COMPUTER GROSS S.P.A.

MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
D.LGS. 8 GIUGNO 2001 N. 231

Approvato con delibera del
Consiglio di Amministrazione del
14 luglio 2025

Sede legale in Empoli (FI), Via del Pino 1
C.F.: 02500250168
P.IVA: 04801490485

Indice

- PARTE GENERALE I -

IL QUADRO NORMATIVO

1 IL DECRETO LEGISLATIVO 8 GIUGNO 2001 N. 231

1.1. LA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI

Il D.Lgs. 8 giugno 2001, n. 231, che reca la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" (di seguito anche il "**D.Lgs. 231/2001**" o, anche solo il "**Decreto**"), entrato in vigore il 4 luglio 2001 in attuazione dell'art. 11 della Legge-Delega 29 settembre 2000 n. 300, ha introdotto nell'ordinamento giuridico italiano, conformemente a quanto previsto in ambito comunitario, la responsabilità amministrativa degli enti[1].

Tale nuova forma di responsabilità, sebbene definita "amministrativa" dal legislatore, presenta i caratteri propri della responsabilità penale, essendo rimesso al giudice penale competente l'accertamento dei reati dai quali essa è fatta derivare ed essendo estese all'ente le medesime garanzie riconosciute alla persona sottoposta alle indagini o all'imputato nel processo penale.

La responsabilità amministrativa dell'ente deriva dalla consumazione di reati, espressamente indicati nel D.Lgs. 231/2001, commessi:

- nel suo interesse[2] o a suo vantaggio[3] (elemento oggettivo):
- da persone funzionalmente legate all'ente (elemento soggettivo), ed in particolare:
  a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso (c.d. **soggetti apicali**);
  b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a) (c.d. **soggetti sottoposti**).

La responsabilità dell'ente è esclusa laddove il reato sia stato posto in essere nell'esclusivo interesse dell'autore dell'illecito.

Oltre all'esistenza dei requisiti sopra descritti, il D.Lgs. 231/2001 richiede anche l'accertamento della colpevolezza dell'ente, al fine di poterne affermare la responsabilità. Tale requisito è riconducibile ad una "*colpa di organizzazione*", da intendersi quale mancata adozione, da parte dell'ente, di misure preventive

[1] L'art.1 del D.Lgs. n. 231 del 2001 ha delimitato l'ambito dei soggetti destinatari della normativa agli *"enti forniti di personalità giuridica, società e associazioni anche prive di personalità giuridica"*. Alla luce di ciò, la normativa si applica nei confronti degli:
- enti a soggettività privata, ovvero agli enti dotati di personalità giuridica ed associazioni "anche prive" di personalità giuridica;
- enti a soggettività pubblica, ovvero gli enti dotati di soggettività pubblica, ma privi di poteri pubblici (c.d. "enti pubblici economici");
- enti a soggettività mista pubblica/privata (c.d. "società miste").

Sono invece esclusi dal novero dei soggetti destinatari: lo Stato, gli enti pubblici territoriali (Regioni, Province, Comuni e Comunità montane), gli enti pubblici non economici e, in generale, tutti gli enti che svolgano funzioni di rilievo costituzionale (Camera dei deputati, Senato della Repubblica, Corte costituzionale, Segretariato generale della Presidenza della Repubblica, C.S.M., ecc.).

[2] L'interesse (da valutare *ex ante*) consiste nella prospettazione finalistica, da parte del reo-persona fisica che commette il reato, di conseguire un'utilità per l'ente a prescindere dall'effettivo conseguimento del beneficio per l'ente.

[3] Il vantaggio (da valutare *ex post*), corrisponde all'effettivo conseguimento di un beneficio per l'ente senza che sia necessario che il reo-persona fisica abbia volontariamente commesso il reato allo scopo di conseguire un'utilità per l'ente.

adeguate a prevenire la commissione dei reati previsti dal Decreto da parte dei soggetti individuati.

Là dove l'ente sia in grado di dimostrare di aver adottato, ed efficacemente attuato, un'organizzazione idonea ad evitare la commissione di tali reati, attraverso l'adozione del modello di organizzazione, gestione e controllo previsto dal D.Lgs. 231/2001, questi non risponderà a titolo di responsabilità amministrativa.

1.2. I REATI PREVISTI DAL DECRETO

I reati, dal cui compimento è fatta derivare la responsabilità amministrativa dell'ente, sono quelli espressamente e tassativamente richiamati dal D.Lgs. 231/2001.

Si rimanda all'Allegato 1 del presente documento per il dettaglio delle singole fattispecie di reato attualmente ricomprese nell'ambito di applicazione del D.Lgs. 231/2001 ("**reati presupposto**") precisando, tuttavia, che si tratta di un elenco destinato ad ampliarsi nel prossimo futuro.

1.3. LE SANZIONI COMMINATE DAL DECRETO

Il sistema sanzionatorio descritto dal D.Lgs. 231/2001, a fronte del compimento dei reati sopra elencati, prevede, a seconda degli illeciti commessi, l'applicazione delle seguenti sanzioni amministrative:

- sanzioni pecuniarie;
- sanzioni interdittive;
- confisca;
- pubblicazione della sentenza.

Le sanzioni pecuniarie:

Le sanzioni pecuniarie consistono nel pagamento di una somma di denaro nella misura stabilita dal Decreto, comunque non inferiore a euro 25.823 e non superiore a euro 1.549.370, da determinarsi in concreto da parte del Giudice mediante un sistema di valutazione bifasico (c.d. sistema "per quote").

Le sanzioni interdittive:

Le sanzioni interdittive sono le seguenti:

- interdizione dall'esercizio dell'attività;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- divieto di contrattare con la Pubblica Amministrazione;
- esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o revoca di quelli eventualmente già concessi;
- divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive si applicano, anche congiuntamente tra loro, esclusivamente in relazione ai reati per i quali sono espressamente previste dal Decreto, quando ricorre almeno una delle seguenti condizioni:

a) l'ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da un soggetto apicale ovvero da un soggetto subordinato quando, in quest'ultimo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;

b) in caso di reiterazione degli illeciti.

Quand'anche sussistano una o entrambe le precedenti condizioni, le sanzioni interdittive tuttavia non si applicano se sussiste anche solo una delle seguenti circostanze:

a) 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; oppure

b) il danno patrimoniale cagionato è di particolare tenuità; oppure

c) prima della dichiarazione di apertura del dibattimento di primo grado, concorrono tutte le seguenti condizioni (qui di seguito, Condizioni ostative all'applicazione di una sanzione interdittiva):

   1) 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;

   2) l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di un Modello;

   3) l'ente ha messo a disposizione il profitto conseguito ai fini della confisca.

Le sanzioni interdittive possono essere applicate anche in via cautelare su richiesta al Giudice da parte del Pubblico Ministero, quando ricorrono le seguenti condizioni:

- sussistono gravi indizi per ritenere la sussistenza della responsabilità dell'ente a norma del Decreto;
- vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede.

Il D.Lgs. 231/2001 prevede, inoltre, che qualora vi siano i presupposti per l'applicazione di una sanzione interdittiva che disponga l'interruzione dell'attività dell'ente, il giudice, in luogo dell'applicazione di detta sanzione, possa disporre la prosecuzione dell'attività da parte di un commissario giudiziale (art. 15 Decreto) nominato per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando 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 può provocare rilevanti ripercussioni sull'occupazione tenuto conto delle dimensioni dell'ente e delle condizioni economiche del territorio in cui è situato.

La confisca

La confisca consiste nell'acquisizione coattiva da parte dello Stato del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato e fatti in ogni caso salvi i diritti acquisiti dai terzi in buona fede; quando non è possibile eseguire la confisca in natura, la stessa può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato.

La pubblicazione della sentenza di condanna

La pubblicazione della sentenza di condanna consiste nella pubblicazione di quest'ultima una sola volta, per estratto o per intero, a cura della cancelleria del Giudice, a spese dell'ente, in uno o più giornali indicati dallo stesso Giudice nella sentenza, nonché mediante affissione nel Comune ove l'ente ha la sede principale.

La pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'ente viene applicata una sanzione interdittiva.

1.4. LA RESPONSABILITA' IN CASO DI VICENDE MODIFICATIVE DELL'ENTE

Il Decreto disciplina il regime della responsabilità dell'ente in caso di trasformazione, fusione, scissione e cessione.

In caso di trasformazione dell'ente resta ferma la responsabilità per i reati commessi anteriormente alla data in cui la trasformazione ha avuto effetto. Il nuovo ente sarà quindi destinatario delle sanzioni applicabili all'ente originario, per fatti commessi anteriormente alla trasformazione.

In caso di fusione, l'ente risultante dalla fusione stessa, anche per incorporazione, risponde dei reati dei quali erano responsabili gli enti che hanno partecipato alla fusione. Se essa è avvenuta prima della conclusione del giudizio di accertamento della responsabilità dell'ente, il Giudice dovrà tenere conto delle condizioni economiche dell'ente originario e non di quelle dell'ente risultante dalla fusione.

