detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-*quater* c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.);
- detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità (art. 635 *ter* c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 *quater* c.p.);
- 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.);
- frode informatica del certificatore di firma elettronica (art. 640 *quinquies* c.p.)
- violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1 comma 11, D.L. 21 settembre 2019 n. 105);
- estorsione (art. 629 comma 3 c.p.).

Di seguito, saranno oggetto d'esame solo quelle figure di reato che potrebbero realizzarsi nello svolgimento dell'attività di UCA.

[17] Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno.

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

La fattispecie si configura quando qualcuno accede o permane abusivamente (cioè senza il consenso del titolare dello *ius excludendi*, colui che ha il diritto di escluderlo) ad un sistema informatico o telematico protetto da misure di sicurezza.

Esempio

Una risorsa dell'area IT accede abusivamente ad un sistema informatico di proprietà di terzi per estrarre copia di un documento. Il reato è configurato altresì nel caso in cui la risorsa, abilitata all'accesso al sistema informatico, vi si mantenga per finalità diverse rispetto a quelle in forza delle quali l'accesso le era stato consentito, o comunque eccedendo i limiti delle istruzioni e direttive ricevute per il corretto utilizzo dello strumento informatico.

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

Il delitto consiste nel procurarsi, riprodurre, diffondere, consegnare o comunicare abusivamente, parole chiave, codici o altri mezzi idonei all'accesso di sistemi informatici o telematici, protetti da misure di sicurezza, al fine di procurare un profitto a sé o ad altri.

La norma punisce già le condotte preliminari all'accesso abusivo ad un sistema informatico, con evidente finalità di prevenzione.

Esempio

Una risorsa dell'area IT si procura in maniera illecita la *password* di accesso ad un sistema informatico verso il quale gli è precluso l'accesso; ovvero nel caso in cui la risorsa, in seguito ad un accesso abusivo al sistema informatico, comunichi a terzi i codici d'accesso ottenuti.

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

La norma punisce le condotte consistenti nell'intercettare fraudolentemente, impedire o interrompere comunicazioni con e tra mezzi informatici o telematici, nonché le condotte consistenti nel rivelare al pubblico notizie illegittimamente apprese.

Esempio

Una risorsa dell'area IT effettua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di una società concorrente.

16.5 Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.)

La fattispecie mira a prevenire il reato di cui all'art. 617 *quater*, punendo la condotta prodromica consistente nella mera installazione delle apparecchiature atte all'intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche.

Esempio

Una risorsa dell'area IT installa un'apparecchiatura finalizzata ad intercettare fraudolentemente le comunicazioni di una società concorrente, per compiere attività di sabotaggio industriale.

16.6 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.)

La fattispecie consiste nel procurarsi abusivamente, detenere, produrre, riprodurre, importare o diffondere o comunque mettere in altro modo a disposizione di altri o nell'installare apparecchiature, dispositivi o programmi informatici, atti allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o a favorire l'interruzione, totale o parziale o l'alterazione del suo funzionamento.

Esempio

Una risorsa dell'area IT si procura un virus idoneo ad intaccare, danneggiandolo illecitamente, un sistema informatico.

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

La disposizione in esame estende la punibilità già prevista per i delitti relativi alla falsità in atti (quindi, le falsità ideologiche e le falsità materiali in atto pubblico), alla falsità in documenti informatici.

La definizione di documento informatico è fornita dall'art. 1, comma 1, lett. p) del D.Lgs. 82/05. Esso consiste in *"una rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"*.

Esempio

Inserimento di dati falsi all'interno di una banca dati.

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

La norma punisce il soggetto che distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

Esempio

Un dipendente cancella dei dati dalla memoria dei server di Compagnia, senza essere stato autorizzato dal responsabile dell'Area Organizzazione/IT.

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

La fattispecie si configura quando attraverso una delle condotte di cui all'art. 635 *bis* c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, un soggetto distrugge, danneggia, rende, in tutto o in parte inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

Pertanto, quando l'alterazione dei dati e delle informazioni rende inservibile il sistema o comunque incide pesantemente sul suo funzionamento, si integra il delitto di danneggiamento di sistemi informatici e non il delitto di danneggiamento di dati (art. 635 *bis* c.p.).

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

La norma punisce la condotta già descritta all'art. 635 *quater* c.p., quando diretta a distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.
Il danneggiamento deve riguardare un sistema informatico utilizzato per il perseguimento di una pubblica utilità, a nulla rilevando la natura pubblica o privata del sistema.

16.11 Estorsione informatica (art. 629, comma 3, c.p.)

La fattispecie si realizza quando un soggetto, mediante le condotte di cui agli artt. 615-*ter*, 617-*quater*, 617-*sexies*, 635-*bis*, 635-*quater* e 635-*quinquies*, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

Esempio

Una risorsa dell'area IT cifra i dati di un'azienda concorrente chiedendo un riscatto in criptovalute per ripristinare gli accessi.

16.12 Attività sensibili di UCA

Consapevole della centralità che hanno assunto le risorse IT nell'organizzazione del business di impresa, UCA ha impartito specifiche politiche di sicurezza per la gestione e l'utilizzo degli strumenti informatici.
Costituiscono attività sensibili nell'ambito dei reati di trattamento illecito dei dati, le seguenti attività:

- l'utilizzo della rete aziendale, di internet, del sistema di posta elettronica;
- abilitazione all'utilizzo del sistema informatico da parte della rete commerciale;
- l'aggiornamento delle pagine e dei documenti, dell'area riservata ad Agenzie e Broker del sito internet aziendale;
- la gestione dei sistemi informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT, nonché la sicurezza informatica;

- la gestione del sito internet aziendale;
- la gestione dei *social network*;
- il trattamento di dati personali di cui l'Ente è in possesso (ad esempio, l'attività di implementazione del sistema Pass con i dati dei clienti/collaboratori)

In generale, possono essere considerate quali attività sensibili, tutte le attività aziendali svolte tramite l'utilizzo dei sistemi informativi aziendali, del servizio di posta elettronica e dell'accesso alla rete internet.

