MOGC - PARTE GENERALE
Modello di Organizzazione Gestione e Controllo
(ai sensi del D.lgs.231/01)

Cloud Care S.p.A.

Sede legale e operativa:
Corso della Vittoria, 31/A 28100 Novara

Sedi operative:
Via Amsterdam, 125 00144 Roma
Via Edward Jenner, 19/21 09121 Cagliari

vers./rev.	del	oggetto della revisione	approvato da
0/0	20/07/2023	Prima emissione	C.d.A. del 28/07/2023
0/1	31/12/2023	Aggiornamento Paragrafi 4.10 e 2.3	

INDICE

1. INTRODUZIONE

Il Decreto Legislativo 8 giugno 2001, n. 231, “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell’art. 11 della legge 29 settembre 2000, n. 300” (di seguito anche “D.lgs.231”), ha introdotto nell’ordinamento italiano la responsabilità amministrativa degli Enti nel caso di reati commessi dai propri dirigenti, amministratori o dipendenti in favore e a beneficio dell’ente stesso.

La portata innovativa del D.lgs.231 risiede nel fatto che possono subire le conseguenze punitive tipiche del reato sia la persona fisica che ha materialmente posto in essere l’illecito sia la persona giuridica che ha un interesse nella condotta illecita o ne ha tratto un vantaggio e per conto della quale il soggetto ha agito.

L'esclusione dalla responsabilità amministrativa dell'ente avviene nel caso in cui il reato sia stato commesso nell'esclusivo interesse proprio o di terzi o se l’ente dimostri di aver adottato ed efficacemente attuato un “Modello di organizzazione e gestione” idoneo a prevenire la commissione di reati.

Di contro, qualora venga perpetrato un reato contemplato dal D.lgs.231 e la Società non sia in grado di dimostrare di aver adottato ed efficacemente attuato il Modello di Organizzazione, Gestione e Controllo, si esporrà al rischio di essere destinataria di sanzioni di natura pecuniaria e interdittiva.

Il Modello di Organizzazione Gestione e Controllo (di seguito MOGC) adottato da Cloud Care S.p.A. (d'ora in avanti Cloud Care) è strutturato nella presente Parte Generale e in una Parte Speciale.

Il presente documento ha il duplice scopo di descrivere il quadro normativo di riferimento illustrando gli elementi principali del D.lgs.231 e il Modello di Organizzazione, Gestione e Controllo adottato da Cloud Care S.p.A. ai sensi del decreto stesso.

La Parte Speciale descrive i reati considerati rilevanti per Cloud Care, i processi aziendali e le corrispondenti attività sensibili per la Società ai sensi del D.lgs.231, ovvero a rischio di reato, le misure di controllo interno a presidio delle suddette attività, le regole di condotta e i divieti.

Oltre a quanto di seguito espressamente stabilito, costituiscono inoltre parte integrante del MOGC:

- Il risk assessment finalizzato all’individuazione delle attività sensibili, qui integralmente richiamato e agli atti della Società;
- il Codice Etico che definisce i principi e le norme di comportamento aziendale;
- Il sistema privacy ai sensi del GDPR 679/16
- tutte le disposizioni, le policy, i provvedimenti interni, i documenti del Sistema di Gestione integrato ISO 9001, ISO 14001, ISO 45001, ISO 27001, PAS 24000, gli atti e le procedure operative aziendali che di questo documento costituiscono attuazione (es. poteri, organigrammi, statuto).

Nel dettaglio il contenuto della presente Parte Generale:

- Elementi del dettato normativo di riferimento ed aspetti caratterizzanti i Modelli di Organizzazione, Gestione e Controllo;
- Il modello di governance aziendale e il MOGC adottato da Cloud Care;
- I destinatari del MOGC: sono censiti i consegnatari dei doveri, obblighi e prescrizioni contenute ed emanate dal presente MOGC;
- L'organismo di vigilanza del MOGC: dettaglia l’istituto dell’OdV e le regole generali che ne disciplinano l’operato;
- I sistemi di controllo preventivi predisposti per impedire la commissione di reati: contiene una panoramica descrizione dei protocolli dettagliati nella Parte Speciale;
- I sistemi di controllo successivi. Sistema disciplinare e meccanismi sanzionatori;
- Meccanismi di aggiornamento e revisione del MOGC finalizzati a garantirne l’adeguatezza nel tempo.

2. IL DECRETO LEGISLATIVO 231/2001

Il D.lgs.231, emanato in esecuzione della delega di cui all'art. 11 della Legge 300/2000, precedentemente citata, è entrato in vigore il 4 luglio successivo, al fine di adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l'Italia aveva già da tempo aderito, quali la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione - anch'essa firmata a Bruxelles il 26 maggio 1997 - sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

Il D. Lgs 231 rappresenta una svolta epocale nella concezione del nostro ordinamento giuridico fondato sul principio costituzionale sancito nell'art. 27 "*la responsabilità penale è personale*" da cui l'assunto "*societas delinquere non potest*", introducendo, con la responsabilità dell'ente, un "*tertium genus*" caratterizzato dai seguenti elementi:

- è conseguente ad una condotta da reato (**reato presupposto**) commesso nell'interesse o vantaggio dell'ente;
- prevede sanzioni severe tipiche della responsabilità penale, di natura pecuniaria e interdittiva;
- è esclusiva del soggetto collettivo (art. 8 D.lgs.231/01 - Autonomia della responsabilità dell'ente);
- è aggiuntiva alla responsabilità dell'autore del reato presupposto, ma rimane autonoma da esso;
- l'autore persona fisica del reato appartiene alla compagine societaria.

I punti cardine del D.lgs.231 sono i seguenti:

- l'individuazione dei soggetti che, agendo nell'interesse o vantaggio della persona giuridica, abbiano commesso un reato e, conseguentemente, possano determinare la responsabilità amministrativa/penale dell'ente;
- la tipologia degli illeciti per i quali (**e solo per essi**) ricorre la responsabilità della persona giuridica;
- l'apparato sanzionatorio a carico delle persone giuridiche;
- i casi di esclusione della responsabilità della persona giuridica.

In altre parole, la responsabilità prevista dal D.lgs.231 a carico dell'Ente scatta qualora:

- sia stato commesso un reato presupposto richiamato dal D.lgs.231;
- l'autore del reato presupposto sia riconducibile ad uno dei soggetti di cui all'art.5;
- il reato sia commesso nell'interesse o a vantaggio dell'ente.

Nella decodificazione di tali criteri di imputazione, l'aspetto attualmente più controverso attiene all'interpretazione dei termini "**interesse**" e "**vantaggio**".

I criteri di imputazione oggettiva dell'interesse o vantaggio, sono **alternativi** e **concorrenti** tra loro:

- il **criterio dell'interesse** esprime una valutazione teleologica del reato, apprezzabile **"ex ante"**, cioè al momento della commissione del fatto e secondo un metro di giudizio marcatamente soggettivo;
- il **vantaggio** ha una connotazione essenzialmente oggettiva, come tale valutabile **"ex post"**, sulla base degli effetti concretamente derivati dalla realizzazione dell'illecito (*Cassazione penale, SS.UU., 24.04.2014, n. 38343*).

Se l'interesse si riferisce alla sfera volitiva della persona fisica che agisce ed è valutabile al momento della condotta, ne deriva che la persona fisica non deve aver agito contro l'impresa. Se ha commesso il reato nel suo interesse personale, affinché l'ente sia responsabile, è necessario che tale interesse sia almeno in parte coincidente con quello dell'impresa (*cfr. anche Cass., V Sez. pen., Sent. n. 40380 del 2012*).

Di contro, il vantaggio si caratterizza come complesso dei benefici - soprattutto di carattere patrimoniale - tratti dal reato, che può valutarsi successivamente alla commissione di quest'ultimo (*Cass., II Sez. pen., Sent. n. 3615 del 2005*).

Il problema di compatibilità del criterio dell'interesse o vantaggio si è posto nel momento in cui il catalogo dei reati-presupposto è stato esteso per includervi quelli "colposi" sia in materia di salute e sicurezza sul lavoro (art. 25 septies) che ambientale (art. 25 undecies).

Viene, difatti, ad esempio, ritenuta sussistente la responsabilità se si ricava oggettivamente vantaggio sotto forma di risparmio di spese o di massimizzazione della produzione, indipendentemente dalla volontà di ottenere il vantaggio stesso (*Cass. Pen. Sez.4^, n. 38363 del 23.05.2018, Consorzio Melinda, S.c.a., Rv274320*); se, nei reati di mera condotta, il risparmio economico per l'ente è determinato dalle mancate adozioni di impianti o dispositivi idonei a prevenire il superamento dei limiti tabellari o dalla sola riduzione dei tempi di lavorazione (*Cass. Pen. Sez.4^, Sent. del 24.01.2019, n.16598, Tecchio, Rv.275570*).

I concetti di interesse e di vantaggio individuabili, dunque, anche **nella commissione di reati colposi d'evento**, **vanno riferiti alla mera condotta e non all'esito antigiuridico**. Vi può essere, quindi, perfetta compatibilità tra l'inosservanza di una prescrizione cautelare e l'esito vantaggioso per l'ente.

2.1 Individuazione dei soggetti che possono commettere il reato (art. 5 D.lgs.231)

Il D.lgs.231 distingue tra:

- **soggetto in posizione c.d. apicale**, ossia una persona che riveste funzioni di rappresentanza, amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persona fisica che esercita, anche di fatto, la gestione e il controllo dell'Ente medesimo.
- **soggetto c.d. subordinato**, ossia una persona sottoposta alla direzione o alla vigilanza di un soggetto in posizione apicale.

In particolare, se il **reato è commesso da un soggetto apicale**, **l'ente è responsabile se non dimostra che**:

- ha adottato. ma anche efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e gestione idonei a impedire reati della specie di quello commesso (art. 6, comma 1, lett. a, D.lgs.231);
- ha istituito un organismo dotato di autonomi poteri di iniziativa e controllo, il quale abbia effettivamente vigilato sull'osservanza dei modelli;
- il reato è stato commesso per fraudolenta elusione dei modelli da parte del soggetto apicale infedele.

Quando il **reato è commesso da un soggetto subordinato**, **la pubblica accusa deve provare** che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza da parte degli apicali.

Questi obblighi non possono ritenersi violati se prima della commissione del reato l'ente abbia adottato ed efficacemente attuato un modello idoneo a prevenire reati della specie di quello verificatosi.

L'efficace attuazione del modello richiede, in via principale (cfr. par. 2.5):

a) una **verifica periodica** e l'eventuale **modifica** dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;
b) un **sistema disciplinare** idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
c) **adeguate iniziative di formazione e informazione** del personale.

2.2 Autonomia della responsabilità dell'ente (art. 8 D.lgs.231)

La disposizione dell'art. 8 chiarisce in modo inequivocabile come quello dell'ente sia un titolo autonomo di responsabilità, anche se presuppone comunque la commissione di un reato.

Se infatti il meccanismo punitivo è stato congegnato in modo tale da rendere le vicende (processuali) delle persone fisiche e quelle dell'ente tra loro strettamente correlate (il simultaneus processus risponde non soltanto ad esigenze di economia, ma anche alla necessità di far fronte alla complessità dell'accertamento), ciò non toglie che in talune limitate ipotesi, l'inscindibilità tra le due possa venir meno. Ciò è ormai confermato da una giurisprudenza consolidata, che afferma sempre di più come la responsabilità dell'ente sia ritenuta autonoma

e distinta rispetto a quella della persona fisica che abbia posto in essere il reato presupposto (*Cass.pen. 3^sez., 28.02,2018, n.9072*).

In questa logica, anche le cause di esclusione della punibilità per particolare tenuità del fatto ex art.131bis c.p., pur se riconosciute applicabili in capo alla persona fisica che, per posizione apicale o per poteri riconosciuti, abbia agito in nome dell'ente, non potranno avere effetto in relazione alla responsabilità dell'ente. Difatti, all'ente viene rimproverata e sanzionata la "**colpa di organizzazione**", essendo il reato unicamente la "premessa storica" della responsabilità amministrativa ex D.lgs.231 (*Cass. Pen. 3^ sez., 15.01.2020, n.1420*).

Parimenti, si ritiene che la causa di non punibilità prevista per alcuni reati di omesso versamento e di natura dichiarativa ed estesa ai reati di cui agli artt.2 e 3 D.lgs. n.74/2000 (con il D.L.n.124 del 26.10.2019 cd. Decreto Fiscale 2020, convertito con L.n.157 del 19.12.2019, anche i reati tributari sono rientrati nel novero dei reati presupposto ex art.25 quinquiesdecies D.lgs.231) riconosca, infatti, che il contribuente possa accedere all'istituto premiale cd. resipiscenza volontaria (voluntary disclosure), ma ciò non possa trovare applicazione in favore dell'ente.

2.3 Fattispecie di reati determinanti la responsabilità dell'ente ai sensi del D.lgs.231

Non tutti i reati commessi dai soggetti di cui al citato art. 5 implicano la responsabilità amministrativa dell'ente, ma occorre la commissione di uno dei reati-presupposto (…della responsabilità dell'ente) indicati in via tassativa dal D.lgs.231 negli artt. 24 e seguenti.

Si riportano a seguire, a titolo informativo, tutte le fattispecie di reato cui è riconducibile la responsabilità dell'Ente, ai sensi del D.lgs.231, alla data di approvazione del presente MOGC.

Si rimanda alla Parte Speciale per il dettaglio dei reati che, in seguito all'analisi dei rischi, sono stati ritenuti applicabili alla specifica realtà di CLOUD CARE e per i quali sono stati definiti opportuni protocolli di mitigazione del rischio.

Art. 24, D.lgs.n. 231/01 - Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture

- Malversazione a danno dello Stato (art. 316-bis c.p.)
- Indebita percezione di erogazioni a danno dello Stato (art.316-ter c.p.)
- *Turbata libertà degli incanti (art. 353 c.p.)*
- *Turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.)*
- Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art.640, comma 2, n.1, c.p.)
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)
- Frode informatica in danno 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 di garanzia e del Fondo europeo agricolo per lo sviluppo rurale (art. 2 L. 898/1986)

Art. 24-bis, D.lgs.n. 231/2001 - Delitti informatici e trattamento illecito di dati

- Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.)
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
- Installazione di apparecchiature atte ad intercettare, impedire 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.)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)
- Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)

- Fattispecie in materia di perimetro di sicurezza nazionale cibernetica (Art. 1, comma 11, D.L. 105/19)

Art. 24-ter, D.lgs.n. 231/2001 - Delitti di criminalità organizzata

- Associazione per delinquere (art. 416 c.p.p.)
- Associazione di tipo mafioso (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 DPR 9 ottobre 1990, n. 309)
- Tutti i delitti se commessi avvalendosi delle condizioni previste dall´art. 416-bis c.p. per agevolare l'attività delle associazioni previste dallo stesso articolo (L. 203/91)
- Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (art. 407, co. 2, lett. a), numero 5), c.p.p.)

