MOGC-01-05

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ADOTTATO AI SENSI DEL DECRETO LEGISLATIVO
8 GIUGNO 2001, N. 231

Emissione del documento	
Redazione	Compliance
Verifica	Paolo Arletti - Matteo Neri (*Amministratori Delegati*)
Approvazione	Consiglio di Amministrazione VISTA TECHNOLOGY S.r.l.

Revisione *01* Approvata dal CDA il *09 giugno 2025*

Questo documento è formato da 38 pagine, inclusi copertina ed indice

Storia del documento			
Rev.	**Data**	**Motivo**	**Pagina**
01	09.06.2025	Nessuna (prima emissione)	Tutte

Sommario

1 Premessa 4
1.1 Principi Generali 4
1.2 Finalità del Modello 4
1.3 Struttura del Modello 4
1.4 Destinatari del Modello 5
2 Riferimenti 5
2.1 Documenti collegati 5
2.2 Acronimi 6
2.3 Indirizzi utili di gruppo 6
2.4 Normativa di riferimento 6
2.5 Definizioni 7
3 Parte Generale 8
3.1 Sezione Prima – Il Decreto Legislativo 8 giugno 2001, n. 231 8
3.1.1 La Responsabilità Amministrativa degli Enti 8
3.1.2 Fonti per la costruzione del Modello: Linee Guida di Confindustria 13
3.2 Sezione Seconda – Il Contenuto del Modello di VISTA TECHNOLOGY S.r.l. 14
3.2.1 Adozione del Modello 14
3.2.2 I Principi ispiratori del Modello 14
3.2.3 Organismo di Vigilanza 22
3.2.4 Sistema disciplinare 30
3.2.5 Diffusione del Modello 35
3.2.6 Aggiornamento del Modello 36
3.2.7 Modalità di nomina del difensore di fiducia dell'Ente 36
4 Parte Speciale 37
4.1 Introduzione 37

1 Premessa

1.1 Principi Generali

VISTA TECHNOLOGY S.r.l. (di seguito anche “VISTA TECHNOLOGY” o la “Società”) nell’ambito della più ampia politica aziendale e cultura etica e di responsabilità sociale comune a tutto il gruppo DGS cui appartiene, sensibile all’esigenza di assicurare condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della Società stessa, ha ritenuto opportuno analizzare e rafforzare tutti gli strumenti di controllo e di governance societaria già adottati, procedendo con l’adozione del Modello di organizzazione, gestione e controllo, previsto dal D.lgs. 231/2001 (di seguito anche “Modello”, “Modello 231” o “MOGC”).

Il presente documento, corredato di tutti i suoi Allegati, illustra quindi il Modello adottato dal Consiglio di amministrazione di VISTA TECHNOLOGY S.r.l. con delibera del 09 giugno 2025, ai sensi del D.lgs. 231/2001 e successive modifiche (di seguito anche solo “Decreto” o “Decreto 231”).

Il Modello di VISTA TECHNOLOGY, così come riportato nel presente documento, è da intendersi a integrazione e completamento del sistema dei controlli interni della Società ed ha l’obiettivo di rappresentare il sistema di regole e principi comportamentali che disciplinano l’attività della Società, nonché gli ulteriori elementi di controllo di cui quest'ultima si è dotata al fine di prevenire i reati e gli illeciti amministrativi per i quali trova applicazione il Decreto, nel rispetto della governance aziendale e del sistema di attribuzione di funzioni e di deleghe di poteri.

1.2 Finalità del Modello

Con l’adozione del presente Modello, VISTA TECHNOLOGY si propone di perseguire le seguenti principali finalità:

- ribadire che ogni condotta illecita è assolutamente condannata dalla Società, anche se ispirata ad un malinteso interesse sociale ed anche se VISTA TECHNOLOGY non fosse apparentemente in condizione di trarne vantaggio, in quanto contrarie, oltre che a disposizioni normative, anche alle norme e regole di condotta cui VISTA TECHNOLOGY si ispira e a cui si attiene nella conduzione della propria attività aziendale;
- sensibilizzare tutti coloro che operano per conto di VISTA TECHNOLOGY, affinché tengano comportamenti corretti e lineari nell’espletamento delle proprie attività;
- determinare in tutti coloro che operano in nome e per conto e comunque nell’interesse o a vantaggio di VISTA TECHNOLOGY e, in particolare, nelle “aree a rischio 231” ovvero nelle aree di attività in cui potenzialmente potrebbero essere realizzate le fattispecie di reato rilevanti ai sensi del Decreto, la consapevolezza del dovere di conformarsi alle disposizioni ivi contenute e più in generale alla regolamentazione aziendale;
- informare i Destinatari che la commissione anche tentata di un reato - anche se effettuata a vantaggio o nell’interesse di VISTA TECHNOLOGY - rappresenta una violazione del Modello organizzativo e del Codice di Etico di gruppo e costituisce un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei confronti dell’autore del reato, ma anche nei confronti della Società, con la conseguente applicazione alla medesima delle relative sanzioni;
- consentire alla Società, grazie ad un sistema di protocolli di controllo ed a una costante azione sulla corretta attuazione di tale sistema di intervenire tempestivamente per prevenire o contrastare la commissione dei reati rilevanti ai sensi del Decreto.