16.13 Comportamenti vietati ai destinatari del MOG

I destinatari del presente Modello devono astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra elencate, ovvero dal porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti fra quelle sopra indicate, possono potenzialmente diventarlo.

I destinatari del presente Modello non devono:

- effettuare copie non specificamente autorizzate di dati e software di UCA;
- svolgere attività di modifica e/o cancellazione di dati, informazioni non autorizzata;
- utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- lasciare incustodito e/o accessibile, senza la preventiva autorizzazione, ad altri il proprio pc;
- installare apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- introdurre e/o conservare sui sistemi di Compagnia documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo che sia stato acquisito con il consenso dei terzi;
- trasferire all'esterno file, documenti, o qualsiasi altra documentazione riservata di proprietà di UCA se non per finalità attinenti allo svolgimento delle proprie mansioni;
- prestare o cedere a terzi qualsiasi apparecchiatura informatica dell'Ente in assenza di preventiva autorizzazione.
- accedere abusivamente al sistema informatico della Compagnia al fine di alterare e/o cancellare dati e/o informazioni altrui;
- collegare alla rete aziendale i computer, i tablet e gli smartphone personali senza la preventiva

autorizzazione;

- introdurre in azienda applicazioni e software che non siano stati preventivamente autorizzati dall'Area IT.

16.14 Principi specifici per le procedure

Tutte le attrezzature, i dati, le informazioni e, in generale, le risorse dell'area IT sono di proprietà di UCA e devono essere utilizzati esclusivamente per motivi di lavoro.

L'Ente osserva i seguenti principi generali:

- riservatezza dei dati aziendali: garantisce che i dati siano preservati da accessi impropri e siano utilizzati esclusivamente da soggetti autorizzati;
- integrità dei dati aziendali: assicura che ogni dato sia realmente quello originariamente immesso nel sistema informatico e che le sue modifiche, eventuali, avvengano in modo legittimo. L'Ente assicura un trattamento corretto delle informazioni, evitando manomissioni da parte di terzi;
- disponibilità dei dati aziendali: garantisce la reperibilità dei dati in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Al fine di garantire il regolare trattamento dei dati, UCA ha messo a punto accorgimenti tecnici, logistici ed organizzativi che hanno per obiettivo la prevenzione di danni, perdite anche accidentali, alterazioni, utilizzo improprio e non autorizzato dei dati personali in conformità a quanto previsto dal Regolamento UE 2016/679 e dal D.Lgs. n. 196/2003, come novellato dal Decreto Legislativo 10 agosto 2018, n. 101.

Il presente documento fa espresso rinvio al Modello Organizzativo *Privacy* (MOP) adottato dalla Compagnia, il quale comprende i processi, le procedure e le attività che in concreto ha svolto l'Ente per garantire un livello di sicurezza e di protezione dei dati adeguato ai rischi provenienti da minacce esterne ed interne.

Ulteriori e specifiche misure a tutela del patrimonio informativo aziendale sono descritte nella documentazione in materia di *cyber security* (e negli allegati richiamati che ne costituiscono parte integrante e sostanziale) cui il presente Modello fa espresso rinvio, il quale definisce le misure di sicurezza assunte dall'Ente al fine di tutelare la *cyber security* aziendale.

In specie, le misure di tutela del patrimonio informativo aziendale avverso minacce interne ed esterne (che sono state individuate e analizzate nel "Documento di valutazione dei rischi aziendali - Sistema informativo Interno") consistono in quanto di seguito elencato in via esemplificativa:

- applicazione di politiche di sicurezza sui firewall con IPS;

- definizione di modalità di accesso ai sistemi;
- definizione di rigide *policy* di sicurezza per gli accessi ai server;
- implementazione di servizi di *backup*;
- svolgimento di test periodici (per es. di *disaster recovery*, di *restore* e verifica di ripristino);
- svolgimento di specifiche attività di *vulnerability assessment* e *penetration test*, finalizzate a individuare e bloccare accessi non autorizzati o avvertire i tecnici reperibili.

Tutte le ulteriori misure a tutela del patrimonio informativo aziendale e di tracciabilità degli accessi sono descritte nella documentazione che complessivamente compone e integra il Piano ICT aziendale, tra cui in particolare il Documento di valutazione dei rischi aziendali-Sistema informativo interno e il *Contingency Plan* ICT.

Il presente Modello, inoltre, fa espresso rinvio al documento sulle misure di sicurezza tecniche ed organizzative predisposto da UCA ai sensi dell'art. 32 del Regolamento UE 2016/679 nel quale sono descritte tutte le misure di sicurezza tecniche e organizzative adottate dalla Compagnia ai fini del trattamento dei dati personali forniti dagli interessati e della protezione del patrimonio informativo.

Per redigere il documento sono stati analizzati i dati personali trattati dall'Ente, sono stati valutati la tipologia di detti dati e gli strumenti utilizzati per il trattamento, nonché i rischi che incombono sui dati stessi e sono stati quindi definiti i criteri di protezione del patrimonio informativo in contesto.

In particolare, nel documento sulle misure di sicurezza tecniche ed organizzative sono indicate idonee informazioni riguardanti:

- gli estremi identificativi del Titolare del trattamento, nonché del Responsabile della protezione dei dati, dei Responsabili esterni; degli autorizzati e dei soggetti espressamente designati al trattamento dei dati nei termini previsti dalla normativa per tempo vigente in materia;
- la puntuale descrizione del trattamento o dei trattamenti realizzati, che permette di valutare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento. In tale descrizione sono precisate le finalità del trattamento, le categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime, nonché i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;
- l'elencazione delle altre misure di sicurezza adottate per prevenire i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

A tal fine, UCA rispetta le seguenti procedure:

- adotta sistemi di validazione delle credenziali di sufficiente complessità, che prevedono l'identificazione e l'autenticazione individuale degli utenti attraverso l'attribuzione di uno *user-id* e di una *password* associata. Le *password* hanno una lunghezza minima di otto caratteri e non è permesso l'uso di più di tre caratteri uguali in successione all'interno della *password*;
- garantisce la modifica periodica delle credenziali di accesso ai sistemi informatici;
- assicura che una stessa *user-id* non venga assegnata a persone diverse, neppure in tempi diversi;
- prevede che in caso di revoca dell'incarico, di cessazione o sospensione del rapporto di lavoro dell'utente la *user-id* sia revocata con effetto immediato;
- prevede che in caso di mutamento di mansioni dell'utente, il profilo del medesimo venga immediatamente modificato;
- assicura che i profili dei vari utenti siano gestiti in relazione alle reali necessità dei medesimi di trattare i diversi dati;
- verifica con cadenza semestrale la validità dei profili;
- effettua periodicamente la revisione degli apparati informatici presenti nei locali;
- dota ogni elaboratore di un prodotto antivirus;
- installa e configura sulle LAN di produzione firewall che analizzano i dati in entrata scartando i pacchetti sospetti;
- effettua giornalmente il *backup* dei *server*;
- assume tecniche di minimizzazione dei dati al fine di garantire che siano trattati soltanto i dati necessari in relazione alla specifica finalità del trattamento perseguita;
- ove sia necessario, tenuto conto della natura dei dati personali trattati e delle caratteristiche del trattamento, prevede l'applicazione delle tecniche di cifratura e pseudonimizzazione dei dati personali;
- predispone un piano di sicurezza e di protezione dei locali e degli archivi contenenti banche dati (attraverso la verifica degli accessi; l'adozione di sistemi di protezione dei dati da accessi non autorizzati);
- predispone dei sistemi di monitoraggio e di tracciamento degli accessi, nonché delle procedure specifiche per la gestione delle violazioni di dati personali e la notifica delle medesime all'Autorità Garante, nonché all'interessato ai sensi degli artt. 33 e 34 del Reg. UE 2016/679

(c.d. *data breach*);

- procede ad una suddivisione di ruoli e responsabilità tra gli addetti al trattamento dei dati;
- verifica che le informazioni, le applicazioni e le apparecchiature informatiche siano utilizzate esclusivamente per motivi di ufficio;
- verifica che la connessione ad internet sia utilizzata per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
- predispone, per tutti gli addetti al trattamento dei dati, specifiche clausole contrattuali di riservatezza e specifici vincoli per ottemperare ai principi in materia di protezione dei dati personali;
- si occupa direttamente, attraverso l'Ufficio IT, dell'aggiornamento delle pagine e dei documenti dell'area pubblica e riservata ad Agenzie e *Broker* del sito internet aziendale;
- garantisce agli intermediari l'assistenza necessaria all'utilizzo della piattaforma informatica.

Tutti i collaboratori e i dipendenti dell'Ente devono attenersi, nel corso dello svolgimento delle proprie mansioni quotidiane e, in particolare, nello svolgimento delle operazioni di trattamento di dati personali:

- al rispetto delle procedure aziendali riguardanti la sicurezza dei sistemi informativi, richiamate nel documento sulle misure di sicurezza assunte dall'Ente e nella normativa aziendale specifica;
- alle prescrizioni impartite dall'Ente negli atti di autorizzazione e/o a responsabile del trattamento dei dati personali relativamente a:
  - ✓ utilizzo dei pc;
  - ✓ utilizzo dei supporti di memorizzazione dei dati;
  - ✓ utilizzo della rete aziendale;
  - ✓ utilizzo di internet;
  - ✓ utilizzo della posta elettronica;
  - ✓ gestione delle *password*;
  - ✓ virus informatici.

A tutti i destinatari del presente documento si richiede di rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti, nonché all'Organismo di Vigilanza, eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche.

16.15 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai delitti informatici e in materia di trattamento illecito di dati

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai delitti informatici e trattamento illecito di dati.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Procedura Backup
- Procedura Change Management e Procedure per l'Acquisizione, lo Sviluppo e la Manutenzione dei Sistemi ICT
- Politica di Acquisizione, Sviluppo e Manutenzione dei Sistemi ICT
- Procedura di Gestione degli Incidenti di Natura ICT
- Procedura di Gestione di Sicurezza della Rete
- Procedura di Logging
- Procedura Gestione delle Risorse ICT
- Procedura per la Gestione delle Identità e dei Diritti di Accesso Fisici e Logici
- Procedura per la Protezione delle Informazioni in Transito
- Procedura per la Sicurezza dei Dati e dei Sistemi
- Procedura Gestione delle Vulnerabilità e Patch e Gestione delle Capacità e Prestazioni
- Politica di Crittografia e di Gestione delle Chiavi Crittografiche
- Politica di Gestione degli Accessi
- Politica di Gestione delle Identità
- Politica delle Misure di Protezione dei Dati Politica delle misure di protezione dei dati, di sicurezza delle informazioni e Politica per la protezione delle informazioni in transito
- Politica relativa alle Risorse Umane per la sicurezza delle informazioni
- Politica sulla Sicurezza delle ICT Operations
- Politica di Continuità dell'Attività
- Politica sulla Sicurezza delle Informazioni
- Procedura ICT Continuity & Disaster Recovery
- Politica di Gestione del Rischio Operativo

- Politica di Esternalizzazione e Scelta dei Fornitori e sull'utilizzo dei Servizi ICT, compresi quelli a Supporto di Funzioni Essenziali o Importanti, prestati da Fornitori Terzi di Servizi ICT.

CAPITOLO 17 DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

17.1 Le fattispecie dei delitti in materia di violazione del diritto d'autore (art. 25 *nonies* D. Lgs. 231/01)

La norma in esame richiama i seguenti reati all'interno del D. Lgs. 231/01:

- messa a disposizione del pubblico, tramite reti telematiche o mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa, incluse le opere altrui non destinate alla pubblicazione, qualora ne risulti offeso l'onore o la reputazione (art. 171, comma 1, lett. a *bis* e comma 3 legge sul diritto d'autore, L. 633/41);
- abusiva duplicazione, a fini di lucro, di programmi per elaboratore o importazione, distribuzione, vendita, detenzione per fini commerciali di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di programmi per elaboratori (art. 171 *bis*, comma 1, L. 633/41);
- 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. 633/1941);
- abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171 *ter*, L. 633/41);falsa dichiarazione, da parte del richiedente l'apposizione del contrassegno alla SIAE, in ordine all'avvenuto assolvimento degli obblighi derivanti dalla normativa sul diritto d'autore

- e sui diritti connessi[18] (art. 171-septies L. n. 633/1941).
- fraudolenta produzione, vendita, importazione, promozione, installazione, modifica e utilizzo per uso pubblico e privato, di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171 *octies*, L. 633/41).