Art. 25 D.lgs.n. 231/2001 - Peculato, concussione, induzione indebita a dare o promettere altre utilità, corruzione e abuso d'ufficio

- Concussione (art. 317 c.p.)
- Corruzione per l'esercizio della funzione (art. 318 c.p.) [articolo modificato dalla L. n. 190/2012]
- Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.)
- Circostanze aggravanti (art. 319-bis c.p.)
- Corruzione in atti giudiziari (art. 319-ter c.p.)
- Induzione indebita a dare o promettere utilità (art. 319-quater) [articolo aggiunto dalla L. n. 190/2012]
- Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)
- Pene per il corruttore (art. 321 c.p.)
- Istigazione alla corruzione (art. 322 c.p.)
- Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.) [articolo modificato dalla L. n. 190/2012]
- Peculato, peculato mediante profitto dell'errore altrui, abuso di ufficio (artt. 314, comma 1, 316, 323 c.p.), nelle sole ipotesi in cui il reato offenda gli interessi finanziari dell'Unione Europea.
- Traffico di influenze illecite (art. 346 bis c.p.)

Art. 25-bis D.lgs.n. 231/2001 - Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.)
- Alterazione di monete (art. 454 c.p.)
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.)
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.)
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.)
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.)
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.)
- Uso di valori di bollo contraffatti o alterati (art. 464 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.)

Art. 25-bis.1 D.lgs. n. 231/2001 - Delitti contro l'industria e il commercio

- 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)
- 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.)

Art. 25-ter D.lgs. n. 231/2001 - Reati societari

- False comunicazioni sociali (art. 2621 c.c.)
- Fatti di lieve entità (art. 2621 bis c.c.)
- False comunicazioni sociali delle società quotate (art. 2622 c.c.)
- Impedito controllo (art. 2625, comma 2, c.c.)
- Indebita restituzione di conferimenti (art. 2626 c.c.)
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
- Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.) [aggiunto dalla legge n. 262/2005]
- Formazione fittizia del capitale (art. 2632 c.c.)
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)
- Corruzione tra privati (art. 2635 c.c.) [aggiunto dalla legge n. 190/2012]
- Illecita influenza sull'assemblea (art. 2636 c.c.)
- Aggiotaggio (art. 2637 c.c.)
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.)

Art. 25-quater D.lgs. n. 231/2001 - Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali

- Associazioni sovversive (art. 270 c.p.)
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270 bis c.p.)
- Assistenza agli associati (art. 270 ter c.p.)
- Arruolamento con finalità di terrorismo anche internazionale (art. 270 quater c.p.)
- Organizzazione di trasferimento per finalità di terrorismo (art. 270 quater.1 c.p.)
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270 quinquies c.p.)
- Finanziamento di condotte con finalità di terrorismo (art. 270 quinquies.1 c.p.)
- Sottrazione di denaro o beni sottoposti a sequestro (art. 270 quinquies.2 c.p.)
- Condotte con finalità di terrorismo (art. 270 sexies c.p.)
- Attentato per finalità terroristiche o di eversione (art. 280 c.p.)
- Atto di terrorismo con ordigni micidiali o esplosivi (art. 280 bis c.p.)
- Atti di terrorismo nucleare (art. 280 ter c.p.)
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289 bis c.p.)
- Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo (art. 302 c.p.)
- Cospirazione politica mediante accordo (art. 304 c.p.)
- Cospirazione politica mediante associazione (art. 305 c.p.)
- Banda armata: formazione e partecipazione (art. 306 c.p.)
- Assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.)
- Impossessamento, dirottamento e distruzione di un aereo (L. n. 342/1976, art. 1)
- Danneggiamento delle installazioni a terra (L. n. 342/1976, art. 2)
- Sanzioni (L. n. 422/1989, art. 3)
- Pentimento operoso (D.lgs. n. 625/1979, art. 5)
- Convenzione di New York del 9 dicembre 1999 (art. 2)

Art. 25-quater.1 D.lgs. n. 231/2001 - Pratiche di mutilazione degli organi genitali femminili

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

Art. 25-quinquies D.lgs. n. 231/2001 - Delitti contro la personalità individuale

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)
- Prostituzione minorile (art. 600-bis c.p.)
- Pornografia minorile (art. 600-ter c.p.)
- Detenzione di materiale pornografico (art. 600-quater)
- Pornografia virtuale (art. 600-quater.1 c.p.) [aggiunto dall'art. 10, L. 6 febbraio 2006 n. 38]
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.)
- Tratta di persone (art. 601 c.p.)
- Acquisto e alienazione di schiavi (art. 602 c.p.)
- Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)
- Adescamento di minorenni (art. 609-undecies)

Art. 25-sexies D.lgs. n. 231/2001 - Reati di abuso di mercato

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

Art. 25-septies D.lgs. n. 231/2001 - Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

- Omicidio colposo (art. 589 c.p.)
- Lesioni personali colpose (art. 590 c.p.)

Art. 25-octies D.lgs. n. 231/2001 - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio

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

Art. 25-octies.1 D.lgs. n. 231/2001 - Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.)
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.)
- *Trasferimento fraudolento di valori (art. 512-bis c.p.)*
- Frode informatica (art. 640-ter c.p.)
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)

Art. 25-novies D.lgs. n. 231/2001 - Delitti in materia di violazione del diritto d'autore

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- 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 legge n.633/1941 comma 2)
- 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 legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

Art. 25-decies D.lgs. n. 231/2001 - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

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

Art. 25-undecies D.lgs.n. 231/2001 - Reati ambientali

- 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.)
- Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. n.150/1992, art. 1 e art. 2)

- 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 od aeromobili (D. Lgs n.152/2006, art. 137)
- Attività di gestione di rifiuti non autorizzata (D. Lgs n.152/2006, art. 256)
- Traffico illecito di rifiuti (D. Lgs n.152/2006, art. 259)
- Attività organizzate per il traffico illecito di rifiuti (D. Lgs n.152/2006, art. 260)
- Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (D. Lgs n. 152/2006, art. 257)
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D. Lgs n.152/2006, art. 258)
- 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 nel trasporto di rifiuti (D. Lgs n.152/2006, art. 260-bis)
- Inquinamento doloso provocato da navi (D.lgs. n.202/2007, art. 8)
- Inquinamento colposo provocato da navi (D.lgs. n.202/2007, art. 9)
- Inquinamento ambientale (art. 452 c.p.)
- Disastro ambientale (art. 452 quater c.p.)
- Circostanze aggravanti (art. 452-octies c.p.)
- Delitti colposi contro l'ambiente (art. 452-quinquies c.p.)
- Traffico e abbandono di materiale ad alta radioattività (Art. 452-sexies c.p.)

Art. 25-duodecies, D.lgs. n. 231/2001 - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare

- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 12, commi 3, 3-bis, 3-ter, 5, art. 22 comma 12 bis, D.lgs. n. 286/1998)

Art. 25 terdecies D.lgs. n. 231/2001 - Razzismo e Xenofobia

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

Art. 25-quaterdecies D.lgs. 231/2001 - Frode in competizioni sportive () [articolo aggiunto dalla L. n. 39/2019]

Art. 25-quinquiesdecies, D.lgs. 231/2001 - Reati tributari

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2 del decreto legislativo 10 marzo 2000 n.74
- Dichiarazione fraudolenta mediante altri artifici, ex art. 3 del D.Lgs 74/00;
- Emissione di fatture o altri documenti per operazioni inesistenti, ex art. 8 D.Lgs 74/00;
- Occultamento o distruzione di documenti contabili, ex art. 10 D.Lgs 74/00;
- Indebita compensazione, ex art. 10 quater D.lgs.74/00;
- Sottrazione fraudolenta al pagamento di imposte, ex art. 11 del D.lgs. 74/00;
- Dichiarazione infedele (in caso di gravi frodi IVA transfrontaliere, art. 4 D.lgs. 74/200)
- Omessa dichiarazione (in caso di gravi frodi IVA transfrontaliere, art. 5 D.lgs. 74/200)
- Indebita compensazione (in caso di gravi frodi IVA transfrontaliere, art. 10 quater D.lgs. 74/200)

Art. 25-sexiesdecies D.Lgs 231/2001 - Reati di contrabbando

Art.25-septiesdecies D.lgs.231/2001 - Delitti contro il patrimonio culturale

- Furto di beni culturali (art. 518-bis c.p.)
- Appropriazione indebita di beni culturali (art. 518-ter c.p.)
- Ricettazione di beni culturali (art. 518-quater c.p.)
- Falsificazione in scrittura privata relativa a beni culturali (art. 518-octies c.p.)
- Violazioni in materia di alienazione di beni culturali (art. 518-novies c.p.)
- Importazione illecita di beni culturali (art. 518-decies c.p.)
- Uscita o esportazione illecite di beni culturali (art. 518-undecies c.p.)
- Distruzione, dispersione, deterioramento, deturpamento (art. 518-duodecies c.p.)
- Contraffazione di opere d'arte (art. 518-quaterdecies c.p.)

Art.25-duodevicies D.lgs.231/20001 - Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici

- Riciclaggio di beni culturali (art. 518-sexies c.p.)
- Devastazione e saccheggio di beni culturali e paesaggistici (art. 518-terdecies c.p.)

L. n. 146/2006 Reati transnazionali Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in ambito transnazionale

- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5, del testo unico di cui al D.lgs.25 luglio 1998, n. 286)
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al D.P.R. 9 ottobre 1990, n. 309)
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al D.P.R. 23 gennaio 1973, n. 43)
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)
- Favoreggiamento personale (art. 378 c.p.)
- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso (art. 416-bis c.p.)

2.3.1 Reati commessi all'estero

Ai sensi dell'art. 4 del D.lgs.231, l'ente può essere chiamato a rispondere in Italia di reati presupposto commessi all'estero.
Il Decreto, tuttavia, subordina questa possibilità alle seguenti condizioni:

- che non proceda lo Stato del luogo in cui è stato commesso il reato;
- che la società abbia la propria sede principale nel territorio dello Stato italiano;
  che il reato sia stato commesso all'estero da un soggetto funzionalmente legato alla società;
  che sussistano le condizioni generali di procedibilità previste dagli articoli 7, 8, 9, 10 del codice penale per poter perseguire in Italia un reato commesso all'estero.

2.4 Apparato sanzionatorio

Le sanzioni previste a carico degli enti a seguito della commissione o tentata commissione dei reati sopra menzionati sono:

1. **sanzioni pecuniarie**: applicate per quote (da un minimo di 100 ad un massimo di 1000);
2. **sanzioni interdittive** (applicabili anche come misure cautelari) consistenti in:
   - interdizione dall'esercizio dell'attività;
   - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
   - divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
   - esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli concessi;
   - divieto di pubblicizzare beni o servizi;
   - esclusione dalla partecipazione a procedure di affidamento delle concessioni e degli appalti di lavori, forniture e servizi e procedure di affidamento di subappalti (art. 80 c.5 lett. f D.lgs.50/2016);
3. **confisca e sequestro preventivo del profitto del reato;**
4. **pubblicazione della sentenza.**

2.4.1 Sanzione amministrativa pecuniaria (artt. 10, 11, 12 D.lgs.231)

Per l'illecito amministrativo dipendente da reato si applica sempre la sanzione pecuniaria.

Nella definizione della sanzione pecuniaria il giudice stabilisce un **numero di quote** entro un intervallo, previsto dalla legge per ogni fattispecie di reato, compreso **tra 100 e 1000 quote**. L'importo di una **quota va da un minimo di euro 258,00 ad un massimo di euro 1.549,00.**

Il **numero di quote viene determinato dal giudice** in funzione dei seguenti elementi:

- gravità fatto;
- grado di responsabilità dell'ente;
- attività svolta dall'ente per eliminare o attenuare le conseguenze del fatto e prevenire la commissione di ulteriori illeciti;
- condizioni economiche e patrimoniali dell'ente (efficacia della sanzione).

La sanzione pecuniaria è ridotta della metà (con limite massimo 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 vantaggio o ne ha ricavato un vantaggio minimo;

- il danno patrimoniale cagionato è di particolare tenuità;

La sanzione è 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 comunque efficacemente adoperato in tal senso;
- è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

Nel caso in cui concorrano entrambe le condizioni previste precedentemente, la sanzione è ridotta dalla metà ai due terzi.
In ogni caso, la sanzione pecuniaria non può essere inferiore a euro 10.329,00.

2.4.2 Sanzioni interdittive (artt. 9, 13, 14 D.lgs.231)

Le **sanzioni interdittive** si applicano in relazione ai reati per le quali siano **espressamente previste** dal D.lgs.231 ed hanno ad oggetto la specifica attività alla quale si riferisce l'illecito commesso nell'interesse e vantaggio dell'ente.

Essendo la sanzione interdittiva una **misura di estrema gravità** per l'organizzazione, la **legge ne subordina l'applicazione al ricorrere di almeno una delle seguenti condizioni**:

- **l'ente ha tratto dal reato un profitto di rilevante entità** e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione e vigilanza quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
- in caso di **reiterazione degli illeciti**. Si ha reiterazione quando l'ente, già condannato in via definitiva almeno una volta per un illecito dipendente da reato, ne commette un altro nei cinque anni successivi alla condanna definitiva.

Il giudice ne determina il tipo e la durata sulla base dei criteri indicati all'art. 11 per la determinazione delle sanzioni pecuniarie, tenendo anche conto dell'idoneità delle singole sanzioni a prevenire illeciti del tipo di quello commesso.

Mentre il divieto di contrattare con la pubblica amministrazione può anche essere limitato a determinati tipi di contratto o a determinate amministrazioni, l'interdizione dall'esercizio di un'attività comporta la sospensione ovvero la revoca delle autorizzazioni, licenze o concessioni funzionali allo svolgimento dell'attività.