1.3 Struttura del Modello

Il Modello di VISTA TECHNOLOGY si compone dei seguenti documenti:

- Il **Codice Etico** del gruppo DGS definisce i principi etici e i valori fondamentali ai quali il gruppo si ispira nello svolgimento delle proprie attività, stabilendo le regole di condotta che tutti i destinatari del Modello sono tenuti a rispettare. Esso rappresenta un riferimento essenziale per promuovere una cultura aziendale fondata sull’integrità, la trasparenza e la

responsabilità, rafforzando il sistema di prevenzione dei reati e degli illeciti previsti dal Decreto.

- La **Parte Generale** (questo documento) descrive i contenuti del Decreto, richiamando le fattispecie di reato che determinano la responsabilità amministrativa da reato in capo all'ente, le possibili sanzioni e le condizioni per l'esenzione della responsabilità (Sezione prima), nonché la struttura organizzativa e di governance della Società e le attività svolte per la costruzione, diffusione e aggiornamento del Modello (Sezione seconda).
- L'allegato alla Parte Generale sui **Reati e gli illeciti amministrativi rilevanti ai sensi del D. Lgs. 231/01** fornisce un'analisi dettagliata delle fattispecie di reato che possono determinare la responsabilità amministrativa dell'ente, illustrando i presupposti normativi, le possibili sanzioni e i criteri di attribuzione della responsabilità. Tale documento costituisce un supporto tecnico-giuridico per una completa comprensione dei rischi e per l'implementazione di adeguati strumenti di prevenzione e controllo.
- La **Parte Speciale** contiene i 17 **Protocolli di Decisione** ovvero un insieme di regole e di principi di controllo e di comportamento ritenuti idonei a governare le aree per le quali è stato rilevato un rischio di potenziale commissione dei reati presupposto della responsabilità amministrativa ex D.lgs. 231/2001.

1.4 Destinatari del Modello

Le regole contenute nel Modello si applicano ai seguenti Destinatari:

- tutti gli amministratori, i procuratori e coloro che rivestono funzioni di rappresentanza, di amministrazione o di direzione in VISTA TECHNOLOGY nonché coloro che esercitano anche di fatto la gestione e il controllo della Società;
- tutti coloro che intrattengono con VISTA TECHNOLOGY un rapporto di lavoro subordinato (dipendenti), ivi compresi i dipendenti di altre società del gruppo distaccati presso la Società;
- tutti coloro che collaborano con VISTA TECHNOLOGY in forza di un rapporto di lavoro parasubordinato (collaboratori a progetto, prestatori di lavoro temporaneo, interinali, stagisti, ecc.).

Dai Destinatari del Modello devono tenersi distinti coloro i quali – pur non formalmente inseriti nell'organizzazione societaria - operano su mandato o per conto di VISTA TECHNOLOGY nell'ambito dei processi e delle attività "sensibili", quali ad esempio, i consulenti, i fornitori, i partners, i collaboratori in genere, che per l'attività svolta possono contribuire a far sorgere una responsabilità in capo alla Società.

Relativamente alla attività svolta da tali soggetti (di seguito anche "Soggetti Terzi"), i contratti che ne regolano i rapporti prevedono specifiche clausole che prescrivono l'impegno a rispettare le previsioni del D.Lgs. 231/2001, del Modello e del Codice Etico di gruppo. I contratti con tali soggetti contengono anche una specifica clausola di recesso e/o di risoluzione connesse all'inadempimento di tali obbligazioni, fermo restando il diritto della Società di rivalersi per gli eventuali danni verificatisi in conseguenza di dette condotte, ivi inclusi i danni causati dall'applicazione da parte del giudice delle misure previste dal Decreto.