Nel caso di scissione, resta ferma la responsabilità dell'ente scisso per i reati commessi anteriormente alla data in cui la scissione ha avuto effetto; gli enti beneficiari della scissione sono solidalmente obbligati al pagamento delle sanzioni pecuniarie inflitte all'ente scisso nei limiti del valore del patrimonio netto trasferito ad ogni singolo ente, salvo che si tratti di ente al quale è stato trasferito anche in parte il ramo di attività nell'ambito del quale è stato commesso il reato. Le sanzioni interdittive si applicano all'ente (o agli enti) in cui sia rimasto o confluito il ramo d'attività nell'ambito del quale è stato commesso il reato. Se la scissione è avvenuta prima della conclusione del giudizio di accertamento della responsabilità dell'ente, il Giudice dovrà tenere conto delle condizioni economiche dell'ente originario e non di quelle dell'ente risultante dalla fusione.

In caso di cessione o di conferimento dell'ente nell'ambito della quale è stato commesso il reato, salvo il beneficio della preventiva escussione dell'ente cedente, il cessionario è solidalmente obbligato con l'ente cedente al pagamento della sanzione pecuniaria, nei limiti del valore dell'ente ceduto e nei limiti delle sanzioni pecuniarie che risultano dai libri contabili obbligatori o dovute per illeciti di cui il cessionario era comunque a conoscenza.

1.5. CONDIZIONE ESIMENTE DELLA RESPONSABILITÀ AMMINISTRATIVA

L'art. 6 del D.Lgs. 231/2001 stabilisce che l'ente non risponde a titolo di responsabilità amministrativa, qualora dimostri che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi (nel seguito anche il "**Modello**" o "**Modello 231**");
- il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curarne il relativo aggiornamento, è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo (nel seguito anche "**Organismo di Vigilanza**" o "**OdV**");
- le persone hanno commesso il reato eludendo fraudolentemente il Modello (qualora il reato sia stato commesso da un soggetto apicale);
- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

L'adozione del Modello 231 consente, dunque, all'ente di potersi sottrarre all'imputazione di responsabilità

amministrativa. La mera adozione di tale documento, con delibera dell'organo amministrativo dell'ente, non è, tuttavia, di per sé sufficiente ad escludere detta responsabilità, essendo necessario che il modello sia efficacemente ed effettivamente attuato.

Con riferimento all'efficacia del modello di organizzazione, gestione e controllo per la prevenzione della commissione dei reati previsti dal D.Lgs. 231/2001, si richiede che esso:

- individui le attività aziendali nel cui ambito possono essere commessi i reati;
- preveda specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individui modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- preveda obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
- introduca un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Con riferimento all'effettiva applicazione del Modello, il D.Lgs. 231/2001 richiede:

- una verifica periodica, e, nel caso in cui siano scoperte significative violazioni delle prescrizioni imposte dal Modello o intervengano mutamenti nell'organizzazione o nell'attività dell'ente ovvero modifiche legislative, la modifica del Modello;
- l'irrogazione di sanzioni in caso di violazione delle prescrizioni imposte dal Modello 231.

1.6. IL BENEFICIO DELLA RIDUZIONE DELLA DURATA DELLE SANZIONI INTERDITTIVE

Il comma 5-*bis* dell'art. 25 del D.Lgs. 231/01, introdotto dalla Legge Anticorruzione n. 3/2019 *"Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici"*, prevede una riduzione delle sanzioni interdittive in caso di consumazione dei reati di concussione, induzione indebita a dare o promettere utilità o corruzione (per un termine compreso tra 3 mesi e 2 anni).

Il beneficio è riconosciuto all'ente che, prima dell'emissione della sentenza di primo grado abbia 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, e si sia efficacemente adoperato:

- per evitare che l'attività delittuosa sia portata a conseguenze ulteriori;
- per assicurare le prove dei reati;
- per l'individuazione dei responsabili;
- per il sequestro delle somme o altre utilità trasferite.

1.7. LE "LINEE GUIDA" DI CONFINDUSTRIA

L'art. 6 del D.Lgs. 231/2001 dispone espressamente che i modelli di organizzazione, gestione e controllo possano essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti.

Ai fini della predisposizione del Modello, vengono quindi prese in considerazione le "*Linee guida per la*

costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001" (di seguito solo "Linee Guida") redatte da Confindustria da ultimo aggiornate nel giugno 2021.

Nella definizione del Modello di organizzazione, gestione e controllo, le Linee Guida di Confindustria prevedono le seguenti fasi progettuali:

- l'identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare in quali aree di attività e secondo quali modalità si possano verificare nel contesto aziendale i reati previsti dal D.Lgs. 231/2001;
- la predisposizione di un sistema di controllo idoneo a prevenire i rischi di reato identificati nella fase precedente, da effettuarsi attraverso la valutazione del sistema di controllo esistente e il relativo grado di adeguamento alle esigenze di prevenzione espresse dal D.Lgs. 231/2001.

Le componenti più rilevanti del sistema di controllo delineato nelle Linee Guida di Confindustria per garantire l'efficacia del modello di organizzazione, gestione e controllo sono di seguito riassunte:

- la previsione di principi etici e di regole comportamentali in un Codice Etico;
- un sistema organizzativo sufficientemente formalizzato e chiaro, in particolare con riguardo all'attribuzione di responsabilità, alle linee di dipendenza gerarchica e alla descrizione dei compiti;
- procedure manuali e/o informatiche che regolino lo svolgimento delle attività, prevedendo gli opportuni e adeguati controlli;
- poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali attribuite dall'ente, prevedendo, là dove opportuno, limiti di spesa;
- sistemi di controllo di gestione, capaci di segnalare tempestivamente possibili criticità;
- informazione e formazione del personale.

Le Linee Guida di Confindustria precisano, inoltre, che le componenti del sistema di controllo sopra descritte devono conformarsi ad una serie di principi di controllo, tra cui:

- verificabilità, tracciabilità, coerenza e congruità di ogni operazione, transazione e azione;
- applicazione del principio di separazione delle funzioni e segregazione dei compiti (nessuno può gestire in autonomia un intero processo);
- istituzione, esecuzione e documentazione dell'attività di controllo sui processi e sulle attività a rischio di reato;
- previsione di un adeguato sistema sanzionatorio per la violazione delle norme del Codice Etico e delle procedure previste dal Modello;
- individuazione dei requisiti dell'Organismo di Vigilanza, riassumibili come segue:
    - autonomia e indipendenza;
    - professionalità;
    - continuità d'azione;
    - obblighi di informazione dell'Organismo di Vigilanza.

È opportuno evidenziare che la difformità rispetto a punti specifici delle diverse Linee Guida non inficia di per sé la validità del Modello. Il singolo Modello, infatti, dovendo essere redatto con riguardo alla realtà

concreta dell'ente cui si riferisce, ben può discostarsi dalle Linee Guida che, per loro natura, hanno carattere generale.

1.8. EVOLUZIONE GIURISPRUDENZIALE

Ai fini della redazione del Modello, Computer Gross S.p.A. ha tenuto in considerazione le più importanti e recenti decisioni giurisprudenziali, tenendo conto dei principi dalle stesse affermati e degli orientamenti col tempo affermatisi.

- PARTE GENERALE II –

IL MODELLO ORGANIZZATIVO

2 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

2.1. LA SOCIETA'

Computer Gross S.p.A. (di seguito anche "Computer Gross" o la "Società") opera nel comparto informatico del terziario avanzato come distributore di soluzioni a valore aggiunto (VAS), proponendo soluzioni e servizi IT dei maggiori fornitori e produttori internazionali ("Vendor") e destinati ai principali rivenditori di prodotti IT software house, system integrator e dealer ("Partner"). La Società è organizzata in Business Unit con personale tecnico e commerciale dedicato a segmenti di mercato (software, networking, POS) e/o ai principali Vendor strategici. Oggi la Società fornisce altresì una completa gamma di soluzioni enterprise nell'ambito delle infrastrutture data center, con particolare attenzione alle tendenze che stanno caratterizzando la trasformazione digitale delle organizzazioni. Grazie alle sue partnership tecnologiche, Computer Gross offre un insieme completo di soluzioni di leader di mercato, integrandole con servizi tecnici, finanziari, marketing e formativi.
Con sede legale ad Empoli, Computer Gross assicura una puntuale presenza sul mercato attraverso rappresentanze commerciali e punti vendita dislocati sull'intero territorio nazionale.
La Società è certificata UNI PdR 125:2022, ISO 14001:2015, ISO/IEC 27001:2013 e ISO 9001:2015.

2.2. FINALITÀ DEL MODELLO

Computer Gross mira al rispetto di un insieme di regole e principi di comportamento che permettano alla Società di operare in maniera efficace e trasparente e di prevenire eventuali comportamenti non corretti o la commissione di illeciti da parte di chi opera in nome e per conto della stessa.