L'interdizione dall'esercizio dell'attività si applica soltanto quando l'irrogazione di altre sanzioni interdittive risulti inadeguata.

Le sanzioni interdittive possono essere applicate congiuntamente.

Qualora sussistano i presupposti per l'applicazione di una sanzione interdittiva che determini l'interruzione dell'attività dell'ente, **il giudice potrebbe disporre**, al posto dell'applicazione dell'interdizione, la prosecuzione dell'attività dell'ente da parte di un **commissario** per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata. Questo avviene se ricorre almeno una delle seguenti condizioni:

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

Nell'ambito dei compiti e dei poteri indicati dal giudice, il commissario cura l'adozione e l'efficace attuazione dei modelli di organizzazione e di controllo idonei a prevenire reati della specie di quello verificatosi.

Il **profitto derivante dalla prosecuzione dell'attività viene confiscato**.

La prosecuzione dell'attività da parte del commissario non può essere disposta quando l'interruzione dell'attività consegua all'applicazione in via definitiva di una sanzione interdittiva.

Nel caso in cui l'ente o una sua unità organizzativa venga stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di reati in relazione ai quali è prevista la sua responsabilità, è sempre

disposta l'interdizione definitiva dall'esercizio dell'attività e non si applicano le disposizioni previste per la riparazione delle conseguenze da reato.

Tali risarcimenti, infatti, ferma restando l'applicazione delle sanzioni pecuniarie, consentono la non assegnazione delle sanzioni interdittive quando, prima della dichiarazione di apertura del dibattimento di primo grado, concorrano le seguenti condizioni:

- l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;
- l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi;
- l'ente ha messo a disposizione il profitto conseguito ai fini della confisca.

Quando nei confronti dell'ente viene applicata una sanzione interdittiva può essere disposta la pubblicazione della sentenza di condanna che dovrà avvenire ai sensi dell'articolo 36 del Codice penale, nonché mediante affissione nel comune ove l'ente ha la sede principale.

La pubblicazione della sentenza è eseguita, a cura della cancelleria del giudice, a spese dell'ente.

L'art. 26 del D.lgs. 231 prevede che, qualora venga impedito volontariamente il compimento dell'azione o la realizzazione dell'evento, l'ente non incorra in alcuna responsabilità. In tal caso, infatti, l'esclusione della responsabilità e delle sanzioni conseguenti si giustifica **in forza dell'interruzione di ogni rapporto di immedesimazione tra ente e soggetti che assumono di agire in suo nome e per suo conto**.

2.4.3 Confisca (art. 19 D.lgs.231)

Nei confronti dell'ente è sempre disposta, con la sentenza di condanna, **la confisca del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato**. Sono fatti salvi i diritti acquisiti dai terzi in buona fede.

Quando non è possibile eseguire la confisca, **la stessa può avere ad oggetto somme di denaro, beni o altre utilità** di valore equivalente al prezzo o al profitto del reato.

2.5 I casi di esclusione della responsabilità della persona giuridica (artt. 6 e 7 D.lgs.231)

Il D.lgs.231 prevede specifiche forme di esonero della responsabilità amministrativa dell'ente.

In particolare, l'articolo 6 c.1 stabilisce che, in caso di un reato commesso da un soggetto apicale (art. 5 c. 1 lett.a), l'ente non risponde qualora sia in grado di dimostrare che:

a) l'organo dirigente **ha adottato ed efficacemente attuato**, prima della commissione del fatto, **modelli di organizzazione e gestione idonei a prevenire reati della specie di quello verificatosi**;
b) il **compito di vigilare** sul funzionamento, sull'efficacia e l'osservanza dei modelli nonché di curare il loro aggiornamento **è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo (OdV);**
c) le persone che hanno commesso il reato **hanno agito eludendo fraudolentemente** i suddetti modelli di organizzazione e gestione;
d) **non vi sia stata omessa o insufficiente vigilanza** da parte dell'organismo preposto.

Sussiste in capo all'ente una presunzione di responsabilità dovuta al fatto che i soggetti apicali esprimono e rappresentano la politica e quindi la volontà dell'ente stesso.

Tale presupposto può essere superato se l'ente riesce a dimostrare la sussistenza delle condizioni sopra riportate.

In tal caso, pur sussistendo la responsabilità personale in capo al soggetto apicale, l'ente non è responsabile ai sensi del D.lgs. 231.

Lo stesso art. 6 al c.2 definisce **a quali esigenze debbano rispondere i modelli di organizzazione e gestione affinché abbiano efficacia esimente**:

a) **individuare le attività** nel cui ambito possano essere commessi i reati;

b) **prevedere specifici protocolli** diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
c) individuare la **modalità di gestione delle risorse finanziarie** idonee ad impedire la commissione dei reati;
d) prevedere **obblighi di informazione nei confronti dell'organismo deputato a vigilare** sul funzionamento e l'osservanza del modello;
e) introdurre un **sistema disciplinare** idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Ai sensi dell'art. 7, commi 3 e 4, sono poi definiti **ulteriori elementi di validità del modello**, in termini di efficacia esimente per i reati commessi da entrambi i soggetti dell'art. 5 ovvero:

- il modello deve prevedere, in relazione alla natura dell'organizzazione, alla sua dimensione ed al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio;
- per essere efficacemente attuato il modello deve prevedere una verifica periodica e l'eventuale modifica dello stesso qualora siano scoperte significative violazioni delle prescrizioni o quando intervengano mutamenti organizzativi o dell'attività.

L'articolo 7 del D.lgs.231, inoltre, regola la **responsabilità amministrativa dell'ente per i reati commessi da soggetti subordinati** (art. 5 c.1 lett.b), ovvero dalle persone sottoposte alla direzione o vigilanza di uno dei soggetti "apicali" individuati all'art. 5 c. 1 lett. a).
In questo caso, dal combinato disposto dei commi 1 e 2 dell'art. 7, **l'ente sarà chiamato a rispondere solo nell'ipotesi in cui il reato sia stato reso possibile dall'inosservanza degli obblighi di direzione e vigilanza**. Tale inosservanza, come già precedentemente riportato, è in ogni caso esclusa se, prima della commissione del reato, l'ente abbia adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire i reati della specie di quello verificatosi.

3. IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO DI CLOUD CARE S.P.A.

3.1 Cloud Care S.p.A.

Cloud Care S.p.A. (di seguito anche Cloud Care) è un'azienda leader nei servizi digitali per le Web Sales con soluzioni avanzate di Chat & Contact Center e Customer Base Management.

Cloud Care è nata nel 2011 per volontà del fondatore Andrea Conte, negli anni si è imposta sul mercato attraverso un percorso in continua ascesa, rafforzando competenze tecnologiche, organizzazione, business e reputazione.

Nel 2021 Cloud Care S.p.A. entra a far parte della Investcorp Holdings B.S.C. attraverso la CloudCare Topco limited, socio unico della CloudCare Bidco S.r.l. la quale possiede circa il 70% delle azioni della Cloud Care S.p.A., il fondatore Andrea Conte detiene il 30% delle azioni ed è CEO della Società.

Cloud Care attualmente ha sedi a Novara, Milano, Roma e Cagliari e occupa circa 115 dipendenti e 780 collaboratori.

Possiede, in qualità di socio unico, Comparasemplice Broker S.r.l., Alipax S.r.l., Spin Up S.r.l. (che a sua volta detiene il 100% di Rewave S.r.l.), Assicurofacile S.r.l e una quota di partecipazione di maggioranza nella società Affida S.r.l.

Le due linee principali di business di Cloud Care sono:

B2C Comparasemplice
Attraverso la piattaforma proprietaria di comparazione ComparaSemplice.it l'azienda è leader delle Web Sales del settore utility Gas&Power e TLC, combinando Sales Force, CRM e Marketing Online.

B2B Business Process Digitalization
Offre servizi, strumenti e competenze per sviluppare processi digitali dedicati al Customer Journey con supporto Chat e AI.

L'offerta di Cloud Care si articola in un sistema di Customer Relationship Management proprietario, sviluppato internamente ed alimentato da un ampio database, una piattaforma di customer service supportata da Intelligenza Artificiale e un approccio end-to-end per la generazione di leads di vendita e la massimizzazione della conversione, attraverso la piattaforma multicanale proprietaria.

Negli anni Cloud Care ha costantemente investito in tecnologia e risorse e dal 2020 ha implementato un Sistema di Gestione Integrato per la Qualità, l'Ambiente, la Salute e Sicurezza dei Lavoratori, la Sicurezza dei dati e delle informazioni e la Responsabilità Sociale d'impresa, certificato secondo le norme ISO 9001, ISO 14001, ISO 45001, ISO 27001 e PAS 24000.

Le procedure del Sistema Integrato sono condivise con tutto il personale, dipendenti e collaboratori, definendo modalità operative e prassi di lavoro che garantiscono la soddisfazione dei clienti nel rispetto di leggi e regolamenti, della sicurezza e dignità dei lavoratori, dell'ambiente e assicurando la sicurezza di tutti i dati e informazioni gestite.

3.2 Il Modello di Governance

La maggioranza delle azioni di Cloud Care sono detenute dalla CloudCare Bidco S.r.l. la quale è partecipata al 100% dalla CloudCare Topco limited (entrambe società della Investcorp Holdings S.B.C.) che esercita la direzione e il coordinamento della Cloud Care S.p.A.

Attraverso Cloud Care S.p.A. controlla anche le società Comparasemplice Broker S.r.l., Alipax S.r.l., Spin Up S.r.l., Rewave S.r.l., Affida S.r.l., Assicurofacile S.r.l.

Cloud Care S.p.A. è un ente giuridicamente autonomo e distinto dalla controllante e dalla Holding Investcorp anche se sottoposta alla direzione e al coordinamento di quest'ultima.

Investcorp Holdings B.S.C. è un gestore di investimenti alternativi, leader a livello mondiale, che opera con sei linee di attività: private equity, immobiliare, investimenti a rendimento assoluto, infrastrutture, gestione del credito e capitale strategico. In particolare, in Europa, investe, attraverso proprie controllate, in società di medie

dimensioni che presentano, come Cloud Care, un forte potenziale di crescita, un solido flusso di cassa, un posizionamento di rilievo nel settore di appartenenza, una ottima gestione e competenza, preferibilmente in settori tecnologici. Il modello post-acquisizione di Investcorp è strutturato in modo da fornire supporto e supervisione alle controllate utilizzando le proprie competenze finanziarie, operative e strategiche nelle diverse linee di attività.

In questa ottica, la direzione ed il coordinamento di Investcorp nei confronti di Cloud Care S.p.A. e quindi delle società appartenenti al gruppo si sviluppa secondo un duplice orientamento, da un lato con la definizione di obiettivi strategici comuni per Cloud Care S.p.A. e le società controllate, in modo tale da garantire l'unicità di visione, assicurare la continuità aziendale nel lungo periodo e la conservazione delle competenze chiave, dall'altro esercitare un continuo orientamento e monitoraggio delle performance delle società, il rispetto degli standard e degli obiettivi definiti, così da essere in grado di prevenire o rimediare a situazioni che ne possano minare la stabilità e la reputazione a causa di comportamenti non allineati con le policy del gruppo.

In particolare, la direzione e il coordinamento si esplicano attraverso

- condivisione di una unica cultura aziendale ed organizzativa tra le società del gruppo;
- progettazione della combinazione sinergica tra le linee di business;
- condivisione di risorse e competenze strategiche;
- condivisione di obiettivi strategici e di risultato attraverso procedure condivise di pianificazione, reporting e controllo;
- gestione unitaria e/o coordinamento dei processi a maggior criticità (es. amministrazione e contabilità, HR, GDPR) delle controllate da parte della Cloud Care S.p.A. che riporta direttamente al team esterno di Investcorp, nel rispetto del principio di segregazione;
- implementazione di meccanismi di verifica per valutare il rispetto degli standard di gruppo e prevenire i comportamenti devianti attraverso attività di internal auditing.

Cloud Care interviene, a tale scopo, attraverso la definizione di policy, procedure, istruzioni di lavoro, sistemi di controllo dei documenti, formazione, controllo della qualità e dei processi e definizione delle competenze del personale nei processi chiave, sistemi informatici validati e requisiti di archiviazione dei documenti.

Le policy e gli standard di Cloud Care sono diffusi e recepiti da tutte le società appartenenti al gruppo all'interno delle proprie organizzazioni.

Cloud Care, in qualità di soggetto giuridico autonomo, ha adottato un sistema di governance tradizionale, nel rispetto degli artt. 2380 e segg. c.c.; la gestione è affidata al Consiglio di amministrazione, il controllo di legalità a un collegio sindacale e il controllo contabile ad una società di revisione.

ASSEMBLEA: L'assemblea è competente a deliberare, in materia ordinaria e straordinaria, sulle materie riservate alla stessa dalla Legge e dallo Statuto.

ORGANO AMMINISTRATIVO: La società può essere amministrata alternativamente da un Amministratore unico o da un Consiglio di amministrazione composto da un minimo di tre ad un massimo di sette amministratori. Il Consiglio di Amministrazione può nominare uno o più Amministratori delegati. Il CdA di Cloud Care ha nominato quale Amministratore delegato il Presidente Andrea Conte determinandone i poteri e le deleghe.

ORGANI DI CONTROLLO: al Collegio Sindacale composto da tre sindaci effettivi e due supplenti, per legge, spetta il compito di vigilare sull'osservanza della legge e dell'atto costitutivo e sul rispetto dei principi di corretta amministrazione, compresa la vigilanza sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento.
Al Revisore spetta il controllo contabile, che per legge comprende il compito di pianificare l'attività di revisione, verificare il sistema dei controlli interni, controllare i conti ed i documenti contabili, redigere la relazione di revisione contabile.

3.2.1 Il sistema delle deleghe e procure

Il Consiglio di amministrazione di Cloud Care è l'organo preposto a conferire ed approvare formalmente le deleghe ed i poteri di firma.
Coerentemente con le indicazioni delle Linee Guida di Confindustria nell'ultima versione di giugno 2021, il livello di autonomia, il potere di rappresentanza, i limiti di spesa attribuiti ai vari titolari di deleghe e procure sono

correttamente individuati, definiti ed assegnati in funzione del livello gerarchico e delle responsabilità di ciascun delegato.
Il sistema di deleghe e procure attualmente adottato in Cloud Care è rispondente alla struttura organizzativa in vigore e rappresentata dall'organigramma allegato al presente documento. Esso si sovrappone ed integra il sistema di conferimento di ruoli e responsabilità ed attribuzione di incarichi e mansioni raffigurato nell'organigramma, nelle job description e nelle procedure aziendali.