2 Riferimenti

2.1 Documenti collegati

Codice Etico del gruppo DGS

MOGC-01-02 - Allegato - Elenco dei reati ex D.Lgs. 231/2001

PL-10-03 - Segnalazioni, suggerimenti, reclami (Whistleblowing)

Protocolli di decisione:

MOGC-02-01 - Selezione, assunzione e gestione del personale
MOGC-02-02 - Approvvigionamento di beni e servizi

MOGC-02-03 - Acquisizione di consulenze e servizi professionali
MOGC-02-04 - Flussi monetari e finanziari
MOGC-02-05 - Amministrazione, contabilità, Bilancio e operazioni sul capitale
MOGC-02-06 - Operazioni straordinarie
MOGC-02-07 - Rapporti infragruppo
MOGC-02-08 - Gestione dei contenziosi e degli accordi transattivi
MOGC-02-09 - Acquisizione e gestione commessa
MOGC-02-10 - Adempimenti con la Pubblica Amministrazione e le Autorità di Vigilanza
MOGC-02-11 - Rapporti con i soci e gli organi sociali
MOGC-02-12 - Gestione della fiscalità
MOGC-02-13 - Gestione omaggi, liberalità, sponsorizzazioni ed eventi di co-marketing
MOGC-02-14 - Rimborso Spese e Spese di rappresentanza
MOGC-02-15 - Marketing e Comunicazione
MOGC-02-16 - Adempimenti in materia di salute e sicurezza sul lavoro e ambiente
MOGC-02-17 - Sicurezza informatica

2.2 Acronimi

ANAC	Autorità Nazionale Anticorruzione
CCNL	Contratto Collettivo Nazionale di Lavoro
CdA	Consiglio di Amministrazione
CdS	Comitato di Sicurezza
CISO	Chief Information Security Officer
Comp	Funzione Compliance
D.lgs.	Decreto legislativo
D.lgs. 231/2001	Decreto Legislativo 8 giugno 2001, n. 231
DPO	Data Protection Officer
INAU	Internal Audit
IO	Istruzione Operativa (es. IO-07-05)
MOGC	Modello di Organizzazione, Gestione e Controllo
OdV	Organismo di Vigilanza
PL	Politica (es. PL-10-03)
PO	Procedura Operativa (es. PO-08-01)
RAC	Responsabile per la prevenzione della corruzione
Resp. WB	Gestore delle segnalazioni whistleblowing ai sensi del D.lgs. 24/2023
TUF	Testo Unico della Finanza

2.3 Indirizzi utili di gruppo

CISO	CISO@dgsspa.com
Comitato di Sicurezza	comitatodisicurezza@dgsspa.com
Compliance	compliance@dgsspa.com
DPO	DPO@dgsspa.com
OdV	odv@vistatech.it
Privacy	privacy@dgsspa.com
Risorse Umane	hrcomunicazioni@dgsspa.com

2.4 Normativa di riferimento

Contratto collettivo nazionale di lavoro (CCNL) 5 febbraio 2021 per i lavoratori addetti all'industria metalmeccanica privata e alla installazione di impianti

Decreto Legislativo 1° settembre 1993, n. 385 - Testo unico delle leggi in materia bancaria e creditizia

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'articolo 11 della legge 29 settembre 2000, n. 300

Decreto Legislativo 9 aprile 2008, n. 81 - Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro

Legge 16 marzo 2006, n. 146 - Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001

Decreto Legislativo 10 marzo 2024, n. 23 - 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 e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

2.5 Definizioni

Autorità Nazionale Anticorruzione (ANAC): ente preposto alla vigilanza in materia di prevenzione della corruzione e trasparenza nella Pubblica Amministrazione e negli enti privati che operano con fondi pubblici.

CISO (Chief Information Security Officer): figura responsabile della gestione della sicurezza delle informazioni e della protezione dei sistemi informatici aziendali da minacce esterne ed interne.

Comitato di Sicurezza (CdS): il comitato (composto da Compliance Officer, CISO, QHSE Officer, DPO e Privacy Officer) è un organismo di governance trasversale, incaricato di definire gli indirizzi strategici, supervisionare e coordinare le attività connesse alla sicurezza delle informazioni, alla conformità normativa in materia di privacy e alla gestione integrata degli standard certificati per tutto il gruppo DGS.

Compliance: funzione aziendale incaricata di garantire il rispetto delle normative vigenti, delle policy interne e delle best practice in materia di governance, gestione del rischio e responsabilità amministrativa degli enti.

Consiglio di Amministrazione (CdA): organo amministrativo della Società responsabile della gestione strategica e operativa, composto da amministratori con poteri di ordinaria e straordinaria amministrazione.

DPO (Data Protection Officer): responsabile della protezione dei dati personali all'interno della Società, con il compito di monitorare la conformità al Regolamento UE 2016/679 (GDPR) e alle normative in materia di privacy.