A tal fine, Computer Gross, consapevole dell'importanza di adottare, ed efficacemente attuare, un sistema idoneo a prevenire la commissione di comportamenti illeciti nel contesto aziendale, ha adottato – con delibera del Consiglio di Amministrazione in data 18 luglio 2013 – il Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001, da ultimo aggiornato con delibera del Consiglio di Amministrazione del 14 luglio 2025, sul presupposto che lo stesso costituisca un valido strumento di sensibilizzazione dei destinatari (come definiti al paragrafo 2.3) ad assumere comportamenti corretti e trasparenti, idonei pertanto a prevenire il rischio di commissione di illeciti penali ricompresi nel novero dei reati-presupposto della responsabilità amministrativa degli enti.

Attraverso l'adozione del Modello, la Società intende perseguire le seguenti finalità:

- vietare comportamenti che possano integrare le fattispecie di reato di cui al Decreto;
- determinare la piena consapevolezza in tutti coloro che operano in nome e per conto di Computer Gross di poter incorrere in un illecito, la cui commissione è fortemente censurata dalla Società, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, potrebbe trarne un vantaggio economico immediato;
- diffondere la consapevolezza che dalla violazione del Decreto, delle prescrizioni contenute nel Modello e dei principi del Codice Etico, possa derivare l'applicazione di misure sanzionatorie anche a carico della Società;

- consentire alla Società, grazie a un insieme di procedure e a una costante azione di monitoraggio sulla corretta attuazione di tale sistema, di prevenire e/o contrastare tempestivamente la commissione di reati rilevanti ai sensi del Decreto.

2.3. DESTINATARI

Le disposizioni del presente Modello sono vincolanti per l'intero Consiglio di Amministrazione, per tutti coloro che rivestono, in Computer Gross, funzioni di rappresentanza, amministrazione e direzione ovvero gestione e controllo (anche di fatto), per i dipendenti (da intendersi come tutti coloro che sono legati alla Società da un rapporto di lavoro subordinato, incluso il personale dirigente), e per i collaboratori sottoposti a direzione o vigilanza delle figure apicali della Società (di seguito i "**Destinatari**").

In particolare, destinatari del Modello sono:

- il Consiglio di Amministrazione e tutti coloro che rivestono funzioni di gestione e direzione nella Società o in una sua divisione e/o unità organizzativa dotata di autonomia finanziaria e funzionale, nonché coloro che esercitano anche di fatto la gestione e il controllo della Società;
- tutti coloro che intrattengono con la Società un rapporto di lavoro subordinato (dipendenti);
- tutti coloro che collaborano con la Società in forza di un rapporto di lavoro parasubordinato (es. apprendisti, ecc.);
- coloro i quali operano su mandato o per conto della Società nell'ambito delle attività sensibili, quali ad esempio i consulenti.

I soggetti ai quali il Modello si rivolge sono tenuti a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con la Società.

2.4. ELEMENTI FONDAMENTALI DEL MODELLO

Gli elementi fondamentali sviluppati da Computer Gross nella definizione del Modello, nel prosieguo dettagliatamente trattati, possono essere così riassunti:

- la mappatura delle attività a rischio di commissione del reato (cosiddette attività "sensibili"), con individuazione di esempi di possibili modalità di realizzazione dei reati, formalizzata nel documento denominato "*Report di Risk Assessment e Gap Analysis*" di cui al paragrafo 2.6;
- l'insieme di procedure e *policy* aziendali, a presidio di tutte le attività aziendali, ivi incluse - in particolare ai fini del presente Modello - quelle attività che, a seguito della menzionata attività di mappatura, sono risultate esposte a un rischio potenziale di commissione dei reati di cui al D.Lgs. 231/2001. Per il dettaglio circa le procedure e le policy aziendali adottate con riferimento a ciascun processo strumentale/sezione speciale si richiama l'Allegato 7 del Modello;
- l'istituzione di un Organismo di Vigilanza a composizione collegiale, cui sono attribuiti specifici compiti di vigilanza sull'efficace attuazione ed effettiva applicazione del Modello in conformità al Decreto;
- l'introduzione di un canale di segnalazione interna per la raccolta di segnalazioni ai sensi del D.Lgs. 10 marzo 2023 n. 24 ("**Decreto Whistleblowing**") di attuazione della Direttiva (UE)

2019/1937 che disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato;

- un sistema sanzionatorio volto a garantire l'efficace attuazione del Modello e contenente le azioni disciplinari e le misure sanzionatorie applicabili ai Destinatari, in caso di violazione delle prescrizioni contenute nel Modello, nella documentazione da esso richiamata e del Codice Etico;
- la previsione di attività di informazione e formazione sui contenuti del presente Modello;
- la previsione di principi di comportamento e protocolli di controllo definiti per ciascun processo strumentale/funzionale diretti a regolare le decisioni di Computer Gross declinati nelle Sezioni della "*Parte Speciale"* del presente Modello.

2.5. CODICE ETICO

Computer Gross, sensibile all'esigenza di improntare lo svolgimento delle attività aziendali al rispetto del principio di legalità, ha adottato il Codice Etico di Gruppo emesso dalla capogruppo Sesa S.p.A. (di seguito, alternativamente il "**Codice**" o il "**Codice Etico**"), di cui all'Allegato 5.

Il Codice sancisce una serie di principi, valori e norme di comportamento da applicare nella gestione aziendale che la Società riconosce come proprie e delle quali esige l'osservanza da parte sia dei propri organi sociali e dipendenti, sia dei terzi che, a qualunque titolo, intrattengano con essa rapporti commerciali.

Il Codice Etico ha, pertanto, una portata di carattere generale e rappresenta un insieme di regole, fatte proprie spontaneamente dalla Società, che la stessa riconosce, accetta e condivide, dirette a diffondere una solida integrità etica ed una forte sensibilità al rispetto delle normative vigenti.

Il rispetto del Codice Etico non serve pertanto soltanto a diffondere all'interno della Società una cultura sensibile alla legalità e all'etica, ma anche a tutelare gli interessi dei dipendenti e di coloro che hanno relazioni con la Società, preservando la Società da gravi responsabilità, sanzioni e danni reputazionali.

In considerazione del fatto che il Codice Etico richiama principi di comportamento (tra cui, legalità, correttezza e trasparenza) idonei anche a prevenire i comportamenti illeciti di cui al D.Lgs. 231/2001, tale documento acquisisce rilevanza ai fini del Modello e costituisce, pertanto, un elemento complementare allo stesso.

2.6. PERCORSO METODOLOGICO DI DEFINIZIONE DEL MODELLO: MAPPATURA DELLE ATTIVITÀ A RISCHIO-REATO - PROCESSI STRUMENTALI E PRESIDI

Il D.Lgs. 231/2001 prevede espressamente, all'art. 6, comma 2, lett. a), che il modello di organizzazione, gestione e controllo dell'ente individui le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Di conseguenza, la Società ha proceduto, con il supporto di un consulente esterno, ad un'analisi approfondita delle stesse. Nell'ambito di tale attività, la Società ha, in primo luogo, analizzato la propria struttura organizzativa rappresentata nell'organigramma aziendale che individua le Direzioni/Funzioni aziendali, evidenziandone ruoli e linee di riporto gerarchico-funzionali.

Computer Gross ha, successivamente, analizzato le proprie attività aziendali sulla base delle informazioni raccolte dai referenti aziendali (i.e. Responsabili di Direzione/Funzione) che, in ragione del ruolo ricoperto, risultano provvisti della più ampia e profonda conoscenza dell'operatività del settore aziendale di relativa competenza.

I risultati di detta attività sono stati raccolti nel documento denominato "*Report di Risk Assessment, Gap Analysis & Action Plan*" suddiviso nelle seguenti sezioni:

- Sez. I "*Mappatura delle attività a rischio reato*", che illustra il rischio potenziale di commissione dei reati previsti dal D.Lgs. 231/01 (classificato per famiglie di reato) in relazione a ciascuna attività sensibile identificata. L'individuazione del livello di rischio potenziale si è basata sulla valutazione della probabilità di accadimento delle fattispecie di reato (bassa – media - alta) legata alla tipicità della condotta descritta nella norma e alla specifica attività aziendale svolta dalla Società;
- Sez. II "*Gap Analysis & Action Plan*", in cui sono stati individuati e valutati i presidi di controllo adottati dalla Società, sia quelli di natura "trasversale", che quelli specifici di ogni area a rischio/attività sensibile, con rilievo di eventuali gap e indicazione di suggerimenti/azioni di implementazione proposte allo scopo, non solo di migliorare il sistema di controllo interno, ma anche di mitigare il rischio di commissione dei reati previsti dal D.Lgs. 231/01. All'interno di questa sezione, per ciascuna attività sensibile, sono stati inoltre individuati i processi strumentali considerati a rischio potenziale di commissione dei reati 231 e i referenti coinvolti.
- Sez. III "*Risk Assessment*", che identifica, sulla base del rischio potenziale e del sistema di controllo rilevati, il rischio residuo di consumazione dei reati 231 sulla base di un giudizio che bilancia, per ciascuna area a rischio, il rischio potenziale con il controllo posto in essere dalla Società. All'interno del documento, conformemente a quanto stabilito dalle Linee Guida di Confindustria, sono state altresì descritte alcune fattispecie di reato consumabili in ciascuna area a rischio, con esempi di condotte illecite e possibili finalità perseguibili dalla Società nella consumazione del reato stesso.