Al momento della redazione del presente MOGC la rappresentanza della società di fronte ai terzi spetta all'Amministratore delegato.

Sono inoltre attribuiti ad altre funzioni aziendali specificatamente individuate, precisi livelli autorizzativi distinti per tipologia di spesa e soglia di valore, nel rispetto del principio di progressione gerarchica e funzionale.

Le deleghe e le procure sono ufficializzate attraverso delibere del CdA e, in alcuni casi, atti notarili coerenti con tali delibere. Ciascun atto di delega o procura o conferimento di poteri bancari di firma fornisce le seguenti indicazioni:

- soggetto delegante e fonte dei poteri di delega e procura;
- soggetto delegato con riferimento alla funzione attribuitagli ed al legame tra la delega e la procura e il ruolo organizzativo ricoperto;
- le attività e gli atti oggetto di delega o procura e gli eventuali limiti di valore entro i quali il potere conferito possa essere esercitato.

Il sistema delle deleghe e dei poteri di firma, oltre che delle specifiche autorizzazioni conferite a precise funzioni aziendali, viene costantemente monitorato ed aggiornato a seguito di modifiche dell'organizzazione aziendale.

3.2.2 La struttura organizzativa

Il sistema di distribuzione dei poteri rappresenta il primo presidio per la prevenzione dei rischi di commissione dei reati e configura i seguenti elementi caratterizzanti la struttura organizzativa di Cloud Care:

- per ogni area aziendale è individuato un manager di riferimento collocato formalmente in organigramma, con espliciti incarichi e responsabilità di funzione;
- l'organizzazione è tale da garantire la chiarezza delle linee gerarchiche ed il coordinamento, il monitoraggio e la rendicontazione periodica delle attività svolte;
- a ciascun manager competono, oltre al coordinamento delle attività relative alla missione assegnata, la valutazione e gestione dei rischi inerenti, la valutazione delle performance, il reporting per linea gerarchica, il controllo di budget, la valorizzazione, valutazione e supervisione del personale assegnato, la cura e la salvaguardia degli asset gestiti.

Al fine di rendere immediatamente chiaro il ruolo e le responsabilità di ogni funzione aziendale in Cloud Care si riporta in allegato al presente documento l'organigramma aziendale che rappresenta le relazioni gerarchiche interne e con le altre società del gruppo.

3.2.3 Le policy e le procedure aziendali

Cloud Care ha definito, in linea con i valori aziendali e con quelli di Investcorp, un sistema di principi etici e regole di comportamento condivisi con tutte le società del gruppo. Questi valori sono rappresentati nel Codice etico aziendale che sancisce i principi cui devono ispirarsi, senza alcuna eccezione, tutti coloro che, a qualsiasi titolo, operano con e per conto di Cloud Care, soci, amministratori, dipendenti, consulenti, partner, fornitori.

Il Codice al suo interno fa riferimento a tutte le policy specifiche disposte per regolamentare gli aspetti di compliance che interessano il gruppo.

Questo sistema di valori di Cloud Care si basa su un sistema articolato di garanzia della compliance aziendale che mediante formazione, informazione, supporto e controllo opera su più livelli attraverso:

- i manager di area;
- l'area QHSE;
- l'area legal e compliance;

- il DPO;
- il Social Performance Team;
- l'OdV;
- Comitato whistleblowing;
- il comitato di audit;
- il comitato compensation.

Il Codice etico e le policy sono disponibili per tutto il personale aziendale attraverso i canali interni di comunicazione.

Sono inoltre pubblicati sul sito istituzionale www.cloud-care.it e sul sito commerciale www.comparasemplice.it a disposizione di tutti gli altri destinatari.

I dipendenti e i collaboratori, all'atto dell'assunzione, sottoscrivono di aver ricevuto il Codice etico e confermano l'impegno all'osservanza dello stesso e delle policy richiamate.

Periodicamente sono organizzate sessioni di sensibilizzazione e formazione sulle policy aziendali rivolte a funzioni/mansioni specifiche invitando i dipendenti ed i collaboratori a seguire training ad hoc messi a disposizione attraverso i canali aziendali di comunicazione interna.

Il Codice e le policy adottate da Cloud Care costituiscono parte integrante del presente MOGC rappresentando, insieme ai documenti del Sistema di Gestione Integrato (procedure, istruzioni, informazioni documentate) ed ai sistemi informativi, i presidi posti per regolamentare i processi aziendali e prevenire le condotte penalmente rilevanti ai sensi del D.lgs. 231. Un siffatto complesso di regole garantisce il corretto svolgimento delle attività, la chiara segregazione dei ruoli e dei poteri e la tracciabilità di ogni operazione, in modo che sia sempre possibile risalire ai responsabili di ogni azione. Inoltre, consente l'armonizzazione dei processi a maggiore criticità tra le società controllate da Cloud Care (es. processi finanziari), prevedendo anche i controlli finalizzati a garantire esattezza, efficacia ed efficienza di tutte le operazioni.

Le procedure informatiche adottate in conformità al Sistema di gestione per la sicurezza delle informazioni certificato ISO 27001 e l'utilizzo di idonei applicativi gestionali (Team System, Vision, Vici, etc.), garantiscono che ogni operazione venga supportata dagli adeguati livelli organizzativi così da poter procedere in qualsiasi momento all'esecuzione di controlli che individuino responsabilità, finalità e motivazioni dell'operazione, con identificazione del ciclo completo di autorizzazione, registrazione e verifica delle operazioni stesse.

3.2.4 La gestione dei processi finanziari ed i contratti intercompany

In Cloud Care sono definite idonee procedure per la gestione delle attività finanziarie che, conformemente alle indicazioni delle Linee Guida di Confindustria, rappresentano un'area di particolare criticità per i reati ex D.lgs. 231.

In questo ambito il controllo procedurale si avvale dei seguenti strumenti consolidati:

- poteri bancari su delega con limiti di importo o firma congiunta;
- criterio della separazione dei compiti tra coloro che svolgono fasi o attività cruciali nei processi a maggior rischio (ad esempio fra la funzione acquisti e quella finanziaria);
- programmazione e definizione di budget e rendicontazione secondo processi standardizzati definiti e condivisi con Investcorp e le altre società controllate;
- gestione centralizzata delle attività contabili e amministrative delle società del gruppo;
- configurazione e controllo dei software gestionali ed assegnazione dei profili autorizzativi da IT;
- supervisione e coordinamento dei processi da parte di Investcorp.

I rapporti contrattuali tra le società del gruppo sono regolamentati da accordi di servizio. Tali contratti disciplinano esattamente l'oggetto e le condizioni dell'accordo, management fees, criteri e modalità di esecuzione, termini di pagamento, controlli e la conservazione delle evidenze documentali attestanti il rispetto delle condizioni contrattuali.

Cloud Care ha predisposto, per le società del gruppo, TeamSystem sul quale sono veicolate tutte le attività contabili ed amministrative del gruppo.

3.3 Il Modello di Organizzazione Gestione e Controllo (MOGC) di Cloud Care

Il Modello di Organizzazione, Gestione e Controllo (di seguito anche MOGC) è un **sistema strutturato ed organico di protocolli, policy, norme interne, procedure, sistemi di controllo**, finalizzato allo svolgimento dell'attività di impresa secondo criteri di trasparenza, correttezza e tracciabilità e per questo idoneo a mitigare il rischio di irregolarità nei processi e conseguentemente a prevenire, ove possibile e concretamente fattibile, la commissione dei reati previsti dal D.lgs. 231.

In particolare, ai sensi del comma 2 dell'articolo 6 del D.lgs 231, il MOGC deve rispondere in modo adeguato alle seguenti esigenze:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- prevedere un sistema interno, che fissi le linee di orientamento generali per assumere e attuare decisioni nei settori "sensibili";
- un sistema di deleghe e di poteri aziendali che assicuri una chiara e trasparente rappresentazione del processo aziendale di formazione, attuazione e controllo delle decisioni;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- attribuire all'Organismo di Vigilanza specifici compiti di controllo sull'efficacia, sull'osservanza e sul corretto funzionamento del Modello e dei Protocolli, nonché sulla loro coerenza con gli obiettivi aziendali e sul loro aggiornamento periodico;
- prevedere obblighi di informazione nei confronti dell'OdV deputato a vigilare sul funzionamento e l'osservanza del modello;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il MOGC di Cloud Care è stato concepito in modo tale da recepire integralmente le policy, le procedure, le direttive operative, gli standard della controllante, oltre al Sistema di Gestione Integrato aziendale certificato ISO 9001, ISO 14001, ISO 45001, ISO 27001 e PAS 24000, costituendo in questo modo un corpo unico. In tal modo si è voluta fornire maggiore efficacia al MOGC, affinché potesse fondarsi su meccanismi organizzativi e gestionali già consolidati.

Il MOGC di Cloud Care è descritto nella presente Parte Generale e nella Parte Speciale, quindi, come già indicato in premessa, oltre a quanto espressamente stabilito in tali documenti, costituiscono parte integrante del MOGC:

- Il risk assessment finalizzato all'individuazione delle attività sensibili, qui integralmente richiamato e agli atti della Società;
- il Codice Etico che definisce i principi e le norme di comportamento aziendale;
- Il sistema privacy ai sensi del GDPR 679/16;
- tutte le disposizioni, le policy, i provvedimenti interni, i documenti del Sistema di Gestione integrato ISO 9001, ISO 14001, ISO 45001, ISO 27001, PAS 24000, gli atti e le procedure operative aziendali che di questo documento costituiscono attuazione (es. poteri, organigrammi, statuto). Tali atti e documenti sono reperibili secondo le modalità previste per la loro diffusione all'interno dell'azienda.

La Parte Speciale è composta da tante sezioni quante sono le fattispecie di reato considerate applicabile a Cloud Care, definendo per ognuna di esse:

- I processi sensibili;
- I principi di comportamento - regole generali e divieti specifici;
- Il riferimento alle procedure specifiche, alle policy ed ai protocolli a presidio dei processi sensibili.

Il MOGC è stato progettato partendo dall'analisi dei processi aziendali svolta in occasione dello sviluppo e successiva certificazione del Sistema di Gestione Aziendale. In tale occasione si è proceduto alla mappatura di

tutti i processi aziendali in relazione ai diversi standard di certificazione adottati e sono stati esaminati i rischi e le opportunità derivanti sia dal contesto esterno in cui opera l'azienda, sia dal contesto interno, ovvero dai punti di forza e di debolezza che caratterizzano l'organizzazione.

Successivamente l'analisi è stata integrata in relazione ai criteri normativi individuanti le forme di responsabilità amministrativa degli enti (per reati commessi nel loro interesse o a loro vantaggio da soggetti che rivestono una posizione apicale nella struttura dell'ente stesso ovvero da soggetti sottoposti alla vigilanza di questi ultimi), e dei più recenti contributi aggiuntivi, ricavabili dalla giurisprudenza formatasi in materia negli ultimi anni.

Si è proceduto ad una razionale individuazione dei profili di rischio collegabili alla concreta attività svolta da Cloud Care (risk assessment), in modo tale da far da ciò discendere i dati peculiari da attribuire al MOGC ritenuto più efficace per prevenire la commissione di tutti quei fatti aventi rilievo penale, che potrebbero essere ricondotti all'ente stesso, e più idoneo ad esimere la società sia da responsabilità, sia dal rischio di una applicazione anticipata in via cautelare delle misure interdittive ex art.13 D.lgs. 231.

In considerazione dell'attività svolta da Cloud Care si è posta attenzione sulla tracciabilità di tutte le fasi di formazione, attuazione e controllo delle decisioni relative ai processi aziendali, attribuendo ampio rilievo agli obblighi di informazione dai vertici verso la base e viceversa così come a quelli con le altre società controllate. Tali obblighi sono previsti a carico di ogni funzione, anche nelle fasi preparatorie del processo decisionale, con una diffusione capillare, tale da non far residuare zone prive delle necessarie comunicazioni informative.

Allo stesso modo, l'osservanza delle direttive aziendali ed i protocolli specifici, espressi all'interno delle policy, delle procedure, dei principi di ordine generale e dei divieti contenuti nella parte Speciale del MOGC e dei precetti del Codice Etico, viene assicurata da una serie di strumenti condivisi sia con la controllante che con le controllate (processi di rendicontazione, due diligence, internal audit) e dagli strumenti di controllo propri del Sistema di gestione aziendale quali ad esempio gli audit sia interni che di terza parte QHSE, 27001, PAS 24000 e da un sistema disciplinare idoneo a sanzionare le violazioni allo stesso MOGC.

Sulla scorta di rilievi giurisprudenziali emersi in tema di responsabilità amministrativa ex D.lgs. 231, è stata altresì prevista l'istituzione di un Organismo di Vigilanza (OdV) con il compito di vigilare sul funzionamento e sulla osservanza delle prescrizioni adottate, provvisto di autonomi ed effettivi poteri di controllo, mai sottoposto alle dirette dipendenze del soggetto controllato (si veda ad esempio, Sent. Cass.pen. Sez. V, 18.12.13, n.4677).

Il precipuo ruolo svolto dall'OdV impone allo stesso di esercitare i compiti di vigilanza, facendo perno soprattutto su un sistema di accesso alle informazioni che sia ben strutturato e consenta di "avere il polso" della situazione societaria in modo costante.

Non a caso, durante le indagini che vedono coinvolti gli enti, viene dato particolare rilievo "**alla qualità ed alla tempestività delle informazioni destinate all'organismo di controllo**, allo scopo di constatare l'effettivo funzionamento dei meccanismi di prevenzione predisposti e la concreta capacità di reazione del citato organismo di vigilanza nello specifico contesto (...)" (rif. Circolare Guardia di Finanza, n.83607/12).