Gestore delle segnalazioni whistleblowing (Resp. WB): soggetto nominato ai sensi dell'art.4, comma 2 del D.lgs. 24/2023 e incaricato della gestione delle segnalazioni c.d. "whistleblowing", ai sensi del suindicato decreto.

Internal Audit (INAU): la Funzione Internal Audit è incaricata di procedere ad una valutazione indipendente e obiettiva dell'adeguatezza, dell'efficacia e della resilienza del sistema di controllo interno, della gestione dei rischi e dei processi di governance del gruppo. Tale attività viene svolta in piena indipendenza dalle aree operative e di business, collocandosi in una posizione di terzietà che ne garantisce l'obiettività. L'attività di controllo si estende sia ai processi core (ad esempio, gestione dei progetti, sicurezza delle informazioni, risorse umane, ciclo attivo e passivo, gestione finanziaria, sistemi IT) sia a quelli trasversali (come compliance normativa, ESG, sicurezza fisica e business continuity).

Modello di organizzazione, gestione e controllo (Modello, Modello 231 o MOGC): insieme di protocolli, procedure e regole aziendali adottati dalla Società ai sensi del D.lgs. 231/2001 per gestire il rischio di commissione di reati e garantire una governance trasparente ed efficace.

Organismo di Vigilanza (OdV): organismo interno con autonomi poteri di iniziativa e di controllo, istituito ai sensi del D.lgs. 231/2001, incaricato di vigilare sul funzionamento e sull'efficace attuazione del Modello, nonché di curare il relativo aggiornamento.

Protocolli di Decisione: insieme di regole e controlli stabiliti dal Modello per regolamentare le attività aziendali considerate a rischio 231, al fine di ridurre la possibilità di commissione di reati presupposto.

Responsabile per la prevenzione della corruzione (RAC): responsabile del Sistema di Gestione del rischio ai sensi della ISO 37001:2016 (Sistemi di Gestione per la prevenzione della corruzione), incaricato di redigere, aggiornare e vigilare sul rispetto delle "Misure di prevenzione della corruzione integrative", in posizione di indipendenza e autonomia, anche di spesa.

Risk assessment: processo di identificazione, analisi e valutazione dei rischi aziendali, volto a individuare le aree sensibili in cui potrebbero verificarsi violazioni delle normative applicabili, compreso il D.lgs. 231/2001.

Whistleblowing: sistema di segnalazione che consente ai dipendenti e ai soggetti terzi di segnalare violazioni delle normative interne (compreso il Modello) o esterne, garantendo la tutela della riservatezza dell'identità del segnalante, della persona coinvolta e della persona segnalata, nonché del contenuto della segnalazione e della relativa documentazione, ai sensi del D.lgs. 24/2023.

3 Parte Generale

3.1 Sezione Prima – Il Decreto Legislativo 8 giugno 2001, n. 231

3.1.1 La Responsabilità Amministrativa degli Enti

3.1.1.1 Il regime giuridico della responsabilità amministrativa degli Enti

Il Decreto Legislativo 8 giugno 2001, n. 231 in parziale attuazione della legge delega 29 settembre 2000, n. 300, disciplina – introducendola per la prima volta nell'ordinamento giuridico nazionale – la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica per alcuni reati commessi nell'interesse o a vantaggio di queste: a) dai cd. soggetti in posizione apicale, vale a dire 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; b) dai cd. soggetti sottoposti, ovvero persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a). In altre parole, è necessario che il reato presupposto sia commesso da una persona fisica che abbia con l'ente rapporti di tipo organizzativo-funzionale; insomma, è necessario che l'agente vesta una posizione qualificata all'interno dell'ente.

In relazione ai reati presupposto previsti dagli artt. 24 e ss. del Decreto, la responsabilità è stata ampliata includendo non solo la persona fisica che ha materialmente commesso il fatto di reato, ma anche gli enti che hanno tratto vantaggio dalla relativa commissione o nel cui interesse il reato è stato commesso. Il "vantaggio" o "interesse" rappresentano due distinti criteri di imputazione della responsabilità, potendo l'ente essere responsabile per il sol fatto che l'illecito viene commesso nel suo interesse, a prescindere dal conseguimento o meno di un concreto vantaggio.

La responsabilità amministrativa da reato degli enti si applica alle categorie di reati espressamente contemplate nel Decreto 231 e può configurarsi anche in relazione a reati commessi all'estero, a condizione che: a) sussistano le condizioni di cui agli artt. da 7 a 10 del Codice Penale; b) per tali reati non proceda lo Stato del luogo in cui è stato commesso il fatto; c) sussistano le particolari condizioni di imputazione del reato all'ente previste dal Decreto 231.