Il Report di *Risk Assessment, Gap Analysis & Action Plan* è custodito dalle funzioni LegalVAS e Compliance di Gruppo, che ne curano congiuntamente l'archiviazione, rendendola disponibile - per eventuale consultazione – a chiunque sia autorizzato dalla Società a prenderne visione.

2.6.1 Le attività sensibili

Nello specifico, dall'analisi della realtà aziendale di Computer Gross sono state individuate le seguenti attività sensibili, così come descritte nell'Allegato 2 al seguente Modello:

- Gestione dei rapporti con la PA per gli adempimenti connessi all'attività tipica aziendale (ad es. Agenzia delle Entrate, Agenzia delle Dogane, ASL, INPS, DTL, ecc.);
- Acquisizione e gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici;
- Gestione delle visite ispettive da parte di esponenti della Pubblica Amministrazione (ad es. GdF, Agenzia delle Entrate, Agenzia delle Dogane, ASL, Garante Privacy, ecc.);
- Gestione della fiscalità e della contabilità;
- Gestione dei flussi finanziari-pagamenti e incassi;
- Gestione dei rapporti con il Socio Unico, il Collegio Sindacale e la Società di Revisione;

- Predisposizione del bilancio (incluse poste estimative) e relative comunicazioni;
- Operazioni relative al capitale sociale: gestione di conferimenti, dei beni sociali, degli utili e delle riserve. Delle operazioni sulle partecipazioni e sul capitale;
- Selezione e assunzione delle risorse umane;
- Gestione del personale (payroll, note spese, rapporti con i sindacati, benefit, incentivi e premi);
- Attività di selezione e valutazione dei fornitori;
- Approvvigionamento di beni e di servizi;
- Attività di sviluppo commerciale, vendita e gestione dei rapporti con gli agenti e incaricati alla vendita;
- Attività di assistenza post-vendita;
- Gestione delle attività di marketing;
- Gestione delle sponsorizzazioni e omaggi;
- Attività di gestione della qualità, compliance e delle certificazioni;
- Attività di gestione del magazzino e degli inventari;
- Attività di import/export;
- Gestione dei sistemi informativi;
- Gestione del sistema della salute e sicurezza sul lavoro;
- Gestione degli aspetti ambientali (rifiuti);
- Gestione del contenzioso giudiziale e stragiudiziale;
- Gestione dei rapporti infragruppo.

2.6.2 Processi aziendali "strumentali/funzionali"

Nell'ambito delle attività sopra rappresentate, sono stati anche individuati dalla Società i processi aziendali c.d. strumentali/funzionali alla commissione del reato, ovverosia quei processi aziendali nel cui ambito, in linea di principio, potrebbero verificarsi le condizioni e/o essere rinvenuti i mezzi per la commissione delle fattispecie di reato rilevanti ai fini del Decreto e a cui sono state ricondotte le attività sensibili.

Vengono di seguito riportati tali processi:

1. Rapporti con la Pubblica Amministrazione e le Autorità Amministrative Indipendenti;
2. Gestione dei flussi finanziari, della fiscalità e della contabilità;
3. Selezione, assunzione e gestione del personale;
4. Gestione del ciclo passivo (acquisti);
5. Gestione del ciclo attivo (vendite);
6. Gestione del processo qualità, compliance e certificazioni;

7. Gestione delle attività di import/export;
8. Gestione delle attività di marketing, omaggi e sponsorizzazioni;
9. Gestione degli adempimenti in materia di salute e sicurezza nei luoghi di lavoro ai sensi del D.Lgs. 81/2008;
10. Gestione degli adempimenti in materia ambientale;
11. Gestione della sicurezza e manutenzione dei sistemi informativi;
12. Formazione del bilancio d'esercizio e gestione dei rapporti con il socio;
13. Gestione dei rapporti con l'Autorità Giudiziaria;
14. Gestione dei rapporti intercompany.

A ciascun processo strumentale/funzionale, rilevante nella realtà aziendale, ritenuto a rischio di commissione dei reati previsti dal Decreto, è stata dedicata una specifica Sezione della Parte Speciale del presente Modello ove sono stati formulati i c.d. **"Protocolli di controllo"**, adottati dalla Società per prevenire il rischio di commissione del reato nella gestione delle attività sensibili e dei processi strumentali/funzionali associati ai reati previsti dal D.Lgs. 231/2001.

2.7. LA STRUTTURA DEL SISTEMA ORGANIZZATIVO E DI CONTROLLO

Nella predisposizione del Modello e sulla base delle aree di attività a rischio-reato risultate rilevanti, la Società ha riesaminato il sistema organizzativo e di controllo esistente, strutturato in una serie complessa di presidi, al fine di verificare se esso fosse idoneo a prevenire gli specifici reati previsti dal Decreto.

In particolare, il sistema organizzativo e di controllo di Computer Gross si basa, oltre che sui principi di comportamento e sui protocolli di controllo declinati nella Parte Speciale, altresì sui seguenti elementi:

- il quadro normativo e regolamentare, nazionale, comunitario e internazionale, applicabile a Computer Gross;
- il Codice Etico, che – come sopra già rappresentato al paragrafo 2.5 – sancisce principi e regole di condotta adottate dalla Società;
- il sistema di deleghe e procure esistente (cui si rimanda ai par. 2.8 e 2.9);
- la struttura gerarchico-funzionale (*cfr*. organigramma aziendale, anche con riferimento alla Salute e Sicurezza sui luoghi di lavoro). Detto documento riflette i cambiamenti effettivamente intervenuti nella struttura organizzativa ed è, pertanto, tenuto costantemente aggiornato;
- l'utilizzo di applicativi gestionali in grado di assicurare segregazione dei ruoli, livelli autorizzativi e controlli automatici;
- i principi di comportamento e i protocolli di controllo declinati nelle Sezioni della Parte Speciale del presente Modello;
- l'implementazione di sistemi informativi integrati, orientati alla segregazione delle funzioni, nonché ad un elevato livello di standardizzazione dei processi e alla protezione delle informazioni in essi contenute, con riferimento sia ai sistemi gestionali e contabili che ai sistemi a supporto delle attività operative connesse al *business*.

L'attuale sistema organizzativo e di controllo di Computer Gross, inteso come apparato volto a gestire e monitorare i principali rischi aziendali, assicura il raggiungimento dei seguenti obiettivi:

- efficacia ed efficienza nell'impiegare le risorse aziendali, nel proteggersi dalle perdite e nel salvaguardare il patrimonio della Società;
- rispetto delle leggi e dei regolamenti applicabili in tutte le operazioni ed azioni della Società;
- affidabilità delle informazioni, da intendersi come comunicazioni tempestive e veritiere a garanzia del corretto svolgimento di ogni processo decisionale.

Alla base di detto sistema sono posti i seguenti principi, ripresi e declinati nelle procedure aziendali e nei protocolli di controllo:

- ogni operazione, transazione e azione deve essere verificabile, documentata, coerente e congrua;
- il sistema garantisce, anche attraverso una coerente attribuzione di poteri e deleghe e di livelli autorizzativi, l'applicazione del principio di segregazione dei compiti (per il quale nessuno deve poter gestire un intero processo in autonomia) e indipendenza funzionale;
- il sistema di controllo interno documenta l'esecuzione dei controlli, anche di supervisione.

La responsabilità in ordine al corretto funzionamento del sistema dei controlli interni è rimessa a ciascuna Direzione/Funzione per tutti i processi di cui essa sia responsabile.

La struttura dei controlli aziendali esistente si articola in:

- controlli di linea, svolti dalle singole Direzioni/Funzioni sui processi di cui hanno la responsabilità gestionale, finalizzati ad assicurare il corretto svolgimento delle operazioni;
- riporti funzionali di Gruppo.

Si segnala altresì che la Società, in conformità al contenuto dell'articolo 6, comma 2 lettera c) del D.Lgs. 231/01, utilizza strumenti informatici, procedure e risorse qualificate - si prefigge l'obiettivo: *i)* di realizzare una gestione dei flussi finanziari ordinata e trasparente; *ii)* di contrastare ogni possibile fenomeno di creazione di fondi occulti e/o provviste destinate alla commissione dei reati previsti dal Decreto stesso.