Il continuo ampliamento dell'elenco dei reati, indicati dal legislatore, determinanti la responsabilità dell'ente, richiede un Organismo di Vigilanza sempre più reattivo, in grado, cioè, sia di "rafforzare" l'attività di prevenzione anche se svolta da altre figure (si pensi ai compiti in materia di salute e sicurezza sul lavoro o ambientali, per impedire la responsabilità dell'ente derivante dalla commissione di delitti colposi), sia di porsi come referente per altre autorità (si pensi agli obblighi derivati dalla cd. normativa antiriciclaggio che richiede all'OdV di comunicare a pubbliche autorità le infrazioni rilevate nell'esecuzione delle sue funzioni).

Per tale motivo, si è preferito delineare un OdV capace di documentare lo svolgimento dei propri compiti anche a distanza di anni. Per far ciò è stata data **estrema importanza alla gestione dei flussi informativi ed all'attività di archivio**. Nelle varie aree individuate all'interno del MOGC, le figure che interagiscono per la realizzazione di ogni scelta/decisione conclusiva della specifica area fanno riferimento ad un **sistema di tracciabilità** che consenta di rilevare la paternità di ogni valutazione finale e della relativa verifica.

Per tale ragione la posizione di colui al quale sono affidati i compiti di controllo e vigilanza è definita come totalmente separata, e con una netta autonomia, dalle posizioni di chi partecipa a vario titolo nella formazione/esecuzione delle decisioni.

Ulteriore aspetto considerato nell'elaborazione del presente MOGC è stato quello relativo alle problematiche connesse alla esatta individuazione della nozione di "**interesse o vantaggio**" dell'ente.

Dall'esperienza giurisprudenziale, emerge che:

- ai fini della configurabilità della responsabilità dell'ente, è sufficiente che venga provato che lo stesso abbia ricavato dal reato un vantaggio, anche quando non è stato possibile determinare l'effettivo interesse vantato ex ante alla consumazione dell'illecito e purché non sia commesso nell'esclusivo interesse del suo autore-persona fisica (si veda Cass. 5^penale, sent.n.10265/14);
- perché possa ascriversi all'ente la responsabilità per il reato è sufficiente che la condotta dell'autore di quest'ultimo tenda oggettivamente e concretamente a realizzare nella prospettiva del soggetto collettivo, "anche" l'interesse del medesimo (v. Cass. 5^ penale, sent.n.40380/12);
- oggi i concetti di interesse e vantaggio, anche nei reati colposi di evento, vanno necessariamente riferiti alla condotta posta in essere e non all'esito antigiuridico. Inoltre, anche all'interno di una mancata normazione preventiva, **l'eventuale mancata predisposizione di cautele da parte dell'organizzazione**, **se avviene in seguito a scelte aziendali consapevoli**, **rappresenta un ambito di rischio concreto** di responsabilità amministrativa dell'ente e può condurre alla commissione di reati presupposto. (Cass. Pen. Sez.3^, 27.01.2020, n.3157).

Occorre a ciò aggiungere che lo stesso D.lgs. n.231 prevede (artt.12 e 13) la diminuzione delle sanzioni pecuniarie e l'inapplicabilità delle misure interdittive se il reato presupposto venga commesso nel prevalente interesse del suo autore o di terzi e l'ente non ne abbia ricavato alcun vantaggio ovvero un vantaggio minimo.

Da questi rilievi, è ricavabile la necessità che sia prestata attenzione all'osservanza del divieto di compiere condotte ritenute e valutate "a rischio".

3.3.1 Finalità del MOGC

In sintesi, il MOGC si propone le seguenti finalità:

- fornire un'adeguata informazione a dipendenti, collaboratori e a tutti coloro che agiscono per conto di Cloud Care, o sono ad essa legati da rapporti rilevanti ai fini del D.lgs.231, in riferimento alle attività che comportano il rischio di commissione dei reati;
- diffondere una cultura d'impresa basata sulla legalità, in quanto Cloud Care condanna ogni comportamento non conforme alla legge o alle disposizioni interne, di conseguenza alle disposizioni contenute nel proprio MOGC;
- un'efficace ed efficiente organizzazione dell'impresa, in particolare dei processi di formazione delle decisioni e sulla loro trasparenza, sulla previsione di controlli, preventivi e successivi, nonché sulla gestione dell'informazione interna ed esterna;
- attuare tutte le misure necessarie per eliminare nel più breve tempo possibile eventuali situazioni di rischio di commissione dei reati.

3.4 L'Amministratore

Le norme ed i principi contenuti nel MOGC devono essere rispettati, in primo luogo, dai soggetti che rivestono, in seno alla Società, una posizione cd. “apicale”. A norma dell’art. 5, comma 1, lett. a) del D.lgs.231, rientrano in questa categoria le 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 i soggetti che “**esercitano, anche di fatto, la gestione o il controllo**” della Società.

In tale contesto, assume rilevanza, in primis, la posizione dei componenti degli organi di amministrazione (“Amministratore”), ovvero Consiglieri del CdA, Presidente del CdA, Amministratore delegato.

3.5 I dipendenti di Cloud Care

Nel caso previsto dall'articolo 5, comma 1, lettera b) (reato commesso da **persone sottoposte alla direzione o alla vigilanza di uno dei soggetti** di cui alla lettera a) **"apicali"**), **l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza**.

Ai sensi dell'art. 7 lett. b) del Decreto è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi. Tale modello deve prevedere, in relazione alla natura e alla dimensione dell'organizzazione, nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

Affinché un Modello si consideri efficacemente attuato dovrà prevedere:

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

Rileva, a tale proposito, la posizione di tutti i dipendenti legati a Cloud Care da un rapporto di lavoro subordinato, indipendentemente dal contratto applicato, dalla qualifica e/o dall’inquadramento aziendale riconosciuto (ad esempio: quadri, impiegati, lavoratori a tempo determinato, lavoratori con contratto di inserimento, ecc. di seguito, i “Dipendenti”).

3.6 Gli altri soggetti tenuti al rispetto del MOGC

Si tratta, in particolare, di tutti i soggetti ("Soggetti Esterni") che sono comunque tenuti al rispetto del MOGC in virtù della funzione svolta in relazione alla struttura societaria e organizzativa di Cloud Care, ad esempio in quanto funzionalmente soggetti alla direzione o vigilanza di un soggetto “apicale”, ovvero in quanto operanti, direttamente o indirettamente, per la Società.

Nell’ambito di tale categoria, rientrano in particolare, in ragione dell’attività svolta da Cloud Care, i seguenti soggetti:

- i collaboratori coordinati e continuativi che intrattengono con la Società un rapporto di lavoro di natura non subordinata per la vendita diretta di beni e di servizi sia attraverso il canale telefonico che attraverso il WEB;
- i collaboratori a progetto, i consulenti, i lavoratori in somministrazione;
- tutti coloro che agiscono in nome e per conto di Cloud Care;
- le società controllate appartenenti al gruppo;
- i fornitori, ditte appaltatrici e partners, Società di revisione;
- i soggetti a cui sono assegnati compiti specifici in materia di salute e sicurezza sul lavoro (Medico competente, responsabili e addetti al SPP se esterni all’azienda).

3.7 Le condotte rilevanti

Costituiscono condotte oggetto di sanzione le azioni o i comportamenti posti in essere in violazione del MOGC, comprendendo anche le condotte, attive o omissive, poste in essere in violazione delle indicazioni e/o delle prescrizioni dell’OdV.

4. L'ORGANISMO DI VIGILANZA PER L'APPLICAZIONE DEL MOGC

L'articolo 6, comma 1, lett. b) dispone, con riferimento all'azione dei soggetti apicali, che "il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento" debba essere affidato "ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo".

Inoltre, sebbene non esista un riferimento legislativo espresso quanto all'azione dei sottoposti all'altrui direzione ai fini dell'efficace attuazione del modello adottato, è richiesta, all'articolo 7, c.4, lettera a) una verifica periodica e l'eventuale modifica dello stesso quando siano scoperte significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione o nell'attività.

L'Organismo di Vigilanza (OdV) è la funzione aziendale cui spetta la vigilanza del MOGC sia in termini di verifica dell'osservanza dei precetti in esso contenuti da parte di tutta la struttura, sia di adeguatezza dello stesso a seguito di violazione delle prescrizioni o mutamenti nell'organizzazione.

L'OdV prevede ed attua un sistema di flussi incrociati di informazioni con l'Amministratore delegato, il CdA e le altre funzioni aziendali e verifica la coerenza tra i comportamenti concreti ed il MOGC istituito.

L'OdV vigila, inoltre, sul mantenimento nel tempo dei requisiti di funzionalità del MOGC attuato, sollecitando le necessarie correzioni attraverso:

- presentazione di proposte di adeguamento inviate agli organi aziendali capaci di dar loro attuazione (ad es. in caso di violazioni del MOGC dovute a modificazioni dell'assetto interno della società e/o delle modalità di svolgimento dell'attività di impresa o a modificazioni normative);
- verifiche sulla attuazione e funzionalità delle soluzioni proposte (cd. follow up).

L'OdV è dotato di autonomi poteri di iniziativa e controllo.

Effettua attività di controllo libera da interferenze e da condizionamenti ed attività di monitoraggio con periodicità adeguata.

L'OdV **non è soggetto**, in tale qualità e nell'ambito dello svolgimento della propria funzione, **al potere gerarchico e disciplinare di alcun organo o funzione societaria.**

4.1 Nomina, durata e composizione dell'ODV

L'OdV di Cloud Care è un organo a struttura monocratica o collegiale, nominato con delibera del CdA. Nell'ambito della nomina il CdA valuta anche il possesso, da parte dei candidati, di specifiche competenze in ambito giuridico e consulenziale.

L'OdV dura in carica sino alla scadenza del mandato del CdA che lo ha nominato. Al termine del mandato rimane in carica con pienezza di poteri e doveri fino alla nomina del nuovo OdV. L'OdV può essere rieletto.

L'OdV può essere revocato anticipatamente per giusta causa, desumibile da un inadempimento specifico, sia doloso o colposo, agli obblighi inerenti all'incarico.

4.2 Condizioni di ineleggibilità

In conformità a quanto previsto dalla dottrina più autorevole e dai recenti orientamenti giurisprudenziali non possono essere nominati componenti dell'OdV coloro che si trovano in una delle seguenti condizioni:

- relazioni di parentela, coniugio o affinità entro il IV grado con l'amministratore della società;
- aver riportato condanna, anche non definitiva ovvero a seguito di sentenza di patteggiamento ex art.444 c.p.p. o di decreto penale di condanna, relativa a reati previsti dal D. Lgs. 231 o a reati per cui sia prevista dalla legge la pena edittale superiore nel massimo ad anni 5 di reclusione;
- abbiano poteri rappresentativi nella società.

4.3 Autonomia e indipendenza

L'OdV deve possedere requisiti di natura soggettiva e oggettiva che ne garantiscano:

- autonomia e indipendenza;
- integrità morale, equità e correttezza;

- onorabilità e autorevolezza;
- professionalità;
- continuità d'azione.

In particolare, il requisito della professionalità deve essere inteso come le capacità e qualifiche per svolgere efficacemente le funzioni di OdV. Questo anche con riferimento al possesso di comprovate competenze in materia di compliance normativa e analisi dei processi.

Le attività poste in essere dall'OdV non possano essere sindacate da alcun altro organismo o struttura aziendale, fermo restando che il CdA vigila sull'adeguatezza del suo intervento, poiché ad esso compete la responsabilità ultima del funzionamento (e dell'efficacia) del MOGC;

L'OdV ha libero accesso presso tutte le funzioni della società, senza necessità di alcun consenso preventivo, al fine di ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal suo ruolo di controllo del MOGC;

L'OdV può avvalersi, sotto la sua diretta sorveglianza e responsabilità, dell'ausilio di tutte le strutture della società, ovvero di consulenti esterni.

4.4 Sospensione, revoca, dimissioni dell'OdV

Il CdA può deliberare la sospensione dell'OdV nel caso in cui lo stesso sia destinatario di avviso di garanzia per uno dei reati indicati dal D. Lgs. 231, fatta salva la reintegrazione dello stesso in caso di successiva mancata richiesta di rinvio a giudizio.

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

- termine della carica;
- revoca dell'OdV da parte del CdA.

La revoca dell'OdV può avvenire solo per giusta causa, anche al fine di garantirne l'assoluta indipendenza.

A titolo esemplificativo, ma non esaustivo, rientrano nella nozione di "giusta causa", le seguenti circostanze:

- gravi negligenze nell'assolvimento dei compiti connessi con lo svolgimento dell'incarico (a titolo meramente esemplificativo: omesso svolgimento dell'attività di audit, omessa predisposizione della reportistica informativa, etc.);
- omessa o insufficiente vigilanza da parte dell'OdV come previsto dall'art. 6, comma 1 lett. d del D.lgs. 231, così come risultante da sentenza di condanna anche non passata in giudicato emessa nei confronti dell'Azienda ai sensi del D.lgs. 231, ovvero da sentenza di applicazione della pena su richiesta (patteggiamento);
- attribuzione di funzioni e responsabilità operative all'interno dell'Azienda incompatibili con i requisiti di autonomia e indipendenza e continuità di azione propri dell'OdV;
- assenza non giustificata alle riunioni regolarmente convocate nella misura di tre assenze su base annua.

La revoca per giusta causa è disposta dal CdA.

Il CdA provvede alla sostituzione dell'OdV nella stessa seduta nella quale ne delibera la revoca.

Ciascun componente dell'OdV potrà rassegnare le proprie dimissioni in ogni momento, tramite notifica scritta.

In caso di OdV plurinominale, la cessazione della maggioranza dei membri dell'OdV causa la decadenza dell'intero OdV; qualora la maggioranza dei membri dell'OdV mantenga la carica, il CdA provvederà alla sostituzione dei soli membri cessati.

4.5 Il regolamento interno dell'OdV

L'OdV, in seguito alla propria nomina, deve tempestivamente predisporre un proprio regolamento interno al fine di disciplinare le modalità per lo svolgimento dei propri compiti contenente e provvedere alla redazione di un programma dei controlli e delle verifiche, anche ai fini dell'aggiornamento del MOGC.