È previsto un articolato sistema sanzionatorio che muove dalle sanzioni pecuniarie fino ad arrivare alle più pesanti sanzioni interdittive, ivi inclusa l'interdizione dall'esercizio dell'attività. È, altresì, sanzionata la commissione del delitto tentato che non è giunto alla sua consumazione perché non si è verificato l'evento voluto dal reo o perché, per ragioni indipendenti dalla sua volontà, l'azione non è comunque giunta a compimento. Diversamente, l'ente non risponde quando ha volontariamente impedito il compimento dell'azione o la realizzazione dell'evento.

Le sanzioni amministrative previste dal Decreto possono infatti essere applicate esclusivamente dal giudice penale, nel contesto garantistico del processo penale, solo se sussistono tutti i requisiti oggettivi e soggettivi fissati dal legislatore: la commissione di un reato nell'interesse o a vantaggio dell'Ente, da parte di soggetti qualificati (apicali o ad essi sottoposti).

La responsabilità amministrativa in capo all'Ente sussiste se chi ha commesso il reato presupposto ha agito nell'interesse o a vantaggio dell'Ente rappresentato. I concetti di interesse e vantaggio afferiscono a sfere diverse: il primo alla tensione soggettiva della condotta verso un risultato favorevole per l'Ente; il secondo al risultato effettivamente conseguito.

Al contrario, l'interesse esclusivo dell'agente (proprio o di un terzo) esclude la responsabilità dell'Ente, versandosi in una situazione di assoluta e manifesta estraneità del medesimo alla commissione del reato.

Ai fini dell'affermazione della responsabilità dell'Ente, oltre all'esistenza dei richiamati requisiti che consentono di collegare oggettivamente il reato all'ente, il legislatore impone inoltre l'accertamento della colpevolezza dell'ente. Siffatto requisito soggettivo si identifica con una colpa da organizzazione, intesa come mancata adozione, da parte dell'ente, di misure preventive adeguate a prevenire la commissione del reato presupposto in concreto verificatosi.

3.1.1.2 I reati che determinano la responsabilità amministrativa dell'ente

Le **fattispecie di reato** suscettibili di configurare la responsabilità amministrativa della Società sono soltanto quelle espressamente indicate dal legislatore negli artt. 24 e ss. del Decreto che, al momento dell'emanazione, contemplava solo alcuni reati nei confronti della Pubblica Amministrazione.

Il legislatore, anche in applicazione di successive direttive comunitarie, ha nel corso degli anni notevolmente ampliato il **catalogo dei Reati** sottoposti all'applicazione del D.lgs. 231/2001, che oggi comprende, in particolare:

- reati contro la Pubblica Amministrazione e contro il patrimonio della Pubblica Amministrazione (artt. 24 e 25 D.lgs. 231/2001);
- reati informatici e trattamento illecito di dati (art. 24-*bis* D.lgs. 231/2001);
- delitti di criminalità organizzata (art. 24-*ter* D.lgs. 231/2001);
- reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis* D.lgs. 231/2001);
- delitti contro l'industria e il commercio (art. 25-*bis*.1 D.lgs. 231/2001);
- reati societari, compresi i reati di corruzione tra privati ed istigazione alla corruzione tra privati (art. 25-*ter* D.lgs. 231/2001);
- reati commessi con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-*quater* D.lgs. 231/2001);
- pratiche di mutilazione degli organi genitali femminili (art. 25-*quater.*1 D.lgs. 231/2001);
- reati contro la personalità individuale (art. 25-*quinquies* D.lgs. 231/2001);
- reati ed illeciti amministrativi di abuso e manipolazione del mercato (art. 25-*sexies* D.lgs. 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 (art. 25-*septies* D.lgs. 231/2001);
- reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio (art. 25-*octies* D.lgs. 231/2001);
- delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-*octies*.1 D.lgs. 231/2001);
- delitti in materia di violazione del diritto d'autore (art. 25-*novies* D.lgs. 231/2001);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 25-*decies* D.lgs. 231/2001);

- reati ambientali (art. 25-*undecies* D.lgs. 231/2001);
- reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, compresi i reati in materia di violazione delle disposizioni contro le immigrazioni clandestine (art. 25-*duodecies* D.lgs. 231/2001);
- reati di razzismo e xenofobia (art. 25-*terdecies* D.lgs. 231/2001);
- frode in competizioni sportive, esercizio abusivo di gioco o di scommesse e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-*quaterdecies* D.lgs. 231/2001)
- reati tributari (art. 25-*quinquiesdecies* D.lgs. 231/2001);
- reati di contrabbando (art. 25-*sexiesdecies* del D.lgs. 231/2001);
- delitti contro il patrimonio culturale (art. 25-*septiesdecies* D.lgs. 231/2001);
- riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-*duodevicies* D.lgs. 231/2001);
- reati transnazionali (art. 10 L. 146/2006).