2.8. IL SISTEMA DI DELEGHE E PROCURE DELLA SOCIETÀ

Il sistema autorizzativo e decisionale si traduce in un sistema articolato e coerente di deleghe di funzioni e procure della Società, fondato sulle seguenti prescrizioni:

- le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;
- ciascuna delega deve definire e descrivere in modo specifico e non equivoco i poteri gestionali del delegato ed il soggetto cui il delegato riporta gerarchicamente/funzionalmente;
- i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli;

- le procure possono essere conferite esclusivamente a soggetti dotati di delega funzionale interna o di specifico incarico e devono prevedere l'estensione dei poteri di rappresentanza e, eventualmente, i limiti di spesa numerici;
- tutti coloro che intrattengono per conto di Computer Gross rapporti con la Pubblica Amministrazione devono essere dotati di delega/procura in tal senso.

2.9. LA STRUTTURA ORGANIZZATIVA IN MATERIA DI SALUTE, SICUREZZA, AMBIENTE

2.9.1. La salute e la sicurezza sul luogo di lavoro

In materia di salute e sicurezza nei luoghi di lavoro, la Società si è dotata di una struttura organizzativa ai sensi del D.Lgs. 81/2008 e s.m.i. (c.d. "**Testo Unico Sicurezza**"), nell'ottica di eliminare ovvero, là dove ciò non sia possibile, ridurre al minimo i rischi di omicidio colposo e di lesioni colpose gravi o gravissime per i lavoratori.

Il ruolo di Datore di Lavoro ai sensi dell'art. 2 del D.Lgs. 81/2008 è in capo al Presidente del Consiglio di Amministrazione – Sig. Paolo Castellacci.

Nell'ambito di tale struttura organizzativa, operano i soggetti di seguito elencati:

- Datore di Lavoro ex art. 2 D.Lgs. 81/2008 (Consigliere Delegato – Sig. Paolo Castellacci)
- Delegato del Datore di Lavoro ex art. 16 del D.Lgs. 81/2008;
- Responsabile al servizio di prevenzione e protezione (RSPP);
- Rappresentante dei lavoratori per la sicurezza (RLS);
- Preposti;
- Medico competente;
- Addetti al primo-soccorso;
- Addetti alla prevenzione degli incendi;
- Addetti al defibrillatore;
- I lavoratori.

Il D.Lgs. 81/2008 rimette al Datore di Lavoro ogni valutazione in merito all'opportunità di delegare specifiche funzioni in materia di salute e sicurezza, mediante delega di funzioni predisposta in conformità all'art. 16 del D.Lgs. 81/2008, a soggetti aziendali dotati di adeguata capacità tecnica, professionalità ed esperienza nella materia.

È competenza specifica del Datore di Lavoro sottoscrivere il Documento di Valutazione dei Rischi ("**DVR**") quale formalizzazione organizzata da parte dell'azienda, della valutazione di tutti i rischi in materia di salute e sicurezza dei lavoratori durante l'esercizio delle rispettive attività e le misure idonee alla prevenzione di infortuni e incidenti attraverso la riduzione del rischio.

I compiti e le responsabilità dei soggetti sopra indicati sono definiti formalmente in coerenza con lo schema organizzativo e funzionale della Società, con riferimento alle figure specifiche operanti nell'ambito delle attività a rischio-reato in materia di salute e sicurezza nei luoghi di lavoro.

Il sistema di gestione degli adempimenti in materia di salute e sicurezza nei luoghi di lavoro di Computer Gross (come indicati, altresì, nella Sezione 9 della Parte Speciale, cui si rimanda) prevede un sistema di controllo anche sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate, attraverso l'opera del RSPP.

Il sistema prevede, inoltre, il riesame e l'eventuale modifica delle soluzioni adottate quando vengono scoperte violazioni significative delle norme relative alla prevenzione degli infortuni, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico (attività svolta per il tramite del RSPP competente, in funzione di quanto previsto dall'art. 28 del D. Lgs. 81/2008 e in occasione della riunione periodica di cui all'art. 35 del D. Lgs. 81/2008).

2.9.2 La tutela ambientale

La Società ha ottenuto la certificazione secondo la norma UNI ISO 14001:2015 e ha adottato una struttura organizzativa ai sensi del D.Lgs. 152/2006 – Norme in materia ambientale -, nell'ottica di eliminare, ovvero là dove ciò non sia possibile, ridurre al minimo i rischi per l'ambiente oltre che per la salute dei lavoratori e della popolazione circostante. Tale struttura organizzativa prevede il mantenimento e lo sviluppo di un sistema di gestione ambientale conforme alla norma UNI ISO 14001:2015 che viene verificato almeno annualmente da un ente terzo indipendente. Viene inoltre individuato all'interno dell'Organo Amministrativo, l'Amministratore Delegato a porre in essere ogni azione utile a garantire la conformità ambientale della Società con facoltà di delegare i relativi adempimenti tecnico operativi alle funzioni preposte sia interne che, quando opportuno e sulla base di specifici accordi di servizio, esterne alla società. Apposito programma formativo diffuso al personale garantisce una adeguata attenzione alle tematica ambientale da parte di tutte le funzioni della Società.

La Società non produce emissioni in atmosfera né scarichi idrici industriali.

3 L' ORGANISMO DI VIGILANZA

L'art. 6, comma 1, del D.Lgs. 231/2001 richiede, quale condizione per beneficiare dell'esimente dalla responsabilità amministrativa, che il compito di vigilare sull'osservanza e funzionamento del Modello, curandone il relativo aggiornamento, sia affidato ad un Organismo di Vigilanza interno all'ente che, dotato di autonomi poteri di iniziativa e di controllo, eserciti in via continuativa i compiti ad esso affidati.

Il Decreto richiede che l'Organismo di Vigilanza svolga le sue funzioni al di fuori dei processi operativi della Società, riferendo periodicamente al Consiglio di Amministrazione, svincolato da ogni rapporto gerarchico con il Consiglio stesso e con i singoli responsabili delle Direzioni/Funzioni.

L'OdV di Computer Gross può essere affidato ad un organo sia monocratico che collegiale. Nel caso di scelta di un organo monocratico, il componente dell'OdV deve essere un soggetto esterno, oppure essere identificato nel responsabile di idonee funzioni di controllo della capogruppo ancorché dotato dei necessari requisiti di indipendenza organizzativa, autonomia di azione e professionalità. Nel caso in cui le funzioni dell'Odv venissero attribuite ad un organo collegiale, questo potrà essere composto da:

- due componenti, di cui almeno uno esterno alla Società (che assume il ruolo di presidente);
- tre membri di cui almeno due di essi esterni alla Società (tra i quali deve essere scelto, a cura dell'OdV stesso, il presidente).

Le funzioni dell'OdV possono essere conferite, altresì, al Collegio Sindacale ai sensi del art. 6 comma 4-bis del Decreto.

In ossequio alle prescrizioni dell'art. 6, comma 4-bis, del D.Lgs. 231/2001, il Consiglio di Amministrazione di Computer Gross ha nominato – con delibera del 12 settembre 2024 – il Collegio Sindacale quale Organismo di Vigilanza collegiale, composto da n. 3 componenti, funzionalmente dipendente dal Consiglio medesimo.

In particolare, la composizione dell'Organismo di Vigilanza è stata definita in modo da garantire i seguenti requisiti:

- *Autonomia e indipendenza*: detto requisito è assicurato dalla composizione collegiale e dall'attività di *reporting* direttamente al Consiglio di Amministrazione, senza tuttavia vincolo di subordinazione gerarchica rispetto a detto organo.
- *Professionalità*: requisito garantito dal bagaglio di conoscenze professionali, tecniche e pratiche di cui dispongono i componenti dell'Organismo di Vigilanza. In particolare, la composizione prescelta garantisce idonee conoscenze giuridiche e dei principi e delle tecniche di controllo e monitoraggio.
- *Continuità d'azione*: con riferimento a tale requisito, l'Organismo di Vigilanza è tenuto a vigilare costantemente, attraverso poteri di indagine, sul rispetto del Modello da parte dei Destinatari, a curarne l'attuazione e l'aggiornamento, rappresentando un riferimento costante per tutto il personale di Computer Gross.

3.1. DURATA IN CARICA, DECADENZA E REVOCA

L'Organismo di Vigilanza resta in carica per il periodo determinato dal Consiglio di Amministrazione nella delibera consiliare di istituzione dell'Organismo. I componenti dell'Organismo sono scelti tra soggetti in possesso di un profilo etico e professionale di indiscutibile valore e non debbono essere in rapporti di coniugio o parentela entro il secondo grado con i Consiglieri di Amministrazione.

I membri dell'Organismo di Vigilanza rimangono in ogni caso in carica oltre la scadenza fissata nella delibera consigliare di relativa nomina fino a quando il Consiglio di Amministrazione non abbia provveduto con specifica delibera consigliare alla nomina dell'Organismo di Vigilanza nella nuova composizione o abbia confermato quella precedente.

Possono essere nominati componenti dell'Organismo di Vigilanza dipendenti della Società e professionisti esterni. Detti ultimi non debbono avere con la Società rapporti tali da integrare ipotesi di conflitto di interessi e da pregiudicarne l'indipendenza.