Il rischio di commissione dei reati sopra indicati è basso nel contesto di riferimento, tuttavia, in un'ottica di prevenzione, si considerano i reati che comportano principali rischi per l'Ente.

17.2 Messa a disposizione del pubblico, tramite reti telematiche o mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa, incluse le opere altrui non destinate alla pubblicazione, qualora ne risulti offeso l'onore o la reputazione (art. 171, comma 1, lett. a *bis* e comma 3 legge sul diritto d'autore, L. 633/41)

La disposizione punisce chi 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 (art. 171, comma 1, lett. a *bis*, L. 633/41) e chi mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno altrui non destinata alla pubblicazione, 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.

Esempio

Il dipendente che carica sulla rete della Compagnia dei contenuti coperti dal diritto d'autore per utilizzarli.

17.3 Duplicazione, a fini di lucro, di programmi informatici o importazione, distribuzione, vendita, detenzione per fini commerciali di programmi contenuti in supporti non contrassegnati dalla SIAE (art. 171 *bis*, comma 1, L. 633/41)

La condotta punita consiste nel duplicare abusivamente, per trarne profitto, programmi per

18 L'art. 171-*septies* L. 633/1941 è stato modificato dalla Legge n. 166/2024 che ha disposto l'abrogazione della lett. a) del comma 1 che sanzionava la condotta di mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno.

elaboratore o ai medesimi fini importare, distribuire, vendere, detenere a scopo commerciale o imprenditoriale o concedere in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE).

È inoltre punito chi, al fine di trarre profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca dati ovvero distribuisce, vende o concede in locazione una banca di dati.

Esempio

Utilizzo di programmi informatici non originali, così da risparmiare il costo della licenza d'uso dei medesimi.

17.4 Attività sensibili di UCA

I delitti di cui sopra possono essere commessi dai destinatari durante l'utilizzo degli applicativi informatici aziendali, nella gestione del sito internet, dei *social network* e nella pianificazione dell'attività pubblicitaria.

Sono considerate attività sensibili:

- tutte le attività aziendali svolte dai destinatari del Modello tramite l'utilizzo dei sistemi informativi aziendali, del servizio di posta elettronica e dell'accesso alla rete;
- la gestione dei sistemi informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT nonché la sicurezza informatica;
- la gestione dei contenuti del sito internet aziendale;
- l'approvvigionamento e l'utilizzo di prodotti, *software*, banche dati ed altre opere dell'ingegno strumentali all'attività dell'Ente o destinati ad omaggi per la clientela;
- la gestione dei flussi informativi elettronici con la Pubblica Amministrazione;
- l'utilizzo di *software* e banche dati;
- la pianificazione dell'attività pubblicitaria e la pubblicizzazione dei prodotti assicurativi.

17.5 Comportamenti vietati ai destinatari del MOG

I destinatari del presente Modello devono astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra elencate, ovvero dal porre

in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti fra quelle sopra indicate, possono potenzialmente diventarlo.

In particolare, è fatto divieto di:

- connettere ai sistemi informatici dell'Ente pc, periferiche, altre apparecchiature o installare *software* senza preventiva autorizzazione dell'Area Organizzazione/IT;
- procedere ad installazioni di prodotti software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano il diritto d'autore;
- modificare la configurazione *software* e/o *hardware* di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale o, comunque, in assenza di preventiva autorizzazione da parte dell'Area Organizzazione/IT;
- divulgare, cedere o condividere con personale interno o esterno all'Ente le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- accedere abusivamente ad un sistema informatico altrui - ovvero nella disponibilità di altri dipendenti - nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto; in generale, utilizzare gli applicativi della Compagnia per finalità non connesse alla mansione svolta;
- acquisire e/o utilizzare prodotti tutelati da diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;
- accedere abusivamente al sito internet della Compagnia al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto ovvero allo scopo di immettervi dati o contenuti multimediali in violazione della normativa sul diritto d'autore;
- effettuare il download di software coperti da *copyright*.

17.6 Principi specifici per le procedure

I destinatari sono tenuti all'osservanza di tutti i principi già indicati nel capitolo dedicato ai reati di trattamento illecito dei dati, ai quali si fa espresso rinvio.

UCA si impegna:

- ad informare adeguatamente gli utilizzatori dei sistemi informatici che il *software* loro assegnato è protetto dalle leggi sul diritto d'autore ed in quanto tale ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;

- a fornire ai destinatari un'adeguata informazione relativamente alle opere protette dal diritto d'autore ed al rischio di realizzazione di tale reato;
- ad assicurare che nell'ambito delle attività di promozione/pubblicizzazione e nella gestione degli eventi, l'utilizzo, la messa a disposizione al pubblico, anche attraverso un sistema di reti telematiche, di opere dell'ingegno protette avvenga nel rispetto della normativa in materia di diritto d'autore;
- ad assicurare l'utilizzo corretto di *software* e delle banche dati in dotazione;
- a limitare gli accessi alle stanze *server* unicamente al personale autorizzato.

17.7 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai delitti in materia di violazione del diritto d'autore

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai delitti informatici e trattamento illecito di dati.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Politica di Acquisizione, Sviluppo e Manutenzione dei Sistemi ICT
- Procedura Gestione delle Risorse ICT
- Procedura per la Gestione delle Identità e dei Diritti di Accesso Fisici e Logici
- Procedura per la Protezione delle Informazioni in Transito
- Procedura per la Sicurezza dei Dati e dei Sistemi
- Politica di Crittografia e di Gestione delle Chiavi Crittografiche
- Politica di Gestione degli Accessi
- Politica di Gestione delle Identità
- Politica delle Misure di Protezione dei Dati Politica delle misure di protezione dei dati, di sicurezza delle informazioni e Politica per la protezione delle informazioni in transito
- Politica relativa alle Risorse Umane per la sicurezza delle informazioni
- Politica sulla Sicurezza delle ICT Operations
- Politica sulla Sicurezza delle Informazioni
- Procedura di Gestione dei Progetti Rilevanti
- Procedura Ufficio Contenzioso
- Procedura Ufficio Gestione Tecnico – Legale.