4.6 Funzioni e poteri dell'Organismo di Vigilanza

L'OdV, con riguardo a quanto previsto dal D. Lgs. 231, è chiamato a svolgere le seguenti funzioni:

- monitorare l'efficacia del MOGC così come pianificato, al fine di verificarne l'efficacia in funzione del quadro normativo, degli assetti societari e del profilo di rischio;
- verificare l'aggiornamento, da parte dei competenti organi e funzioni societarie, del MOGC, delle regole e dei principi organizzativi in esso contenuti o richiamati per esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative rilevanti, nuove direttive da parte della controllante;
- assicurare una costante e indipendente azione di sorveglianza sul regolare andamento dell'operatività e sulla conformità dei processi di Cloud Care ai sensi del dettato del MOGC, al fine di prevenire o rilevare l'insorgere di comportamenti o situazioni anomale e rischiose;
- effettuare periodicamente verifiche mirate su specifiche operazioni poste in essere nell'ambito dei processi sensibili;
- disporre verifiche straordinarie e/o indagini mirate laddove si evidenzino disfunzioni del MOGC o si sia verificata la commissione di reati oggetto delle attività di prevenzione;
- riferire costantemente del proprio operato all'Amministratore Delegato o al Presidente del CdA e relazionare periodicamente il CdA e l'organo di controllo (Collegio sindacale), almeno una volta l'anno, in ordine alle attività svolte, alle segnalazioni ricevute, agli interventi correttivi e migliorativi del MOGC e al loro stato di realizzazione;
- verificare l'implementazione di un adeguato piano formativo sui principi delineati nel MOGC, nel Codice etico aziendale e nelle altre policy aziendali per i destinatari del modello;
- istituire specifici canali informativi "dedicati" (via e-mail, via posta ordinaria e via telefono) diretti a facilitare il flusso di segnalazioni e informazioni verso l'OdV e valutarne periodicamente l'adeguatezza;
- segnalare tempestivamente al CdA, all'Amministratore delegato e all'organo di controllo (Collegio sindacale) qualsiasi violazione del MOGC accertata dall'OdV stesso e ogni informazione rilevante al fine del corretto adempimento delle disposizioni di cui al D.lgs. 231;

4.7 Budget assegnato all'OdV

Il CdA dota l'Organismo di Vigilanza di un budget adeguato allo svolgimento dei suoi compiti, quali lo svolgimento di consulenze e trasferte, assicurando che lo stesso possa disporne se richiesto.

Le risorse finanziarie sono gestite mediante apposito capitolo di spesa all'interno del bilancio aziendale. L'OdV formula ogni anno per l'anno successivo una previsione annuale di massima (budget) in merito alle risorse finanziarie di cui necessita per lo svolgimento dei compiti ad esso assegnati.

Tale previsione è presentata al CdA all'interno della relazione annuale, per relativa verifica.

4.8 Flussi e obblighi informativi da e verso l'OdV

L'OdV deve relazionare ed informare il CdA e il Collegio sindacale, con periodicità almeno annuale, sui seguenti aspetti:

- l'attività di controllo e vigilanza svolta con indicazione puntuale e tempestiva delle eventuali criticità emerse, delle segnalazioni ricevute e delle sanzioni disciplinari eventualmente irrogate dai soggetti competenti;
- l'effettiva attuazione del MOGC, nonché le proposte di aggiornamento e modifica dello stesso;
- la segnalazione di eventuali comportamenti che violino le prescrizioni del MOGC o il mancato espletamento da parte degli organi gestori della Società dei propri compiti di verifica e/o d'indagine;
- ogni informazione ritenuta utile ai fini dell'assunzione di determinazioni urgenti da parte degli organi deputati.

L'OdV deve relazionare ed informare il CdA sulla base di due diverse linee di reporting:

- la prima, su base continuativa, direttamente verso il Presidente del CdA e Amministratore delegato;
- la seconda, su base annuale, nei confronti del CdA. L'OdV a tal proposito dovrà predisporre una relazione annuale sulle attività svolte, diretta al CdA e al Collegio sindacale.

In caso di urgenza, il CdA o il Presidente del CdA o il Collegio Sindacale hanno la facoltà di convocare in qualsiasi momento l'OdV. Dal canto suo, l'OdV è tenuto a riferire oralmente in maniera tempestiva al CdA, all'AD

o al Presidente del CdA o al Collegio Sindacale ovvero potrà richiedere ai soggetti competenti la convocazione di tali organi gestori. I colloqui con i soggetti di cui sopra devono essere verbalizzati e le copie dei verbali devono essere conservate presso gli uffici dell'OdV.

In ogni caso, poiché l'obbligo di informazione all'OdV è un ulteriore strumento per agevolare l'attività di vigilanza sull'efficacia del MOGC, oltre che di accertamento a posteriori delle cause che hanno reso possibili potenziali violazioni del MOGC, devono essere garantiti adeguati flussi di informazione verso l'OdV.

L'OdV, nello svolgimento dei propri compiti, potrà richiedere ed acquisire dati, informazioni, documenti, modalità di esecuzione/attuazione delle attività sulla base ed in relazione a criteri che periodicamente determinerà con eventuale indicazione di aree o progetti specifici.

La mancata collaborazione con l'OdV costituisce un illecito disciplinare per i Dirigenti Apicali, Altri Soggetti Apicali e/o Dipendenti.

4.9 Informazioni periodiche relative all'attività societaria

L'OdV definisce con proprio regolamento le modalità per l'effettuazione dei controlli periodici e redige annualmente un Piano dei controlli per l'anno successivo che viene sottoposto al CdA in occasione della relazione annuale sulle attività svolte.

Oltre ai documenti, i dati e le informazioni che l'OdV acquisisce nello svolgimento delle proprie funzioni, i Destinatari del MOGC sono tenuti comunque a comunicare all'OdV tutte le notizie di rilievo inerenti atti e fatti aziendali e che possono essere importanti per l'espletamento dei compiti assegnati all'OdV stesso.

Si riporta a seguire un elenco esemplificativo e non esaustivo, di informazioni che devono essere trasmesse all'OdV, oltre alle ulteriori indicate nel regolamento dell'OdV o dallo stesso richieste al fine di ricostruire l'intero processo decisionale.

Informazioni periodiche:

- bilancio con la relativa nota integrativa e la relazione sulla gestione, Relazione della Società di Revisione, Relazione del Collegio sindacale;
- elenco aggiornato delle deleghe e sub-deleghe di funzioni e delle procure rilasciate in azienda;
- ordine del giorno dei verbali del consiglio di amministrazione;
- eventuali decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
- elenco delle sponsorizzazioni, donazioni e delle liberalità erogate;
- incarichi alle società di revisione;
- verbali conseguenti alle ispezioni svolte dagli organi di controllo esterni, in particolare, qualora emergano rilievi, lo stato di attuazione dell'eventuale piano di azione elaborato al fine di eliminare detti rilievi;
- verbali di audit interni;
- verbali di audit dell'ente di certificazione;
- bilancio sociale con i dati relativi al personale e alla formazione;
- verbale di riunione annuale ex art. 35 TU;

Informazioni occasionali:

- eventuali criticità risultanti dalle attività di controllo di primo livello svolte dalle varie funzioni aziendali coinvolte nelle aree a rischio reato;
- richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per reati di cui al D.lgs. 231/01;
- informazioni in merito ad eventuali operazioni straordinarie;
- comunicazione di particolari criticità da parte del Collegio sindacale e/o della Società di revisione;
- provvedimenti e/o le notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità dai quali si evinca lo svolgimento di indagini che interessano, anche indirettamente, la Società, i suoi dipendenti o i componenti degli organi sociali;
- segnalazioni di incidente/infortunio con prognosi >40 gg;
- modifiche dell'assetto organizzativo;
- acquisizioni, cessioni e fusioni di aziende del Gruppo;

- modifiche dell'assetto procedurale della Società (con riferimento alle attività sensibili 231);
- relazioni su procedimenti disciplinari e sanzioni con potenziale impatto 231;
- informazione di visite, ispezioni e accertamenti avviati da parte degli enti competenti (a titolo meramente esemplificativo: ASL, INPS, INAIL, ISS) e, alla loro conclusione, eventuali rilievi e sanzioni comminate.

4.10 Segnalazione di condotte illecite e rilevanti ai sensi del D. Lgs. 231/01 - Whistleblowing

In ottemperanza a quanto disposto dalla normativa vigente (D.lgs. 24/2023 attuazione della Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione), sono stati abrogati i commi 2-ter e 2-quater dell'articolo 6 del D.lgs. 231 ed è stato modificato il comma 2bis così come di seguito riportato:

Art. 6 comma 2-bis

I modelli di cui al comma 1, lettera a), prevedono, ai sensi del decreto legislativo attuativo della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare, adottato ai sensi del comma 2, lettera e).

Il suddetto decreto D.lgs.24/2023 prevede, in sintesi:

- un regime di tutela verso specifiche categorie di soggetti che segnalano informazioni, acquisite nel contesto lavorativo, relative a violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'ente;
- misure di protezione, tra cui il divieto di ritorsioni, a tutela del Segnalante nonché dei Facilitatori, dei colleghi e dei parenti del segnalante e dei soggetti giuridici collegati al Segnalante;
- l'istituzione di canali di segnalazione interni all'organizzazione (di cui uno di tipo informatico) per la trasmissione di Segnalazioni che garantiscano, anche tramite il ricorso a strumenti di crittografia, la tutela della riservatezza dell'identità del Segnalante, della Persona coinvolta e/o comunque menzionata nella Segnalazione, del contenuto della Segnalazione e della relativa documentazione;
- oltre alla facoltà di sporgere denuncia all'autorità giudiziaria o contabile, la possibilità (qualora ricorra una delle condizioni previste all'art. 6, comma 1, del d.lgs. n. 24/2023) di effettuare Segnalazioni esterne tramite il canale gestito dall'Autorità Nazionale Anticorruzione (di seguito ANAC), nonché di effettuare Divulgazioni pubbliche (al ricorrere di una delle condizioni previste all'art. 15, comma 1, del d.lgs. n. 24/2023), tramite la stampa o mezzi elettronici o di diffusione in grado di raggiungere un numero elevato di persone;
- provvedimenti disciplinari nonché sanzioni amministrative pecuniarie irrogate da ANAC nei casi previsti dagli artt. 16 e 21 del d.lgs. n. 24/2023

Nel rispetto del dettato normativo sono stati predisposti i seguenti canali di segnalazione:

- **Piattaforma Whistleblowing**: al link https://cloud-care-whistleblowing.peoplegest.it/#/

  La piattaforma è idonea a garantire la riservatezza dell'identità del segnalante mediante l'utilizzo di protocolli sicuri e strumenti di crittografia. Al termine dell'inserimento, la Piattaforma fornisce un codice identificativo univoco di 16 cifre che consente di verificare lo stato di lavorazione e inviare e ricevere comunicazioni (anche in forma anonima);

- **Registrazione vocale**: opzione presente all'interno della Piattaforma che prevede la registrazione della dichiarazione del segnalante dietro consenso espresso.

- **Incontro diretto**: con un membro del Comitato Whistleblowing o con L'organismo di Vigilanza di Cloud Care.

Al seguente link: https://www.comparasemplice.it/whistleblowing è possibile reperire tutte le informazioni inerenti il contenuto delle segnalazioni e le modalità di presentazione, oltre che la pagina di accesso al portale. Sono inoltre pubblicati i seguenti documenti:

- Procedura whistleblowing
- Informativa privacy
- FAQ

Allo scopo di gestire il processo di segnalazione è stato nominato il Comitato Whistleblowing del quale fanno parte la Funzione Legal e Compliance di Cloud Care nonché l'Organismo di Vigilanza nominato ai sensi dell'art. 6, punto 1, lett. b) del D.lgs.231/01.

La possibilità di inviare una segnalazione ai sensi degli articoli precedenti completa il sistema di compliance già istituito da Cloud Care nel proprio Sistema di Gestione Integrato in conformità al quale è stata predisposta una procedura per le segnalazioni e i reclami che possono essere presentate, a seconda dell'ambito di interesse, alle diverse funzioni aziendali (Social Performance Team, QHSE, DPO) da parte di dipendenti, collaboratori o altri soggetti interessati (vedi anche PR48 Procedura segnalazioni e reclami).

Cloud Care ha già espresso nel proprio Codice etico, il proprio impegno a contrastare qualunque forma di ritorsione nei confronti di dipendenti o collaboratori che in buona fede presentino reclami, sollevino questioni e/o problemi, esercitino i propri diritti sul luogo di lavoro, e/o partecipino alle indagini, avendo ragionevoli motivi di credere che si sia verificata o si stia verificando una violazione occasionale o continuata di leggi, regolamenti, procedure e del codice etico aziendale, o rifiutino di partecipare ad attività che sospettino essere illecite o illegali.

5. I MECCANISMI DI CONTROLLO PREVENTIVI. GLI INTERVENTI PREDISPOSTI PER IMPEDIRE LA COMMISSIONE DI REATI

5.1 Individuazione delle attività sensibili

L'art. 6., comma 2, lett. a) del D. Lgs. 231 recita:

[..... In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli [.....] devono rispondere alle seguenti esigenze:

a) individuare le attività nel cui ambito possono essere commessi reati.....]

Indica, pertanto, come uno dei requisiti del MOGC, l'individuazione delle cosiddette "aree sensibili" o "a rischio", cioè di quei processi e di quelle aree di attività aziendali in cui potrebbe determinarsi il rischio di commissione di uno dei reati espressamente richiamati dal D. Lgs. 231.

Per la costruzione del MOGC si è quindi partiti dall'analisi della realtà operativa di Cloud Care e dei processi aziendali, già effettuata in occasione della valutazione del contesto interno ed esterno e dei rischi connessi al Sistema di gestione Integrato, per individuare, tra le aree/settori aziendali quelli nei quali esiste un rischio di commissione dei reati previsti dal D. Lgs. 231.

Allo stesso tempo, è stata condotta un'indagine approfondita sugli elementi costitutivi dei reati in questione, allo scopo di identificare le condotte concrete che, nel contesto aziendale, potrebbero realizzare le fattispecie delittuose.

5.2 L'attività di Risk assessment

La mappatura delle funzioni/aree e dei processi aziendali a rischio di commissione dei reati è stato il riferimento preliminare per la valutazione e l'analisi dei rischi reato all'interno di Cloud Care e costituisce un elemento informativo base per la realizzazione del MOGC, nonché per indirizzare le azioni di controllo dell'OdV.