Il Consiglio di Amministrazione nomina e revoca il Presidente dell'Organismo di Vigilanza. In mancanza di nomina da parte dell'organo amministrativo, lo stesso verrà eletto dal medesimo Organismo di Vigilanza.

I compensi dei componenti dell'Organismo di Vigilanza non costituiscono ipotesi di conflitto di interessi.

Non può essere nominato componente dell'Organismo di Vigilanza, e, se nominato decade:

- l'interdetto, l'inabilitato, il fallito o chi è stato condannato, ancorché con condanna non definitiva, ad una pena che importi l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità di esercitare uffici direttivi, ovvero sia stato condannato, anche con sentenza non definitiva o con sentenza di applicazione della pena su richiesta delle parti *ex* art. 444 c.p.p. (c.d. sentenza di patteggiamento), per aver commesso uno dei reati previsti dal D.Lgs. 231/2001;
- essere titolare, direttamente o indirettamente, di partecipazioni azionarie in Computer Gross o Società controllanti, controllate o collegate tali da permettere di esercitare il controllo o un'influenza notevole sulla Società, ovvero comunque da comprometterne l'indipendenza;

- essere titolari di deleghe, procure o, più in generale, poteri o compiti o rapporti economici, di collaborazione o consulenziali che possano pregiudicarne l'indipendenza del giudizio o della funzione;
- avere rapporti di coniugio, parentela o di affinità entro il quarto grado con amministratori o soggetti apicali della Società o con amministratori non indipendenti di altre società appartenenti al gruppo Sesa;
- essere stato sottoposto a misure di prevenzione disposte dall'autorità giudiziaria, salvi gli effetti della riabilitazione;
- essere destinatari di un provvedimento di applicazione di una sanzione in sede amministrativa per uno degli illeciti amministrativi di cui agli articoli 185, 187-bis e 187- ter del TUF.

I componenti che abbiano un rapporto di lavoro subordinato con la Società decadono automaticamente dall'incarico, in caso di cessazione di detto rapporto, e indipendentemente dalla causa di interruzione dello stesso, o di assunzione di nuova mansione incompatibile con i requisiti per la composizione dell'OdV.

Il Consiglio di Amministrazione può revocare, con delibera consiliare, i componenti dell'Organismo in ogni momento ma solo per giusta causa.

Costituiscono giusta causa di revoca dei componenti:

- l'omessa comunicazione al Consiglio di Amministrazione di un conflitto di interessi che impedisca il mantenimento del ruolo di componente dell'Organismo stesso;
- la violazione degli obblighi di riservatezza in ordine alle notizie e informazioni acquisite nell'esercizio delle funzioni proprie dell'Organismo di Vigilanza;
- per i componenti legati alla Società da un rapporto di lavoro subordinato, l'avvio di un procedimento disciplinare per fatti da cui possa derivare la sanzione del licenziamento;
- la sentenza di applicazione della pena su richiesta delle parti *ex* art. 444 c.p.p. (c.d. sentenza di patteggiamento), ove risulti dagli atti l'omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Qualora la revoca avvenga senza giusta causa, il componente revocato potrà chiedere di essere immediatamente reintegrato in carica.

Costituisce, invece, causa di decadenza dell'intero Organismo di Vigilanza:

- l'accertamento di un grave inadempimento da parte dell'Organismo di Vigilanza nello svolgimento dei propri compiti di verifica e controllo;
- la sentenza di condanna della Società, anche non divenuta irrevocabile, ove risulti dagli atti l'omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Ciascun componente può recedere in ogni momento dall'incarico con preavviso scritto di almeno 30 giorni, da comunicarsi al Presidente del Consiglio di Amministrazione a mezzo di raccomandata A.R., che riferirà in Consiglio di Amministrazione.

Nel caso in cui a seguito di revoca, recesso o decadenza di uno dei due componenti o altro fatto che possa ridurre la composizione dell'Organismo di Vigilanza a un componente, lo stesso Organismo potrà in ogni caso svolgere le proprie funzioni e operare fino alla data della delibera consigliare integrativa della

composizione con la nomina del componente mancante, che dovrà avvenire entro massimo tre mesi dalla causa di revoca, recesso o decadenza dalla carica.

L'Organismo di Vigilanza provvede a disciplinare in autonomia le regole per il proprio funzionamento in un apposito Regolamento, in particolare definendo le modalità operative per l'espletamento delle funzioni ad esso rimesse.

3.2. POTERI E FUNZIONI DELL'ORGANISMO DI VIGILANZA

All'Organismo di Vigilanza sono affidati i seguenti compiti:

- vigilare sulla diffusione all'interno della Società della conoscenza, della comprensione e dell'osservanza del Modello;
- vigilare sull'osservanza del Modello da parte dei Destinatari nell'ambito delle aree di attività potenzialmente a rischio di reato;
- Verificare l'adeguatezza del Modello 231 rispetto alle previsioni del Decreto e alle evoluzioni giurisprudenziali in materia, curando in particolare la sua efficacia a prevenire comportamenti illeciti;
- segnalare alla Società l'opportunità di aggiornare il Modello, là dove si riscontrino esigenze di adeguamento in relazione a mutate condizioni aziendali e/o normative o significative violazioni delle prescrizioni del Modello stesso.

L'OdV si riunisce con cadenza almeno trimestrale e le deliberazioni sono prese a maggioranza assoluta di voti. A parità di voti prevale quello di chi presiede la riunione.

Nello svolgimento di dette attività, l'Organismo provvede ai seguenti adempimenti:

- coordinarsi e collaborare con le Direzioni/Funzioni aziendali (anche attraverso apposite riunioni) per il miglior monitoraggio delle attività aziendali identificate nel Modello a rischio reato;
- effettuare verifiche mirate su determinate operazioni o su atti specifici, posti in essere nell'ambito delle aree di attività aziendale individuate a potenziale rischio di reato, anche con il supporto delle Direzioni/Funzioni aziendali;
- verificare l'effettivo svolgimento delle iniziative di informazione e formazione sul Modello intraprese dalla Società, supportando la funzione responsabile dell'attività di formazione – su richiesta – nella verifica della relativa adeguatezza;
- verificare l'istituzione e il funzionamento di uno specifico canale informativo "dedicato" (l'indirizzo di posta elettronica odv231@computergross.it), diretto a facilitare il flusso di informazioni verso l'Organismo da parte delle Direzioni/Funzioni aziendali coinvolte nei processi aziendali potenzialmente a rischio di reato;
- segnalare immediatamente al Consiglio di Amministrazione eventuali violazioni del Modello, ritenute fondate, da parte degli Amministratori della Società, nel rispetto della normativa whistleblowing in vigore;
- segnalare immediatamente al Socio Unico eventuali violazioni del Modello, ritenute fondate, da parte dell'intero Consiglio di Amministrazione, nel rispetto della normativa whistleblowing in vigore.

Ai fini dello svolgimento degli adempimenti sopra elencati, l'Organismo è dotato dei poteri di seguito indicati:

- emanare disposizioni e ordini di servizio intesi a regolare le proprie attività e predisporre e aggiornare l'elenco delle informazioni, dette "**Flussi Informativi**" (come definiti al paragrafo 3.4.), che devono pervenirgli dalle Direzioni/Funzioni aziendali;
- accedere, senza autorizzazioni preventive, a ogni documento aziendale rilevante per lo svolgimento delle funzioni allo stesso attribuite dal D.Lgs. 231/2001;
- disporre che i responsabili delle Direzioni/Funzioni aziendali e, in ogni caso, tutti i Destinatari, forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso;
- ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo, ovvero di aggiornamento del Modello.

Per un miglior svolgimento delle proprie attività, l'Organismo può delegare uno o più compiti specifici a singoli suoi componenti, che li svolgeranno in nome e per conto dell'Organismo stesso. In merito ai compiti delegati, la responsabilità da essi derivante ricade sull'Organismo nel suo complesso.

Per lo svolgimento delle proprie attività l'OdV predispone:

- un Programma Annuale della vigilanza in coerenza con i principi contenuti nel Modello 231, che riporta le attività programmate ed i relativi interlocutori.
- un Rapporto annuale relativo all'attività svolta, in ordine all'attuazione del Modello, all'emersione di eventuali aspetti critici e comunica l'esito delle attività svolte nell'esercizio dei compiti assegnati.

Le attribuzioni dell'OdV non costituiscono in alcun modo limitazione o deroga alle prerogative e ai doveri del vertice societario (CdA e Amministratore Delegato), il quale continua anche dopo l'adozione del Modello a mantenere la piena operatività delle attribuzioni connesse allo svolgimento del proprio Ufficio, con ogni conseguente potere e responsabilità di legge.