CAPITOLO 18 INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA

18.1 La fattispecie di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 *decies* D.Lgs. 231/2001)

La fattispecie contemplata dall'art. 377 *bis* c.p. punisce chi mediante minaccia o violenza, offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni false la persona chiamata a rendere all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando la persona chiamata ha la facoltà di non rispondere.

Trattasi di un delitto contro l'amministrazione della giustizia: la norma tutela il bene giuridico della genuinità della prova.

Esempio

Offerta di denaro ad un soggetto chiamato a rendere dichiarazioni in un processo che coinvolge l'azienda.

18.2 Attività sensibili di UCA

La principale attività sensibile individuata è la gestione dei rapporti con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale con riferimento a ogni ipotesi di indagine o di procedimento giudiziario penale riguardante o connesso con l'attività aziendale.

18.3 Comportamenti vietati ai destinatari del MOG

I destinatari del Modello non devono:

- intrattenere rapporti con persone sottoposte alle indagini preliminari e imputati nel processo penale al fine di turbare la loro libertà di autodeterminazione;
- riconoscere forme di liberalità o altre utilità a coloro che siano sottoposti alle indagini preliminari e imputati nel processo penale per indurli a omettere dichiarazioni o a falsare le stesse in favore dell'azienda.

18.4 Principi specifici per le procedure

Ai destinatari del presente Modello è richiesto di:

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

18.5 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Procedura Segreteria Societaria
- Procedura Rapporti con le Autorità
- Procedura Ufficio Gestione Tecnico – Legale
- Procedura Ufficio Contenzioso
- Politica relativa al Sistema di Controllo Interno.

CAPITOLO 19 I REATI TRIBUTARI

Il presente Capitolo del Modello, dopo una breve descrizione dei reati presupposto, identifica le aree di rischio, i principi di comportamento e le procedure che tutti i Destinatari del presente Modello devono adottare al fine di prevenire il verificarsi dei reati specifici.

19.1 Le fattispecie dei reati tributari (art. 25 *quinquiedecies* D. Lgs. 231/01[19])

I reati tributari previsti dal Decreto sono i seguenti:

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 commi 1 e 2 bis D.Lgs. n. 74/2000).
- dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000).
- dichiarazione infedele (art. 4 D.Lgs. 74/2020).
- omessa dichiarazione (art. 5 D.Lgs. 74/2020).
- emissione di fatture o altri documenti per operazioni inesistenti (art. 8 commi 1 e 2 bis D.Lgs. n. 74/2000).
- occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000).
- sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000).
- indebita compensazione (art. 10 *quater* D.Lgs. n. 74/2000).

19.2 Dichiarazione fraudolenta mediante uso di fatture o di altri documenti per operazioni inesistenti (art. 2 D.Lgs. 74/2000)

Il reato si configura nei casi in cui, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, vengano indicati, in qualunque dichiarazione relativa a dette imposte, elementi passivi fittizi. Tali fatture o documenti, per l'integrazione del reato, devono essere stati registrati nelle scritture contabili obbligatorie o, comunque, devono esser stati detenuti a fine di prova nei confronti dell'Amministrazione finanziaria.

[19] L'art. 25 *quinquiesdecies* D.Lgs. 231/01 è stato introdotto dal D.L. 124/2019 ed è stato successivamente modificato, con l'ingresso di nuove fattispecie incriminatrici tra i reati presupposto, dal D.Lgs. 75/2020 (segnatamente, sono confluiti nel novero dei reati presupposto con il D.Lgs. 75/2020 i reati di cui agli artt. 4, 5 e 10 *quater* D.Lgs. 74/2000).

19.3 Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. 74/2000)

La fattispecie riguarda le condotte, finalizzate all'evasione fiscale, consistenti nel compimento di operazioni oggettivamente in tutto o in parte inesistenti (simulate), ovvero di operazioni riferite a soggetti fittiziamente interposti. In alternativa, per il compimento del reato in oggetto, si può ricorrere a documenti falsi e ad altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'Amministrazione finanziaria. Affinché il reato sia integrato, occorre tuttavia che nelle dichiarazioni relative alle imposte sui redditi o sul valore aggiunto siano superate specifiche soglie di punibilità (previste dall'art. 3[20]).

19.4 Dichiarazione infedele (art. 4 D.Lgs. 74/2000)

La fattispecie si verifica quando, al fine di evadere le imposte sui redditi o sul valore aggiunto, vengono indicate nella dichiarazione annuale relativa a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti. Anche in tal caso sono previste specifiche soglie di punibilità per l'integrazione del reato *de quo*[21]. Il reato comporta la responsabilità dell'ente ai sensi del decreto 231/01 solo se commesso nell'ambito di sistemi fraudolenti transfrontalieri (connessi al territorio di almeno un altro Stato membro dell'Unione Europea) al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.

19.5 Omessa dichiarazione (art. 5 D.Lgs. 74/2000)

La fattispecie punisce il soggetto che, essendovi obbligato, al fine di evadere le imposte sui redditi o

---

20 Nello specifico, occorre che nelle dichiarazioni relative alle imposte sui redditi o sul valore aggiunto siano indicati elementi attivi per un ammontare inferiore a quello effettivo, ovvero passività fittizie quando, congiuntamente: a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a 30.000 euro; b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore 1.500.000 euro, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al 5% dell'ammontare dell'imposta medesima o comunque a 30.000.

21 Nello specifico, occorre che nelle dichiarazioni relative alle imposte sui redditi o sul valore aggiunto siano indicati elementi attivi per un ammontare inferiore a quello effettivo, ovvero passività fittizie quando, congiuntamente: a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a 100.000 euro; b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al 10% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a 2.000.000 di euro.

sul valore aggiunto, non presenta una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a 50.000 euro. Parimenti, il reato è integrato nel caso di chi, essendovi obbligato, ometta di presentare la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore a 50.000 euro. Il reato comporta la responsabilità dell'ente ai sensi del Decreto 231/01 solo se commesso nell'ambito di sistemi fraudolenti transfrontalieri (connessi al territorio di almeno un altro Stato membro dell'Unione Europea) al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.