Per un dettaglio delle singole fattispecie di reato per le quali è prevista la responsabilità amministrativa ex D.lgs. 231/2001 si rimanda al catalogo allegato presente Modello (Allegato I).

3.1.1.3 Le sanzioni applicabili all'Ente

Il Decreto stabilisce un articolato sistema di sanzioni amministrative nel caso in cui l'Ente sia responsabile per un reato presupposto commesso da un apicale o sottoposto.

Tale sistema prevede quattro specie di sanzioni:

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

Le **sanzioni pecuniarie** vengono comminate in ogni caso di condanna definitiva. La determinazione della misura della sanzione, a norma dell'art. 10 del Decreto, si basa su un complesso sistema di quote. L'importo di una quota va da un minimo di €258,00 (euro duecentocinquantotto/00) ad un massimo di € 1.549,00 (millecinquecentoquarantanove/00). Per ogni fattispecie di reato presupposto il Decreto prevede l'applicazione della sanzione pecuniaria fino a un determinato numero di quote.

La sanzione da irrogarsi in concreto viene stabilita dal giudice, sulla base dei criteri stabiliti dall'art. 11 del Decreto ovvero: gravità del fatto, grado della responsabilità dell'ente, attività svolta dall'ente per delimitare o attenuare le conseguenze del fatto e prevenire la commissione di ulteriori reati. L'importo della singola quota è stabilito tenendo conto delle condizioni economiche e patrimoniali dell'ente.

Le **sanzioni interdittive** consistono nelle seguenti misure:

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

La durata delle sanzioni interdittive non può essere inferiore ai tre mesi, né eccedere i due anni.

La loro applicazione è prevista solo per alcuni dei Reati specificamente indicati nel Decreto 231.

Condizione per la comminazione delle sanzioni interdittive è il ricorrere di almeno uno dei seguenti presupposti: (a) che l'ente abbia tratto dal reato un profitto di rilevante entità e, al contempo, che il

reato sia stato commesso da un soggetto in posizione apicale o, se commesso da soggetti sottoposti, che la commissione del reato sia stata agevolata da gravi carenze del Modello organizzativo; (b) che vi sia stata reiterazione dell'illecito.

Nella scelta della sanzione interdittiva applicabile il giudice deve attenersi agli stessi criteri già visti sopra per le misure pecuniarie. In particolare, è richiesto che la sanzione interdittiva abbia il carattere della specificità, ossia abbia ad oggetto la specifica attività alla quale si riferisce l'illecito dell'ente. Fra le varie misure interdittive, quella della sospensione dall'esercizio dell'attività non può esser comminata se non quando l'irrogazione di ogni altra sanzione risulti inadeguata. È anche possibile che più sanzioni interdittive vengano applicate congiuntamente.

Nei casi in cui sussistono i presupposti per comminare una sanzione interdittiva che comporta l'interruzione dell'attività dell'ente, se l'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può comportare un grave pregiudizio per la collettività, ovvero se l'interruzione dell'attività, date le dimensioni dell'ente e le condizioni economiche del territorio sul quale si trova, può avere rilevanti ripercussioni sull'occupazione, è previsto che il giudice possa, in luogo della sanzione interdittiva, disporre che l'attività dell'ente continui sotto la guida di un commissario per un periodo pari alla durata della sanzione che sarebbe stata inflitta.

Le misure interdittive sono, in linea di principio, temporanee. Tuttavia, nel caso in cui una stessa persona giuridica venga condannata per almeno tre volte nei sette anni successivi all'interdizione temporanea dall'attività e abbia tratto dal reato un profitto di rilevante entità, il Decreto prevede la sanzione dell'interdizione definitiva dall'esercizio dell'attività. Inoltre, la sanzione dell'interdizione definitiva dall'esercizio dell'attività è disposta anche quando l'Ente o una sua unità organizzativa è utilizzato allo scopo unico o prevalente di commettere o agevolare la commissione di un reato presupposto ai sensi del Decreto. Possono essere applicate, sempre in via definitiva, anche le sanzioni del divieto di contrattare con la Pubblica Amministrazione e di pubblicizzare beni e servizi quando l'Ente è stato condannato, alla medesima sanzione interdittiva, per almeno tre volte in sette anni.