Il Consiglio di Amministrazione della Società assegna all'Organismo di Vigilanza un *budget* di spesa annuale nell'importo proposto dall'Organismo stesso e, in ogni caso, adeguato rispetto alle funzioni ad esso rimesse. L'Organismo delibera in autonomia le spese da sostenere nel rispetto dei poteri di firma aziendali e, in caso di spese eccedenti il *budget*, viene autorizzato direttamente dal Consiglio di Amministrazione.

Oltre quanto sopra, in relazione all'entrata in vigore del D.Lgs. 10 marzo 2023 n. 24 ("**Decreto Whistleblowing**") di attuazione della "*Direttiva (UE) 2019/1937 che disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato*", l'Organismo di Vigilanza è chiamato a:

- vigilare sull'implementazione da parte della Società di un canale di segnalazione interna e sulla sua rispondenza (quanto a "disegno") al Decreto Whistleblowing, nonché sul conseguente aggiornamento del Modello in riferimento al canale stesso (sul punto vedasi il paragrafo 3.4);
- vigilare sull'avvenuta adozione da parte della Società di una procedura Whistleblowing ("Procedura Whistleblowing"), di cui all'Allegato n.4, per disciplinare il procedimento per la gestione delle segnalazioni interne effettuate dal Whistleblower, ovvero gli adempimenti e le modalità di raccolta,

gestione e archiviazione delle segnalazioni effettuate attraverso l'utilizzo del canale interno implementato dalla Società;

- vigilare sulla formazione, informazione e diffusione di quanto previsto in tal senso nel Modello e nella Procedura Whistleblowing;
- vigilare sull'effettività e sull'accessibilità del canale di segnalazione interna implementato dalla Società;
- vigilare sull'effettivo funzionamento e sull'osservanza di quanto previsto nel Modello e nella Procedura Whistleblowing.

3.3. REPORTING DELL'ORGANISMO DI VIGILANZA

Come sopra già anticipato, al fine di garantire la piena autonomia e indipendenza nello svolgimento delle relative funzioni, l'Organismo di Vigilanza comunica direttamente al Consiglio di Amministrazione della Società.

Segnatamente, l'Organismo di Vigilanza riferisce lo stato di attuazione del Modello e gli esiti dell'attività di vigilanza svolta nelle seguenti modalità:

- su necessità al Presidente del Consiglio di Amministrazione e all'Amministratore Delegato per garantire un costante allineamento con il vertice aziendale in merito alle attività svolte;
- con cadenza annuale nei confronti del Consiglio di Amministrazione, attraverso una relazione scritta, nella quale vengano illustrate le attività di monitoraggio svolte dall'Organismo stesso, le criticità emerse e gli eventuali interventi correttivi o migliorativi opportuni per l'implementazione del Modello;
- occasionalmente, qualora i due organi siano distinti, nei confronti del Collegio Sindacale, ove ne ravvisi la necessità, in relazione a presunte violazioni poste in essere dai vertici aziendali o dai componenti del Consiglio di Amministrazione, potendo ricevere dal Collegio Sindacale richieste di informazioni o di chiarimenti in merito alle suddette presunte violazioni.

L'Organismo di Vigilanza può essere convocato in qualsiasi momento dal Consiglio di Amministrazione e, a sua volta, può richiedere a tale organo di essere sentito qualora ravvisi l'opportunità di riferire su questioni inerenti al funzionamento e all'efficace attuazione del Modello o in relazione a situazioni specifiche.

A garanzia di un corretto ed efficace flusso informativo, nonché al fine di un completo e corretto esercizio dei propri compiti, l'Organismo ha inoltre facoltà di richiedere chiarimenti o informazioni direttamente ai soggetti con le principali responsabilità operative.

3.4. FLUSSI INFORMATIVI E SEGNALAZIONI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

Il D.Lgs. 231/2001 enuncia, tra le esigenze che il Modello deve soddisfare, l'istituzione di specifici obblighi informativi nei confronti dell'Organismo di Vigilanza da parte delle Direzioni/Funzioni della Società, diretti a consentire all'Organismo stesso lo svolgimento delle proprie attività di vigilanza e di verifica.

A tale proposito devono essere comunicate all'Organismo di Vigilanza le seguenti informazioni (c.d. "**Flussi informativi**"):

- su base periodica, una serie di informazioni, dati, notizie e documenti previamente identificati dall'Organismo di Vigilanza, secondo le modalità e le tempistiche definite dall'Organismo medesimo;

- nell'ambito delle attività di verifica dell'Organismo di Vigilanza, ogni informazione, dato, notizia e documento ritenuto utile e/o necessario per lo svolgimento di dette verifiche, previamente identificati dall'Organismo e formalmente richiesti alle singole Direzioni/Funzioni;
- occasionalmente, qualsiasi altra informazione di qualsivoglia natura riguardante l'attuazione del Modello in aree considerate a rischio di reato e l'osservanza delle disposizioni del Decreto, che possono essere di aiuto nello svolgimento delle attività dell'Organismo di Vigilanza.

Oltre a quanto sopra, deve essere presentata all'Organismo di Vigilanza qualsiasi comunicazione relativa anche alle seguenti questioni:

- misure e/o notifiche da parte della polizia o di qualsiasi altra autorità, comprese quelle amministrative, che coinvolgono la Società o persone di alto livello e che indicano che sono in corso indagini, anche contro ignoti, per i reati previsti dal Decreto, fatti salvi gli obblighi di riservatezza e segretezza imposti dalla legge;
- richieste di assistenza legale presentate da personale dirigente e/o da dipendenti quando un procedimento giudiziario è avviato dopo la presunta commissione di un reato previsto dal Decreto;
- modifiche nel sistema di deleghe e procure, modifiche statutarie o organigrammi;
- le sanzioni disciplinari applicate per una violazione del Modello o una decisione di non procedere insieme alle motivazioni di tale decisione;
- report relativi a gravi lesioni personali (omicidio colposo, lesioni personali gravi o gravissime, e in generale qualsiasi lesione personale che implica una prognosi superiore a 40 giorni) occorse a dipendenti o collaboratori della Società;

L'Organismo di Vigilanza, con l'assistenza della Società, identifica formalmente le modalità di trasmissione di tali informazioni, notificando le Direzioni rilevanti che hanno il dovere di effettuare le comunicazioni.

Per ricevere i Flussi informativi l'OdV ha attivato la seguente casella di posta elettronica odv231@computergross.it il cui accesso è riservato ai solo componenti dell'Organismo. L'omesso invio di informazioni all'Organismo di Vigilanza integra violazione del presente Modello.

LA GESTIONE DELLE SEGNALAZIONI WHISTEBLOWING

Il Decreto Whistleblowing ha modificato l'art. 6, comma 2-bis del D.Lgs. 231/2001, nonché abrogato i commi 2-ter e 2-quater del medesimo articolo, stabilendo che i Modelli devono prevedere:

- canali di segnalazione interna, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione;
- la tutela della riservatezza e il divieto di ritorsione in qualunque forma nei confronti del segnalante;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto, oltre che delle prescrizioni del Modello e del Codice Etico, anche di quanto previsto ai sensi del Decreto Whistleblowing.

In conformità a quanto previsto dal Decreto Whistleblowing, Computer Gross ha:

- adottato un proprio canale di segnalazione interna "Piattaforma" accessibile tramite il sito web della Società o il seguente link https:// whistleblowing.sesa.it

- nominato il responsabile della gestione della Piattaforma ("**Responsabile del Sistema**");
- implementato una specifica linea telefonica (055-9073602) dedicata alle segnalazioni (non anonime), disponibile 24 ore al giorno 365 giorni all'anno dotata di segreteria telefonica permanente che tiene traccia delle segnalazioni ricevute.
- reso possibile effettuare le segnalazioni anche tramite posta ordinaria (anche in forma anonima) tramite il sistema delle "tre buste" ovvero prevedendo che la segnalazione venga inserita in due buste chiuse, includendo, nella prima, i dati identificativi del segnalante, unitamente a un documento di identità (ove la segnalazione non sia anonima); nella seconda, l'oggetto della segnalazione e prevedendo che entrambe le buste vengano inserite in una terza busta riportando, all'esterno, la dicitura "riservata al gestore della segnalazione".

L'Organismo di Vigilanza di Computer Gross è stato nominato dal Consiglio di Amministrazione della Società Responsabile del Sistema Whistleblowing.

Il procedimento per la gestione delle segnalazioni interne, ovvero gli adempimenti e le modalità di raccolta, gestione e archiviazione delle stesse, i presupposti per effettuare segnalazioni esterne, nonché i flussi informativi tra il Responsabile Whistleblowing nominato dalla Società e gli altri organi/funzioni aziendali che, in relazione alla tipologia di segnalazione, possono essere coinvolti nella sua gestione, son disciplinati nella Procedura Whistleblowing allegata al presente Modello e il cui contenuto si intende qui integralmente richiamato.

In caso di segnalazioni che riguardino lo stesso Organismo di Vigilanza (ad oggi anche nominato Responsabile del Sistema) della Società, il ruolo di Responsabile del Sistema è assunto dall'Organo Amministrativo di Computer Gross.