19.6 Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, commi 1 e 2 bis, D.Lgs. 74/2000)

La norma punisce il soggetto che, 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. Trattasi dunque di fattispecie speculare a quella prevista dall'art. 2 che sanziona, invece, la condotta di annotazione di tali fatture o documenti per operazioni inesistenti.

19.7 Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. 74/2000)

Il reato si configura quando un soggetto, al fine di evadere le imposte sui redditi o sul valore aggiunto, o 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.

19.8 Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. 74/2000)

La norma punisce il soggetto che, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore a 50.000 euro, simuli una vendita, o compia altri atti fraudolenti, per privarsi di beni che l'Amministrazione Finanziaria potrebbe aggredire in caso di riscossione coattiva. Punisce, inoltre, il comportamento di chi espone nella documentazione presentata per la procedura di transazione fiscale elementi attivi di ammontare inferiore a quello effettivo, o elementi passivi fittizi di

importo superiore a 50.000 euro, con lo scopo di ottenere un ridotto pagamento di tributi e accessori, per sé o per altri.

19.9 Indebita compensazione (art. 10 quater D.Lgs. 74/2000)

Il reato si configura ogniqualvolta il contribuente non versa le somme dovute, utilizzando in compensazione dei crediti d'imposta inesistenti o non spettanti, per un importo superiore ai 50.000,00 euro annui. Con l'espressione "somme dovute" ci si riferisce a qualsiasi versamento da eseguire mediante modello F24. Il reato comporta la responsabilità dell'ente ai sensi del decreto 231/01 solo se commesso nell'ambito di sistemi fraudolenti transfrontalieri (connessi al territorio di almeno un altro Stato membro dell'Unione Europea) al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.

19.10 Attività sensibili di UCA

Le aree ritenute maggiormente a rischio per l'Azienda in relazione ai reati tributari sono considerate le seguenti:

a) AFC per la redazione del bilancio;
b) Alta Direzione con riferimento alla formalizzazione di ordini e contratti;
c) AFC per le ritenute relative al personale ed ai lavoratori autonomi;
d) AFC e IT per il ciclo attivo e passivo.

19.11 Principi generali di comportamento

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualsiasi titolo, siano coinvolti nelle attività sensibili rispetto ai reati tributari previsti dall'art. 25 *quinquiesdecies* del D. Lgs.231 2001.

A tali soggetti, in via generale, è richiesto di:

- rispettare scrupolosamente tutte le procedure formalizzate, ritenute idonee a fornire modalità operative per lo svolgimento, l'archiviazione delle attività relative alla gestione delle acquisizioni di beni e servizi ed alla gestione degli adempimenti contabili, fiscali e contributivi;
- verificare che i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative e gestionali assegnate;
- instaurare e mantenere qualsiasi rapporto con i terzi in tutte le attività relative all'acquisto o

alla vendita di beni e servizi sulla base di criteri di correttezza e trasparenza che garantiscano il buon andamento della funzione e/o servizio;

- osservare rigorosamente tutte le leggi e i regolamenti che disciplinano l'attività della Compagnia, con particolare riferimento alle attività che comportano l'emissione di documenti contabili attivi ed il ricevimento di documenti contabili passivi;
- instaurare e mantenere qualsiasi rapporto con l'Agenzia delle Entrate sulla base di criteri di massima correttezza e trasparenza;
- garantire massima collaborazione e trasparenza nei rapporti con il Collegio sindacale e la società incaricata della revisione legale.

19.12 Comportamenti vietati ai destinatari del MOG

I destinatari del Modello devono astenersi dal porre in essere comportamenti tali da integrare una delle fattispecie di reato individuate dall'art. 25 *quinquiesdecies* del Decreto, ovvero dal porre in essere comportamenti che, sebbene non siano così gravi da costituire una delle fattispecie di reato anzidette, possono potenzialmente diventarle.

È fatto espresso divieto ai Destinatari di:

- alterare il funzionamento di sistemi informativi e telematici o manipolare i dati in essi contenuti;
- indicare nelle dichiarazioni fiscali elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi;
- indicare nelle dichiarazioni fiscali una base imponibile in misura inferiore a quella effettiva (ad esempio costi fittiziamente sostenuti e/o ricavi indicati in misura inferiore a quella reale);
- porre in compensazione crediti inesistenti;
- emettere o utilizzare fatture o altri documenti contabili relativi ad operazioni inesistenti;
- emettere o utilizzare fatture o altri documenti contabili per corrispettivi superiori agli importi effettivi;
- emettere o utilizzare fatture o altri documenti contabili che indichino soggetti diversi da quelli tra cui è effettivamente intercorso il rapporto sotteso;
- effettuare pagamenti a fronte dell'emissione di fatture relative ad attività mai ricevute.

19.13 Principi specifici per le procedure

Ai destinatari del Modello è richiesto, in linea con quanto sancito dal Codice Etico, di mantenere una condotta improntata ai principi di onestà e correttezza, agendo con trasparenza e buona fede nello svolgimento delle proprie attività.

Il presente documento individua i seguenti principi/manuali/procedure da rispettare al fine di eliminare il rischio per l'Ente di incorrere in uno dei reati considerati nei superiori paragrafi:

- ciclo attivo: come da procedura inserita nel Manuale Operativo della contabilità e bilancio quanto alla fatturazione ed alla contabilità ciclo tecnico;
- ciclo passivo: come da procedura inserita nel Manuale Operativo della contabilità e bilancio quanto alla fatturazione ed alla contabilità ciclo tecnico e nella Procedura dell'Ufficio contratti;
- salvataggio e archiviazione dati libri contabili obbligatori e altri documenti obbligatori: come da procedura inserita nel Manuale Operativo della contabilità e bilancio quanto a produzione e stampa dei bollati;
- ritenute lavoratori autonomi e dispendenti: come da procedura inserita nel Manuale Operativo della contabilità e bilancio quanto al controllo ritenute lavoratori autonomi e dipendenti;
- formazione del bilancio annuale: come da procedura inserita nel Manuale Operativo bilancio annuale e semestrale.