L'attività di Risk assessment, la cui documentazione costituisce parte integrante del MOGC, ai sensi dell'art. 6 c.2 lett.a), è stata condotta con lo scopo di:

- esaminare le aree potenzialmente sensibili in relazione ai reati ex D. Lgs. 231;
- valutare l'idoneità, l'efficacia e l'adeguatezza dei protocolli esistenti, la loro effettiva applicazione, individuando eventualmente le aree passibili di miglioramento. In particolare, si è provveduto ad esaminare, la struttura dei controlli di primo livello, contenuti nelle procedure operative, di secondo e terzo livello previsti dalle direttive aziendali e dalle policy della controllante;
- verificare il coordinamento e l'integrazione dei diversi sistemi di gestione e controllo aziendali, per un equilibrio ottimale tra intensità dei controlli e la necessaria flessibilità e snellezza operativa.

L'attività di risk assessment si è svolta in più fasi sequenziali:

La prima è consistita nel determinare, in base alle informazioni raccolte, quali fossero, tra i reati appartenenti al catalogo del D. Lgs. 231/01, quelli applicabili alla specifica realtà di Cloud Care.

È stato predisposto il documento "Analisi preliminare rischio reato" nel quale, per ogni reato 231 determinante la responsabilità amministrativa dell'ente, sono state descritte:

- le fattispecie delittuose in esso richiamate;
- i comportamenti penalmente rilevanti rispetto al particolare reato;
- l'attinenza o meno dei reati e delle possibili condotte con i principali processi aziendali.

Successivamente è stata elaborata una tabella riepilogativa "Mappatura processi reati" nella quale, in relazione ad ogni area/processo, sono stati definiti:

- responsabili, funzioni interessate, funzioni/aree collegate;
- le attività sensibili riferibili alle diverse funzioni;
- i reati 231 applicabili al singolo processo, indicando, per ognuno di essi, l'applicabilità delle sanzioni pecuniarie e di quelle interdittive ed i riferimenti normativi delle fattispecie delittuose rilevate come attinenti.

La fase successiva di Risk assessment ha avuto per oggetto la valutazione dell'idoneità, efficacia e adeguatezza delle procedure e dei protocolli esistenti e la loro effettiva applicazione quali misure di prevenzione dei reati e, conseguentemente, il livello di rischio di reato, residuo rispetto alla situazione "as is". L'obiettivo è stato determinare se tali presidi fossero sufficienti e potessero confluire nel MOGC oppure se ed in quali processi si rendesse necessario un rafforzamento delle misure in essere.

Si è provveduto quindi a "misurare", per ogni processo, il valore del rischio residuo in base al quale sono state definite le eventuali misure di contenimento necessarie a ricondurlo ad un livello accettabile.

La valutazione del rischio è stata condotta sulla base dei criteri più comunemente utilizzati in letteratura, ovvero la probabilità di accadimento dell'evento e l'impatto dell'evento stesso.

La metodologia adottata in Cloud Care per la mappatura dei rischi ed i corrispondenti risultati sono descritti dettagliatamente nell'allegato " Relazione preliminare analisi dei rischi".

In base all'analisi effettuata è stato ritenuto che non vi siano attività, nell'ambito di Cloud Care, che possano prefigurare alcuni dei reati previsti dal D.lgs. 231 (Allegato "Analisi preliminare rischio reato"), tuttavia, Cloud Caresi impegna, qualora intervenissero cambiamenti nel business, nella struttura organizzativa e/o nella sua operatività, a verificare l'eventuale esposizione alla commissione dei reati precedentemente esclusi e conseguentemente, a predisporre le misure preventive necessarie.

Ciò premesso, si ritiene che anche l'astratto rischio di realizzazione dei suddetti reati sia attualmente sufficientemente gestito attraverso le condotte generali, ispirate a criteri di cautela, correttezza e trasparenza, così come disposto dal presente MOGC.

5.2.1 Aggiornamento del documento di mappatura del rischio

Uno dei compiti dell'Organismo di Vigilanza è verificare che il MOGC e, di conseguenza, la mappatura dei rischi, conservino nel tempo i requisiti di efficacia e validità richiesti dal D.lgs. 231. Come indicato precedentemente, l'OdV provvederà affinché la mappatura dei rischi e conseguentemente, se necessario, il MOGC, siano sempre aggiornati, mediante formulazione di proposte da sottoporre all'approvazione del CdA, qualora si verifichi una delle seguenti condizioni:

- variazioni dei requisiti di legge, così come definiti dal D.lgs. 231, in particolare a partire dalle fattispecie di reati previsti dallo stesso D.lgs. 231;
- variazioni significative nel profilo di rischio aziendale, anche a seguito di eventi che hanno condotto o potrebbero portare alla commissione dei reati di cui al D.lgs. 231.

5.3 Il Codice di etico

Il Codice etico è il documento all'interno del quale Cloud Care ha definito i principi guida che devono ispirare, per tutte le società del Gruppo, le condotte degli gli organi sociali e dei loro componenti, dei manager aziendali, dei dipendenti, dei soggetti esterni (consulenti, collaboratori, fornitori, partner in generale) che a vario titolo si relazionano con la Società nell'ambito delle proprie attività.

Tale documento ha lo scopo di sancire i fondamenti ed i comportamenti riconosciuti e condivisi da Cloud Care, da Investcorp e da tutte le società del gruppo e costituisce, unitamente alle policy in esso richiamate, al Sistema di Gestione Integrato aziendale, alle procedure e agli altri documenti prescrittivi che regolano le attività, il sistema di compliance del gruppo e uno degli elementi fondamentali del MOGC per la prevenzione ed il contrasto di possibili reati ai sensi del D.lgs. 231.

Al fine di garantire il rispetto del MOGC da parte di tutti i soggetti interessati, Cloud Care ha definito idonee clausole di adesione ai valori definiti in tutti i contratti dalla medesima stipulati.

5.4 Il Sistema dei controlli preventivi

5.4.1 I Protocolli e le altre misure di controllo e prevenzione

L'art. 6 del D. Lgs. 231 stabilisce, tra l'altro, al comma 2 lett. b) che il MOGC deve prevedere:

- specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati.

Pertanto Cloud Care ha impostato il MOGC come un **sistema strutturato ed organico di protocolli, policy, norme interne, procedure, sistemi di controllo** e idoneo ad assicurare che i processi e le attività particolarmente sensibili, in relazione alle fattispecie di reato previste dal D.lgs. 231, siano svolti in maniera controllata e nel rispetto di alcuni principi fondamentali, quali la verificabilità, documentabilità, coerenza e congruenza di ogni operazione, la separazione delle funzioni, la documentazione dei controlli stessi.

Tutto ciò in funzione del profilo di rischio così come individuato nella fase preliminare di valutazione.

Le misure di controllo e prevenzione previste nel MOGC e vincolanti per tutti i destinatari dello stesso, sono descritte nel documento MOGC – Parte Speciale.

Si sottolinea, peraltro, che l'elencazione presente nel citato documento non può dirsi in alcun modo esaustiva di tutte le disposizioni vincolanti del MOGC che, pertanto, deve essere sempre preso in considerazione nella sua interezza, ovvero costituito da tutti i documenti di cui si compone e che in esso vengono richiamati.

Tutti i destinatari del MOGC sono tenuti a uniformarsi ai controlli definiti da Cloud Care ed il mancato rispetto degli stessi è riportato all'attenzione dell'OdV.

Per un corretto funzionamento del MOGC è, pertanto, fondamentale che ciascuna funzione aziendale si attenga scrupolosamente a quanto in esso definito.

5.4.2 Comunicazione e formazione sul MOGC

L'attività di comunicazione e formazione deve essere improntata a principi di completezza, chiarezza, accessibilità e continuità, al fine di consentire ai diversi destinatari la piena consapevolezza delle disposizioni aziendali da rispettare e delle norme etiche che devono ispirare i loro comportamenti.

L'attività di comunicazione e formazione è supervisionata dall'OdV, cui sono assegnati, tra gli altri, i compiti di promuovere e definire le iniziative per la diffusione della conoscenza e della comprensione del MOGC, la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei contenuti del MOGC, nonché il promuovere ed elaborare interventi di comunicazione e formazione sui contenuti del D.lgs. 231, sugli impatti della normativa sull'attività dell'azienda e sulle norme comportamentali.

Al momento dell'assunzione l'area HR promuove la conoscenza del MOGC e del Codice Etico; in particolare ai neoassunti viene consegnata un'informativa con riferimento all'applicazione della normativa di cui al D.lgs.231 nell'ambito della Società e del Gruppo.

È inoltre prevista la pubblicazione di tutta la documentazione di riferimento in una sezione appositamente dedicata di Magncacarta.

La funzione HR cura e promuove adeguate iniziative di diffusione in caso di revisione del MOGC con il supporto dell'area QHSE.

L'attività di formazione, eventualmente anche tramite corsi on line, è differenziata, nei contenuti e nelle modalità di erogazione, in ragione del ruolo ricoperto dai destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno i destinatari funzioni di rappresentanza della Società.

Il materiale formativo viene reso disponibile a tutto il personale interessato attraverso i canali aziendali di comunicazione interna.

La partecipazione ai corsi di formazione ha carattere obbligatorio

A titolo meramente esemplificativo il contenuto della formazione sarà così articolato:

Per il personale direttivo e con funzioni di rappresentanza dell'ente: si procederà ad una formazione iniziale generale sulla normativa e sul MOGC e, successivamente, all'aggiornamento periodico nei casi di significativa modifica del MOGC, e, in particolare, nel caso di introduzione da parte del Legislatore di ulteriori reati presupposto.

Per il personale non direttivo coinvolto nelle attività sensibili: la formazione oltre ai contenuti generali descritti precedentemente, riguarderà in particolare procedure operative, disposizioni aziendali e ruolo dell'OdV. Anche in questo caso eventuali modifiche nella posizione organizzativa o nei processi aziendali potrebbero prevedere l'integrazione e l'aggiornamento della formazione.

Sarà cura dell'OdV verificare:

- la qualità dei corsi;
- la frequenza degli aggiornamenti;
- l'effettiva partecipazione agli stessi del personale.

Per i soggetti esterni, incluse le società controllate: verrà distribuita una nota informativa generale. Sarà cura dell'OdV verificarne l'adeguatezza e l'effettiva comunicazione.

6. I SISTEMI DI CONTROLLO SUCCESSIVI. SISTEMA DISCIPLINARE E MECCANISMI SANZIONATORI

L'esistenza di un sistema disciplinare in grado di scoraggiare l'adozione delle condotte vietate è condizione essenziale ed imprescindibile per assicurare l'efficienza e l'effettività del MOGC.

Gli articoli 6, comma 2, lett. e) (per i soggetti in posizione apicale) e 7, comma 4, lett. b) (per i soggetti sottoposti all'altrui direzione) del D.lgs. 231 sanciscono, infatti, espressamente, che il modello adottato debba prevedere "un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello".

Cloud Care ha adottato, unitamente agli altri protocolli costituenti il MOGC, un sistema disciplinare idoneo a sanzionare i comportamenti realizzati in violazione delle prescrizioni del MOGC stesso. Tale sistema è reso disponibile a tutti i soggetti in posizione apicale ed ai dipendenti attraverso i canali interni di comunicazione affinché ne sia garantita la piena conoscenza da parte di tutti i Destinatari.

Il sistema disciplinare è definito nel rispetto delle norme vigenti, ivi incluse, laddove applicabili, quelle previste nella contrattazione collettiva ed ha natura eminentemente interna a Cloud Care, non potendo ritenersi sostitutivo, bensì aggiuntivo rispetto alle norme di legge o di regolamento vigenti, nonché integrativo delle altre norme di carattere intra-aziendale, ivi incluse quelle di natura disciplinare.

I requisiti cui il sistema sanzionatorio deve rispondere, nel silenzio del D.lgs. 231, sono desumibili dalla dottrina e dalla giurisprudenza esistenti che li individua in:

- Specificità ed autonomia: la specificità si estrinseca nella predisposizione di un sistema sanzionatorio interno alla Società inteso a punire ogni violazione del MOGC, indipendentemente dal fatto che da essa consegua o meno la commissione di un reato; il requisito dell'autonomia, invece, si estrinseca nell'autosufficienza del funzionamento del sistema disciplinare interno rispetto ai sistemi esterni (es. giudizio penale), ovvero, la Società è chiamata a sanzionare la violazione indipendente dall'andamento del giudizio penale instauratosi e ciò in considerazione del tipo di violazione afferente i protocolli e le procedure previste nel MOGC;
- Compatibilità: il procedimento di accertamento e di comminazione della sanzione, nonché la sanzione stessa, non possono essere in contrasto con le norme di legge e con quelle contrattuali che regolano il rapporto di lavoro in essere con Cloud Care;
- Idoneità: il sistema deve essere efficiente ed efficace ai fini della prevenzione per la commissione dei reati;
- Proporzionalità: la sanzione applicabile od applicata deve essere proporzionata alla violazione rilevata;
- Redazione per iscritto e idonea divulgazione: il sistema sanzionatorio deve essere redatto per iscritto ed oggetto di diffusione, informazione e formazione puntuale per i destinatari.
- Oggetto di sanzione sono, in particolare, le violazioni del MOGC:
- commesse dai soggetti posti in posizione "apicale", in quanto titolari di funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e/o funzionale;
- titolari del potere, anche solo di fatto, di gestione o di controllo della Società;
- perpetrate dai soggetti sottoposti all'altrui direzione o vigilanza o operanti in nome e/o per conto della Società.

Cloud Care, consapevole della necessità di rispettare le norme di legge e le disposizioni vigenti in materia, assicura che le sanzioni irrogabili ai sensi del Sistema Disciplinare siano conformi a quanto previsto dai contratti collettivi nazionali del lavoro applicabili al settore, nella fattispecie dal CCNL Telecomunicazioni – Servizi di telefonia del 12/11/2020 tra Assotelecomunicazioni, Asstel e SLC-CGL, FISTEL-CISL, UILCOM-UIL, UGL Telecomunicazioni, dal CCNL per i Dirigenti del Commercio, assicura altresì, che sul piano procedurale, si applichi l'art. 7 della L. n. 300, 30.05.1970 (Statuto dei lavoratori) per la contestazione dell'illecito e per l'irrogazione della relativa sanzione.

Per i destinatari legati da contratti di natura diversa da un rapporto di lavoro dipendente (amministratori e, in generale, i soggetti esterni), le misure applicabili e le procedure sanzionatorie devono avvenire nel rispetto della legge e delle condizioni contrattuali.