La **confisca del prezzo o del profitto del reato** è sempre disposta in caso di condanna. Quando non è possibile eseguire la confisca dei beni che hanno costituito il prezzo o il profitto del reato, la stessa può avere ad oggetto somme di danaro, beni o altre utilità di valore equivalente.

La **pubblicazione della sentenza di condanna** in uno o più giornali indicati dal giudice a spese dell'ente condannato può esser disposta dal giudice nei casi in cui viene irrogata una sanzione interdittiva.

Durante le more del procedimento penale, su richiesta del pubblico ministero, il giudice può disporre alcune delle misure interdittive descritte sopra in via cautelare. Ciò è possibile in presenza di gravi indizi circa la sussistenza della responsabilità dell'ente e di fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede. Le misure cautelari non possono avere durata superiore a un anno. Anche in sede cautelare è possibile che in luogo delle sanzioni interdittive si disponga il commissariamento dell'ente per tutto il tempo della durata della sanzione che sarebbe stata applicata.

3.1.1.4 L'esenzione dalla responsabilità: il Modello di organizzazione, gestione e controllo

Il D.lgs. 231/2001 espressamente prevede, agli artt. 6 e 7, l'esenzione dalla responsabilità amministrativa qualora l'Ente si sia dotato di effettivi ed efficaci modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi. L'adeguata organizzazione rappresenta pertanto il solo strumento in grado di escludere profili di "colpa" dell'Ente e, conseguentemente, di escludere l'applicazione delle sanzioni a carico dello stesso.

Precisamente, una volta accertato che un soggetto in posizione apicale ha commesso un reato nell'interesse o a vantaggio dell'ente, l'ente non risponderà per l'operato del soggetto in posizione apicale se viene dimostrato che:

a) prima della commissione del reato, aveva adottato ed efficacemente attuato un Modello Organizzativo idoneo a prevenire la commissione di reati della specie di quello commesso;

b) era stato istituito all'interno dell'ente un organismo dotato di poteri di iniziativa e controllo (il cd. Organismo di Vigilanza) incaricato di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento;
c) le persone che hanno commesso il reato hanno eluso fraudolentemente il Modello di organizzazione e gestione;
d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

Nel caso di commissione del reato ad opera di un soggetto sottoposto, la responsabilità dell'Ente sussiste se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Secondo l'art. 7 del Decreto 231, non vi è inosservanza degli obblighi di direzione e vigilanza se l'Ente, prima della commissione del fatto, ha adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

L'onere probatorio sull'adozione e attuazione di un Modello idoneo a prevenire reati della specie di quello verificatosi ricade sulla difesa dell'ente; mentre l'accusa ha l'onere di provare l'omessa direzione o vigilanza e il collegamento fra questa e il reato commesso.

Fulcro della disciplina della responsabilità amministrativa degli enti è costituito dalle previsioni relative ai Modelli, che, tuttavia, non costituiscono un obbligo per gli Enti, bensì una mera facoltà.

L'adozione ed effettiva attuazione di un Modello organizzativo il cui contenuto corrisponda a quello richiesto dal Decreto costituisce, infatti, la circostanza oggettiva che permette di escludere la sussistenza della colpa organizzativa dell'ente, e, di conseguenza, la responsabilità di questo in caso di reati commessi da soggetti apicali o sottoposti.

Ai Modelli organizzativi il sistema del Decreto attribuisce molteplici funzioni. Essi, se approntati e implementati prima della commissione del reato, possono:

- consentire l'esenzione da responsabilità della persona giuridica, al ricorrere degli ulteriori presupposti previsti dall'art. 6 del Decreto;
- se adottati in seguito alla commissione del reato, purché prima della dichiarazione di apertura del dibattimento di primo grado:
  - determinare una riduzione della sanzione pecuniaria (al ricorrere degli ulteriori presupposti di cui all'art. 12, comma 2 del Decreto);
  - determinare l'esclusione delle sanzioni interdittive (se ricorrono gli ulteriori presupposti di cui all'art. 17 del Decreto);
  - se adottati in seguito all'applicazione di una misura cautelare, possono comportarne la sospensione a norma dell'art. 49 del Decreto.

Quanto all'efficacia del Modello, il legislatore, all'art. 6, comma 2 – comma 2 bis, D.lgs. 231/2001, statuisce che il Modello deve soddisfare le seguenti esigenze:

- individuare le attività nel cui ambito esiste la possibilità che vengano commessi i Reati previsti dal Decreto;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individuare le modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei Reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.;
- introdurre un sistema per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro.