I rischi sono peraltro mitigati dalla presenza del Collegio Sindacale e della Società di Revisione che effettua verifiche a campione in sede di bilancio e periodiche e che è chiamata a sottoscrivere le dichiarazioni fiscali.

Ai fini della mitigazione del rischio di commissione dei reati previsti dall'art. 25-*quinquiesdecies* del Decreto (reati tributari) si intendono inoltre richiamati i principi di comportamento del presente modello riferiti ai reati societari.

19.14 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai reati tributari

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai reati tributari.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Politica per la Valutazione delle Attività e delle Passività diverse dalle riserve tecniche
- Politica di Gestione delle Attività e delle Passività
- Politica di Gestione del Capitale
- Procedura Asset And Liability Management
- Politica di Gestione del Patrimonio Immobiliare
- Procedura di Valutazione degli Immobili
- Politica relativa alla Gestione dei Rischi
- Politica di Gestione del Rischio Liquidità
- Politica di Gestione del Rischio Operativo
- Politica relativa alla Funzione Attuariale
- Politica di Formazione dell'Organo Amministrativo, di Controllo e del Personale Rilevante
- Politica relativa alla Funzione di Verifica di Conformità alle Norme
- Politica relativa alla Funzione di Revisione Interna
- Politica degli Investimenti
- Procedura sui Processi e Responsabilità nelle procedure di Trasmissione dei Dati Anagrafici e Societari
- Procedura sui Flussi Informativi verso l'Alta Direzione
- Procedura Segreteria Societaria
- Procedura Rapporti con le Autorità
- Procedura Ufficio Gestione Tecnico – Legale
- Procedura Ufficio Contenzioso
- Procedura Ufficio Contratti
- Politica relativa al Sistema di Controllo Interno
- Procedura di Gestione dei Processi e delle Procedure.

CAPITOLO 20 ABUSI DI MERCATO

20.1 Le fattispecie in materia di abusi di mercato (artt. 25 *sexies* D.Lgs. 231/2001 e 187 *quinquies* T.U.F.)

L'art. 25 *sexies* D.Lgs. 231/01 richiama i seguenti reati:

- abuso di informazioni privilegiate (art. 184 TUF);
- manipolazione di mercato (art. 185 TUF).

In aggiunta, l'art. 187 quinquies TUF (a seguito della modifica operata dal D.Lgs. 107/2018) prevede che l'ente sia punito con una sanzione amministrativa pecuniaria da 20.000 a 15.000.000 di euro, ovvero fino al 15% del fatturato (quando tale importo sia superiore a 15.000.000 di euro), nel caso in cui sia commessa nel suo interesse o a suo vantaggio una violazione del divieto di cui all'articolo 14 (divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate) o del divieto di cui all'articolo 15 (divieto di manipolazione del mercato) del Regolamento (UE) n. 596/2014 (c.d. "Regolamento MAR" - *Market Abuse Regulation*):

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria o funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

Il rischio di commissione dei reati sopra indicati è basso nel contesto di riferimento, non essendo UCA una società quotata, tuttavia, in un'ottica di prevenzione, si considerano le fattispecie (di reato e amministrative) che comportano principali rischi per l'Ente, di seguito descritte.

20.2 Abuso di informazioni privilegiate (art. 184 TUF)

Prima di descrivere la fattispecie, si rende doverosa una premessa in ordine al concetto di "informazione privilegiata" - fulcro della disciplina in materia di abusi di mercato - per la cui definizione l'art. 180, comma 1, lett. b-ter) del TUF rinvia all'art. 7 del Regolamento (UE) n. 596/2014 (c.d. "Regolamento MAR" - *Market Abuse Regulation*). In particolare, l'art. 7 del Regolamento MAR individua quattro elementi fondamentali che devono contraddistinguere l'informazione privilegiata:

a. deve avere carattere preciso (deve riferirsi a circostanze o eventi, in atto o di verificazione

ragionevolmente prevedibile, caratterizzati da un elevato grado di oggettività e di certezza, con esclusione delle notizie del tutto vaghe o comunque non supportate da dati oggettivi; deve essere inoltre sufficientemente specifica, circostanziata e determinata, tale da permettere di trarre conclusioni univoche in ordine al suo effetto sul prezzo dello strumento finanziario);

b. dev'essere di natura non pubblica;
c. deve concernere, in modo diretto o indiretto, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari (si parla di "*market information*" ove l'informazione riguardi gli strumenti finanziari quotati; si parla di "*corporate information*" ove l'informazione riguardi emittenti di strumenti finanziari quotati);
d. qualora venisse divulgata, dev'essere idonea ad incidere sensibilmente sui prezzi degli stessi strumenti finanziari interessati o connessi (c.d. "*price-sensitive information*").

La fattispecie punisce chiunque, essendo in possesso di informazioni privilegiate in quanto membro di organi di amministrazione, direzione o controllo di una società emittente o in quanto socio dell'emittente o, comunque avendole apprese nell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:

a. utilizzando tali informazioni, acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o di terzi, su strumenti finanziari (c.d. "*insider trading*");
b. comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato (c.d. "*tipping*"); a tal fine, non rileva l'effettivo utilizzo dell'informazione da parte del destinatario della comunicazione;
c. raccomanda o induce altri, sulla base di tali informazioni, al compimento di taluna delle operazioni indicate nella lettera a) (c.d. "*tuyautage*").

La fattispecie sanziona altresì chi, essendo in possesso di informazioni privilegiate per la preparazione o per l'esecuzione di attività delittuose, commette taluno dei fatti di cui sopra. Si pensi al caso si chi, a seguito di un accesso abusivo ad un sistema informatico aziendale, entri in possesso di informazioni riservate c.d. "*price sensitive*" e le utilizzi per compiere operazioni su strumenti finanziari.