In particolare, nel caso dei collaboratori coordinati e continuativi il cui rapporto di collaborazione rientra tra le casistiche previste dal D. Lgs 81/2015 in quanto compreso tra le collaborazioni per cui gli accordi collettivi nazionali stipulati da associazioni sindacali comparativamente più rappresentative sul piano nazionale prevedono discipline specifiche riguardanti il trattamento economico e normativo, in ragione delle particolari esigenze produttive ed organizzative del relativo settore, si fa riferimento all'Accordo Collettivo Nazionale per i collaboratori telefonici dei call center del 01/03/18 2018 tra Assocall e UGL al quale Assocontact, associazione datoriale di Cloud Care, ha aderito.

6.1 Destinatari e loro doveri

I destinatari del Sistema Disciplinare corrispondono ai destinatari del MOGC stesso.

I destinatari hanno l'obbligo di uniformare la propria condotta alle misure di organizzazione, gestione e controllo delle attività aziendali definite nel MOGC ed ai principi sanciti nel Codice etico.

Ogni eventuale violazione dei suddetti principi, misure e procedure, rappresenta, se accertata:

- nel caso di dipendenti e dirigenti, un inadempimento contrattuale in relazione alle obbligazioni che derivano dal rapporto di lavoro ai sensi di quanto pattuito secondo il CCNL applicabile, a gli artt. 2104 e 2106 del c.c.;
- nel caso di amministratori, l'inosservanza dei doveri ad essi imposti dalla legge e dallo statuto ai sensi dell'art. 2392 c.c.;
- nel caso dei sindaci, l'inosservanza dei doveri imposti dalla legge e dallo statuto ai sensi dell'art. 2403 c.c.;
- nel caso dei collaboratori coordinati e continuativi rappresenta giusta causa di cessazione del contratto e responsabilità del collaboratore ai sensi dell'art. 8 dell'Accordo Collettivo Nazionale per i collaboratori telefonici dei call center del 01/03/18;
- nel caso di altri Soggetti Esterni, costituisce inadempimento contrattuale e legittima a risolvere il contratto, fatto salvo il risarcimento del danno.

Il procedimento per l'irrogazione delle sanzioni tiene dunque conto delle particolarità derivanti dallo status giuridico del soggetto nei cui confronti si procede.

In ogni caso, l'OdV deve essere coinvolto nel procedimento d'irrogazione delle sanzioni disciplinari.

L'OdV verifica che siano adottate procedure specifiche per l'informazione di tutti i soggetti sopra previsti, sin dal sorgere del loro rapporto con la Società, circa l'esistenza ed il contenuto sistema sanzionatorio.

6.2 Le condotte rilevanti

Ai fini del Sistema Disciplinare di Cloud Care e nel rispetto delle previsioni di cui alla contrattazione collettiva (laddove applicabili), costituiscono violazioni del MOGC tutte le condotte, commissive o omissive (anche colpose), che siano idonee a ledere l'efficacia dello stesso quale strumento di prevenzione del rischio di commissione dei reati rilevanti ai fini del D.lgs.231.

Nel rispetto del principio costituzionale di legalità, nonché di quello di proporzionalità della sanzione, tenuto conto di tutti gli elementi e/o delle circostanze ad essa inerenti, si ritiene opportuno definire le possibili violazioni, graduate secondo un ordine crescente di gravità.

In particolare, per quanto concerne le attività sensibili identificate come a rischio di reato nelle sezioni del MOGC - Parte speciale, assumono rilevanza le seguenti condotte:

- violazioni di una o più regole procedurali e/o comportamentali previste nel MOGC e nei protocolli, configurabili come mancanze lievi;

- violazioni di una o più regole procedurali e/o comportamentali previste nel MOGC e nei Protocolli configurabili come mancanze più gravi se da esse non deriva pregiudizio alla normale attività della Società
- violazioni di una o più regole procedurali e/o comportamentali previste nel MOGC e nei Protocolli configurabili come mancanze ancor più gravi; violazioni idonee ad integrare l'elemento oggettivo di uno dei reati suscettibili di fondare la responsabilità dell'Ente;
- violazioni di una o più regole procedurali e/o comportamentali previste nel MOGC e nei Protocolli tali da ledere irreparabilmente il rapporto di fiducia non consentendo la prosecuzione del rapporto di lavoro; violazioni finalizzate alla commissione di uno dei reati idonei a fondare la responsabilità dell'Ente o comunque idonee ad ingenerare il pericolo che sia contestata la responsabilità della Società.

Il sistema sanzionatorio definisce inoltre, esplicitamente, le possibili violazioni concernenti il settore della salute e sicurezza sul lavoro e il settore ambientale anch'esse graduate secondo un ordine crescente di gravità.

6.3 Principi generali relativi alle sanzioni

Le sanzioni irrogate a fronte delle infrazioni devono, in ogni caso, rispettare il principio di gradualità e di proporzionalità rispetto alla gravità delle violazioni commesse.

La determinazione della tipologia, così come dell'entità della sanzione inflitta a seguito della commissione d'infrazioni, ivi compresi illeciti rilevanti ai sensi del D.lgs. 231, deve essere improntata al rispetto e alla valutazione di quanto segue:

- l'intenzionalità del comportamento da cui è scaturita la violazione;
- la negligenza, l'imprudenza e l'imperizia dimostrate dall'autore in sede di commissione della violazione, specie in riferimento alla effettiva possibilità di prevedere l'evento;
- la rilevanza ed eventuali conseguenze della violazione o dell'illecito;
- la posizione rivestita dal soggetto agente all'interno dell'organizzazione aziendale, specie in considerazione delle responsabilità connesse alle sue mansioni;
- eventuali circostanze aggravanti e/o attenuanti che possano essere rilevate in relazione al comportamento tenuto dal destinatario, tra le quali, è annoverata a titolo esemplificativo, la comminazione di precedenti sanzioni disciplinari a carico dello stesso soggetto nei due anni precedenti la violazione o l'illecito;
- il concorso di più destinatari, in accordo tra loro, nella commissione della violazione o dell'illecito.

L'iter di contestazione dell'infrazione e la comminazione della sanzione sono diversificate sulla base della categoria di appartenenza del soggetto agente.

6.3.1 Sanzioni nei confronti dei dipendenti

I comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dedotte nel presente MOGC sono definiti come illeciti disciplinari.

Le sanzioni irrogabili nei confronti dei dipendenti rientrano in quelle previste dal sistema disciplinare aziendale e/o dal sistema sanzionatorio previsto dal CCNL, nel rispetto delle procedure previste dall'articolo 7 dello Statuto dei lavoratori ed eventuali normative speciali applicabili.

Il sistema disciplinare aziendale della Società è quindi costituito dalle norme del codice civile in materia e dalle norme pattizie previste dal CCNL. In particolare, il sistema disciplinare descrive i comportamenti sanzionati, a seconda del rilievo che assumono le singole fattispecie considerate e le sanzioni in concreto previste per la commissione dei fatti stessi sulla base della loro gravità.

In relazione a quanto sopra, il MOGC fa riferimento alle sanzioni ed alle categorie di fatti sanzionabili previste dall'apparato sanzionatorio esistente nell'ambito del CCNL, al fine di ricondurre le eventuali violazioni del MOGC nelle fattispecie già previste dalle predette disposizioni.

Si precisa, ai sensi dell'art. 6 comma 2-bis lettera d) così come modificato dalla Legge 179/17, che le sanzioni dovranno essere applicate anche nei confronti di chi viola le misure di tutela del segnalante ("…..presentare a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente

decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate…").

Per quanto riguarda l'accertamento delle suddette infrazioni, il procedimento disciplinare e l'irrogazione delle sanzioni, restano invariati i poteri del datore di lavoro, eventualmente conferiti ad appositi soggetti all'uopo delegati.

È previsto il necessario coinvolgimento dell'Organismo di Vigilanza nella procedura di irrogazione delle sanzioni per violazione del MOGC, nel senso che non potrà essere irrogata una sanzione disciplinare per violazione del MOGC senza la preventiva comunicazione all'Organismo di Vigilanza.

Tale comunicazione diviene superflua allorquando la proposta per l'applicazione della sanzione provenga dall'Organismo di Vigilanza.

All'Organismo di Vigilanza dovrà essere data parimenti comunicazione di ogni provvedimento di archiviazione inerente i procedimenti disciplinari di cui al presente paragrafo.

Ai lavoratori verrà data un'immediata e diffusa informazione circa l'introduzione di ogni eventuale nuova disposizione, diramando una circolare interna per spiegare le ragioni e riassumerne il contenuto.

6.3.2 Sanzioni nei confronti dei dirigenti apicali

Il rapporto dirigenziale è rapporto che si caratterizza per la sua natura fiduciaria. Il comportamento del dirigente si riflette infatti non solo all'interno della Società, ma anche all'esterno; ad esempio, in termini di immagine rispetto al mercato e in generale rispetto ai diversi portatori di interesse.

Pertanto, il rispetto da parte dei dirigenti di quanto previsto nel MOGC e l'obbligo di farlo rispettare è considerato elemento essenziale del rapporto di lavoro dirigenziale, poiché costituisce stimolo ed esempio per tutti coloro che da questi ultimi, dipendono gerarchicamente.

Eventuali infrazioni poste in essere da dirigenti, in virtù del particolare rapporto di fiducia esistente tra gli stessi e la Società e della mancanza di un sistema disciplinare di riferimento, saranno sanzionate con i provvedimenti disciplinari ritenuti più idonei al singolo caso, sempre nel rispetto dei principi generali precedentemente individuati, compatibilmente con le previsioni di legge e contrattuali ed in considerazione del fatto che le suddette violazioni costituiscono, in ogni caso, inadempimenti alle obbligazioni derivanti dal rapporto di lavoro.

Gli stessi provvedimenti disciplinari sono previsti nei casi in cui un dirigente consenta, espressamente o per omessa vigilanza, di adottare, a dipendenti a lui sottoposti gerarchicamente, comportamenti non conformi al MOGC e/o in violazione dello stesso, ovvero comportamenti che possano essere qualificati come infrazioni.

È previsto il necessario coinvolgimento dell'OdV nella procedura di irrogazione delle sanzioni ai dirigenti per violazione del MOGC, nel senso che non potrà essere applicata alcuna sanzione per violazione del MOGC ad un dirigente senza il preventivo coinvolgimento dell'Organismo di Vigilanza.

Tale coinvolgimento si presume, quando la proposta per l'applicazione della sanzione provenga dall'Organismo di Vigilanza.

All'Organismo di Vigilanza dovrà essere data parimenti comunicazione di ogni provvedimento di archiviazione inerente ai procedimenti disciplinari di cui al presente paragrafo.

6.3.3 Misure nei confronti dei componenti il Consiglio di Amministrazione e il Collegio Sindacale

In caso di violazione del MOGC da parte del Presidente del CdA, dell'AD, di un componente del Consiglio di Amministrazione o del Collegio Sindacale, l'OdV informerà senza indugi0 e per iscritto, l'intero Consiglio di Amministrazione e il Collegio Sindacale.

L'Organo sociale cui il responsabile della violazione appartiene provvederà ad assumere le iniziative più opportune e adeguate coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo statuto, come previsto dal sistema disciplinare.

6.3.4 Misure nei confronti degli altri Soggetti Esterni

Qualsiasi condotta posta in essere da tutti i soggetti esterni che a qualunque titolo (collaboratori, consulenti, partner, fornitori) intrattengono rapporti con Cloud Care e che sia in contrasto con le regole definite nel MOGC, potrà determinare, come previsto dall'Accordo contrattuale applicabile, nel caso dei collaboratori del call center, o da specifiche clausole contrattuali inserite nelle lettere di incarico, negli accordi e nei contratti, l'immediata risoluzione del rapporto contrattuale.

Tali comportamenti saranno valutati dall'OdV che riferirà tempestivamente al CdA.

È compito dell'OdV, individuare e valutare l'opportunità dell'inserimento delle suddette clausole nei contratti che regolamentano il rapporto con detti soggetti nell'ambito delle attività aziendali potenzialmente esposte alla commissione dei reati di cui al D.lgs. 231.

Cloud Care si riserva altresì la facoltà di proporre domanda di risarcimento, qualora da tale condotta derivino alla stessa danni concreti, sia materiali (in particolare l'applicazione da parte del giudice delle misure pecuniarie o interdittive previste dal D. Lgs. 231) che di immagine.

7. APPLICAZIONE, AGGIORNAMENTO E DIFFUSIONE DEL MOGC

Come già illustrato precedentemente, tra i compiti affidati all'OdV rientra la cura dell'aggiornamento del MOGC.

L'OdV ha il compito di monitorare il necessario e continuo aggiornamento e adeguamento del MOGC e dei Protocolli ad esso connessi, eventualmente suggerendo mediante comunicazione scritta all'organo amministrativo o alle funzioni aziendali di volta in volta competenti le correzioni e gli adeguamenti necessari o opportuni.

Il Consiglio di Amministrazione è responsabile, unitamente alle funzioni aziendali eventualmente interessate, dell'aggiornamento del MOGC e del suo adeguamento in conseguenza di un mutamento degli assetti organizzativi o dei processi operativi, di significative violazioni del MOGC stesso, di integrazioni legislative. Gli aggiornamenti e adeguamenti del MOGC, o dei Protocolli ad esso connessi, sono comunicati mediante appositi avvisi inviati a mezzo mail, pubblicate sulla rete aziendale e, se del caso, attraverso la predisposizione di sessioni informative illustrative degli aggiornamenti e degli adeguamenti più significativi.

8. ALLEGATI E DOCUMENTI DI RIFERIMENTO COSTITUENTI IL MOGC

1. MOGC – PARTE GENERALE
2. MOGC – PARTE SPECIALE (inclusi i documenti in esso richiamati)
3. MOGC – CODICE ETICO
4. Allegato 1 MOGC Analisi preliminare dei rischi da reato
5. Allegato 2 MOGC Mappatura processi reati
6. Allegato 3 MOGC Relazione preliminare analisi dei rischi
7. Allegato 4 MOGC - SISTEMA DISCIPLINARE
8. Allegato 5 MOGC flussi comunicazione OdV
9. Documenti del Sistema di gestione integrato ISO 9001, ISO 14001, ISO 45001, ISO 27001, PAS 24000
10. Tutte le procedure e regolamenti aziendali
11. Codice etico
12. Policy aziendali
13. Documenti GDPR UE 2016/679
14. DVR