Coordinamento delle attività di vigilanza nel Gruppo

Al fine di realizzare il collegamento funzionale tra gli OdV delle Società del Gruppo Sesa possono essere previste riunioni congiunte, anche per la formulazione di indirizzi comuni riguardo le attività di vigilanza, le eventuali modifiche e integrazioni da apportare ai modelli organizzativi e in occasione del verificarsi di eventi o circostanze di particolare rilevanza.

In ogni caso qualsiasi attività di coordinamento non dovrà mai determinare una limitazione di autonomia dell'OdV di Computer Gross.

L'OdV potrà avvalersi, nell'espletamento del compito di vigilare sul funzionamento e l'osservanza del Modello 231, anche delle funzioni di controllo allocate presso la Capogruppo, sulla base di un predefinito rapporto contrattuale sottoscritto dalla Società.

Raccolta e conservazione delle informazioni

Tutte le informazioni, la documentazione, le questioni condivise con l'Organismo di Vigilanza e le informazioni raccolte dallo stesso durante l'espletamento delle sue funzioni devono essere depositate dall'Organismo di Vigilanza in un apposito database informatico e/o cartaceo istituito presso la Società per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati, se non diversamente previsto dalla legge.

I dati e le informazioni conservate nel data base sono posti a disposizione di soggetti esterni all'OdV previa autorizzazione dell'OdV. Questo ultimo definisce con apposita disposizione interna criteri e condizioni di accesso al database nel rispetto della normativa vigente.

4 IL SISTEMA SANZIONATORIO

La definizione di un sistema sanzionatorio, applicabile in caso di violazione delle disposizioni del presente Modello – e di tutta la documentazione che di esso fa parte -, costituisce condizione necessaria per garantire l'efficace attuazione del Modello stesso, nonché presupposto imprescindibile per consentire alla Società di beneficiare dell'esimente dalla responsabilità amministrativa.

Il sistema disciplinare si rivolge ai dirigenti, ai dipendenti, agli Amministratori, ai membri degli organi di controllo e ai terzi (consulenti, collaboratori, agenti, procuratori, clienti e partner commerciali etc.) con cui la Società entra in contatto nello svolgimento di relazioni d'affari, prevedendo corrispondenti provvedimenti di sanzione.

Il sistema sanzionatorio adottato dalla società è riportato nel documento "Sistema Disciplinare" allegato al presente Modello e il cui contenuto si considera interamente richiamato (Allegato 6).

In particolare, per quanto riguarda le sanzioni nei confronti dei terzi destinatari, si specifica che la Società inserisce, nelle lettere di incarico e/o negli accordi negoziali, apposite clausole volte a prevedere, in caso di violazione delle prescrizioni relative al Modello, l'applicazione delle misure sanzionatorie.

5 DIFFUSIONE DEL MODELLO E FORMAZIONE

Computer Gross, consapevole dell'importanza che gli aspetti informativi e formativi assumono in una prospettiva di prevenzione, ha definito programmi di comunicazione e di formazione volti a garantire la divulgazione ai Destinatari dei principali contenuti del Decreto, del Decreto Whistleblowing e degli obblighi dagli stessi derivanti, nonché delle prescrizioni del Modello e della Procedura Whistleblowing.

La diffusione del Modello

Con riguardo alla diffusione al personale aziendale del Modello, del Codice Etico e della Procedura whistleblowing nel contesto aziendale, la documentazione sarà pubblicata sul portale aziendale il cui accesso è garantito a tutto il personale della Società.:

La Società:

- si assicura che il Modello, il Codice Etico e la Procedura Whistleblowing siano pubblicati sulla intranet aziendale e/o su qualsiasi altro strumento di comunicazione interna ritenuto idoneo;
- organizza attività formative dirette a diffondere la conoscenza del D.Lgs. 231/2001, del Decreto Whistleblowing e delle prescrizioni del Modello, del Codice Etico e della Procedura Whistleblowing, nonché pianifica sessioni di formazione per il personale, anche in occasione di aggiornamenti e/o modifiche del Modello, nelle modalità ritenute più idonee.

Per quanto riguarda la diffusione del Modello verso l'esterno, i contenuti del Modello 231 adottato dalla Società sono portati a conoscenza di tutti coloro con i quali Computer Gross intrattiene relazioni contrattuali, tramite la pubblicazione della presente Parte Generale del Modello nel sito internet della Società.

Computer Gross provvede, ove possibile, altresì, ad inserire nei contratti con le controparti commerciali, finanziarie e consulenti apposite clausole contrattuali che prevedono, in caso di inosservanza del Modello o del Codice Etico, la possibile risoluzione degli obblighi negoziali e la richiesta di risarcimento per eventuali danni.

La formazione sul Modello

L'attività di formazione sul Modello e sul Decreto è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, del grado di coinvolgimento degli stessi nelle attività sensibili indicate nel Modello, dell'esercizio di eventuali funzioni di rappresentanza della Società.

Per tutti i destinatari del Modello, in ogni caso, potranno essere organizzati corsi di formazione, meeting, anche mediante l'utilizzo di strumenti di e-learning

La Società si impegna a garantire il costante aggiornamento della formazione dei Destinatari del Modello in relazione a modifiche significative dello stesso o del quadro normativo di riferimento.

La formazione del personale ai fini dell'attuazione del Modello è gestita dalla Società, in stretta cooperazione con l'Organismo di Vigilanza. I contenuti dei programmi di formazione sono condivisi infatti con l'Organismo di Vigilanza che vigila affinché gli stessi siano erogati tempestivamente.

La documentazione relativa alle attività di informazione e formazione è conservata a cura della funzione della Società, disponibile per la relativa consultazione da parte dell'Organismo di Vigilanza e di chiunque sia autorizzato a prenderne visione.

6 ADOZIONE E AGGIORNAMENTO DEL MODELLO

L'adozione del Modello costituisce responsabilità del Consiglio di Amministrazione di Computer Gross.

Le modifiche e\o le integrazioni della parte generale del Modello 231 sono deliberate dal CdA. L'aggiornamento della Parte Speciale è curato sistematicamente su iniziativa dell'Amministratore Delegato. Ogni iniziativa di modifica o aggiornamento deve essere comunicata all'OdV.

Le modifiche possono avvenire anche su proposta dell'OdV, che, in ogni caso, deve segnalare al CdA, anche nel corso delle informative periodiche, eventuali fatti che evidenzino la necessità di aggiornare il Modello.

In generale, Il Modello deve sempre essere tempestivamente aggiornato quando:

- siano intervenute violazioni o elusioni delle prescrizioni in esso contenute, che ne abbiano dimostrato l'inefficacia o l'incoerenza ai fini della prevenzione dei reati;
- si siano verificati eventi che abbiano evidenziato la presenza di rischi precedentemente non previsti o l'inadeguatezza delle misure di prevenzione adottate;
- identificazione di nuove aree a rischio/ attività sensibili e processi strumentali/funzionali alla commissione del reato, connessi allo svolgimento di nuove attività da parte della Società o a variazioni di quelle precedentemente individuate;
- mutamenti dell'assetto organizzativo o al quadro normativo da cui derivino conseguenze sul Modello;
- mutamenti del sistema di segnalazione interna e delle disposizioni di legge emanate in tal senso;
- identificazione di possibili aree di miglioramento del Modello riscontrate dall'Organismo di Vigilanza a seguito delle periodiche attività di verifica.

Costituiscono in ogni caso modifiche sostanziali quelle che incidono sulla composizione, durata in carica e operatività dell'Organismo di Vigilanza, nonché sulle regole del sistema sanzionatorio.

L'Organismo di Vigilanza, nell'ambito dei poteri conferiti ai sensi dell'art. 6, comma 1, lettera b) e art. 7, comma 4 lettera a) del Decreto, è responsabile di sottoporre al Consiglio di Amministrazione proposte di aggiornamento e adeguamento del presente Modello.

Le modifiche, gli aggiornamenti e le integrazioni del Modello devono sempre essere segnalate all'Organismo di Vigilanza.

Le procedure operative adottate in attuazione del presente Modello sono modificate dalle competenti funzioni aziendali, qualora risultino inefficaci ai fini della corretta attuazione delle disposizioni del Modello. Le funzioni aziendali competenti dovranno modificare o integrare le procedure al fine di rendere effettiva qualsiasi revisione del presente Modello.

L'Organismo di Vigilanza è tenuto informato dell'aggiornamento delle procedure esistenti e dell'attuazione di quelle nuove.

Qualora si rendano necessarie modifiche al Modello di natura esclusivamente formale, quali chiarimenti o precisazioni del testo, il Presidente del Consiglio di Amministrazione, su proposta, o comunque sentito l'Organismo di Vigilanza, può provvedervi autonomamente. Di tali modifiche è data successiva comunicazione, nella prima seduta utile, all'intero Consiglio di Amministrazione.