20.3 Divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate (art. 14 MAR)

L'art. 14 del Regolamento MAR prevede che non è consentito: a) abusare o tentare di abusare di informazioni privilegiate; b) raccomandare ad altri di abusare di informazioni privilegiate o indurre altri ad abusare di informazioni privilegiate; oppure c) comunicare in modo illecito informazioni privilegiate.

Per capire che cosa sia l'abuso di informazioni privilegiate, occorre far riferimento all'art. 8 MAR:

a. si ha abuso di informazioni privilegiate quando una persona, in possesso di informazioni privilegiate, le utilizza, acquisendo o cedendo, per conto proprio o per conto di terzi, direttamente o indirettamente, gli strumenti finanziari cui tali informazioni si riferiscono. È considerato abuso di informazioni privilegiate anche l'uso di dette informazioni tramite annullamento o modifica di un ordine concernente uno strumento finanziario al quale le informazioni si riferiscono, quando tale ordine è stato inoltrato prima che la persona interessata entrasse in possesso di dette informazioni privilegiate;

b. si ha raccomandazione (c.d. "*tuyautage*") nel caso in cui una persona, in possesso di informazioni privilegiate, raccomandi sulla base di tali informazioni ad un soggetto di acquisire o cedere strumenti finanziari, oppure raccomandi la cancellazione o la modifica di un ordine già emesso, relativo ad uno strumento finanziario al quale si riferisce l'informazione privilegiata.

Quanto alla condotta di comunicazione illecita di informazioni privilegiate, occorre far riferimento all'art. 10 MAR: essa è integrata quando una persona, in possesso di informazioni privilegiate, le comunica a terzi, tranne quando la comunicazione avvenga nel contesto del normale esercizio di un'occupazione, una professione o una funzione.

20.4 Attività sensibili di UCA

La principale attività sensibile individuata concerne la gestione e la divulgazione delle informazioni da/verso l'esterno (nei rapporti con gli *stakeholders*, il mercato, il pubblico, ecc.).

20.5 Comportamenti vietati ai destinatari del MOG

I destinatari del Modello non devono:

- utilizzare e/o comunicare informazioni privilegiate di cui siano in possesso, a qualsiasi titolo e per ogni ragione, a terzi (clienti, consulenti, *traders*, persone operanti nel settore dei mercati

finanziari, ecc.) per ragioni e finalità diverse da quelle inerenti l'ufficio o il ruolo ricoperto;

- comunicare, diffondere, divulgare attraverso qualsiasi mezzo informazioni, notizie, dati, voci non corrispondenti alla realtà o di cui comunque sia dubbia la veridicità, laddove le stesse siano anche solo potenzialmente idonee a determinare un'alterazione sensibile del prezzo di strumenti finanziari;
- lasciare incustodita la documentazione relativa ad informazioni privilegiate;
- partecipare, anche attraverso l'uso dei *social media*, a gruppi di discussione o *chat* al fine di scambiare, venire in possesso o comunicare informazioni privilegiate o *price sensitive*;
- discutere ad alta voce di informazioni privilegiate o *price sensitive* in luoghi pubblici o aperti al pubblico o, comunque, in luoghi affollati.

20.6 Principi specifici per le procedure

Ai destinatari del presente Modello è richiesto di:

- mantenere riservate tutte le informazioni, i dati, i documenti e le notizie acquisite a causa o in occasione dello svolgimento delle proprie funzioni, sia relativi alla Società, sia agli strumenti finanziari dalla stessa detenuti;
- garantire la riservatezza, adottando ogni possibile cautela, su tutte le informazioni privilegiate di cui vengano comunque a conoscenza. A tal fine, tra le misure adottate da UCA, la Politica relativa alle Risorse Umane per la Sicurezza delle Informazioni prevede un'informativa da inviare annualmente a dipendenti e fornitori terzi ed in occasione di ogni nuova assunzione/nuovo contratto che comprende i seguenti aspetti: 1) tutto il personale e i fornitori terzi sono tenuti a conoscere, comprendere e rispettare le politiche, le procedure e i protocolli di sicurezza ICT. Ciascun individuo ha la responsabilità di contribuire alla protezione delle informazioni e alla salvaguardia delle risorse aziendali; 2) UCA promuove una cultura di trasparenza e incoraggia il personale e i fornitori terzi a segnalare eventuali comportamenti o attività anomale tramite i canali di segnalazione predisposti; 3) l'obbligo per i dipendenti di restituire immediatamente tutte le risorse ICT ed i patrimoni informativi di proprietà della Compagnia, in caso di cessazione del rapporto di lavoro.

20.7 Elenco delle Politiche, delle Procedure e dei protocolli adottati da UCA da osservare nello svolgimento delle "attività sensibili" relative ai reati in materia di abusi di mercato

Di seguito sono riportate le Politiche, le Procedure e i protocolli adottati dalla Compagnia che devono essere pedissequamente osservati dai Destinatari del Modello nello svolgimento dei processi a rischio e delle attività sensibili, con riferimento ai reati in materia di abusi di mercato.

Tali documenti sono parte integrante del Modello e s'intendono integralmente richiamati:

- Politica sull'Informativa al Pubblico e Politica sulle Informazioni da Fornire all'IVASS
- Procedura Comunicati Stampa
- Procedura sui Processi e Responsabilità nelle procedure di Trasmissione dei Dati Anagrafici e Societari
- Procedura Rapporti con le Autorità
- Procedura per la Gestione delle Identità e dei Diritti di Accesso Fisici e Logici
- Procedura per la Protezione delle Informazioni in Transito
- Procedura per la Sicurezza dei Dati e dei Sistemi
- Politica di Crittografia e di Gestione delle Chiavi Crittografiche
- Politica di Gestione degli Accessi
- Politica di Gestione delle Identità
- Politica delle Misure di Protezione dei Dati Politica delle misure di protezione dei dati, di sicurezza delle informazioni e Politica per la protezione delle informazioni in transito
- Politica relativa alle Risorse Umane per la sicurezza delle informazioni
- Politica sui Conflitti di Interesse
- Politica di Operatività Infragruppo
- Politica degli Investimenti
- Politica relativa al Sistema di Controllo Interno
- Procedura di Gestione dei Progetti Rilevanti
- Procedura di Gestione dei Processi e delle Procedure.