La caratteristica dell'effettività del Modello è invece legata alla sua efficace attuazione che, a norma dell'art. 7, comma 4, D.lgs. 231/2001, richiede:

- 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 (aggiornamento del Modello);
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

3.1.2 Fonti per la costruzione del Modello: Linee Guida di Confindustria

L'art. 6, comma 3 del Decreto 231 stabilisce che i modelli organizzativi possono essere adottati sulla base di codici di comportamento (o linee guida) redatti dalle associazioni rappresentative di categoria e comunicati al Ministero della Giustizia. In particolare, Confindustria ha pubblicato le proprie "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231/2001" già nel marzo 2002, provvedendo ad aggiornarle, a seguito delle varie modifiche subite dal Decreto 231, nel marzo 2008, nel luglio 2014 e, da ultimo, il 25 giugno 2021 a seguito delle novità legislative, giurisprudenziali e della prassi applicativa nel frattempo intervenute. Rispetto alle precedenti versioni, le nuove Linee Guida approfondiscono alcuni temi, quali il sistema integrato di gestione dei rischi, i sistemi di controllo ai fini della compliance fiscale, il whistleblowing e le comunicazioni delle informazioni non finanziarie. La sezione dedicata all'Organismo di Vigilanza riprende le Guidelines precedenti, ponendo particolare enfasi e rinforzando il punto relativo al budget destinato all'OdV ed all'importanza della collaborazione tra OdV e Collegio Sindacale, richiamando i principi stabiliti nel "Codice di Corporate Governance".

Le Linee Guida di Confindustria individuano uno schema fondato sui processi di risk management e *risk assessment* che può essere in sintesi così riepilogato:

- individuazione delle aree di rischio, volta a verificare in quale area/settore aziendale sia possibile la realizzazione degli eventi pregiudizievoli previsti dal D.lgs. 231/2001;
- predisposizione di un sistema di controllo in grado di prevenire i rischi attraverso l'adozione di appositi protocolli. Le componenti più rilevanti del sistema di controllo ideato da Confindustria sono:
    - Codice Etico;
    - sistema organizzativo;
    - procedure manuali ed informatiche;
    - poteri autorizzativi e di firma;
    - sistemi di controllo di gestione;
    - comunicazione al personale e sua formazione.

Le componenti del sistema di controllo devono essere informate ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- applicazione del principio di separazione delle funzioni, secondo il quale nessuno può gestire in autonomia un intero processo;
- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio per la violazione delle norme del Codice Etico e delle procedure previste dal Modello;
- obblighi di informazione da parte dell'Organismo di Vigilanza.

Per la predisposizione del proprio Modello, VISTA TECHNOLOGY ha quindi espressamente tenuto conto:

- delle disposizioni del D.lgs. 231/2001, della relazione ministeriale accompagnatoria e del decreto ministeriale 26 giugno 2003 n. 201 recante il regolamento di esecuzione del D.Lgs. 231/2001;
- delle linee guida predisposte da Confindustria;
- della dottrina e della giurisprudenza formatesi sino ad oggi.

3.2 Sezione Seconda – Il Contenuto del Modello di VISTA TECHNOLOGY S.r.l.

3.2.1 Adozione del Modello

3.2.1.1 L'Attività e la Struttura Organizzativa di VISTA TECHNOLOGY S.r.l.

VISTA TECHNOLOGY è una società controllata del gruppo DGS, un gruppo privato attivo nel settore dell'*Information and Communication Technology* (di seguito "*ICT*") il quale fornisce soluzioni professionali di valore ad alto contenuto tecnologico, attraverso la combinazione di una visione strategica legata agli obiettivi di business, con un'anima innovativa legata alla tecnologia.

Il gruppo DGS è costituito da un insieme di Società che fanno capo alla Capogruppo DGS S.p.A. che detiene il 100% del capitale sociale di VISTA TECHNOLOGY S.r.l., assumendo pertanto la qualifica di Socio Unico.

Il gruppo, che opera sul mercato tramite la Capogruppo DGS S.p.A., è organizzato attraverso tre Business Unit (Digital Solutions, Cyber Solutions e Advisory) coprendo l'intera catena del valore *ICT*: pianificazione, progettazione, sviluppo, integrazione, implementazione e manutenzione di soluzioni ed infrastrutture sistemiche complesse, basate su tutte le principali tecnologie presenti sul mercato.

Nello specifico, VISTA TECHNOLOGY si occupa della produzione e commercializzazione di software di cyber sicurezza; è specializzata nell'integrazione di soluzione per Cloud Native Application Infrastructure, Cloud Data Center e Networking, Secure Devops e Data Intelligence.

La Società si rivolge a Clienti appartenenti sia al settore pubblico che privato, con diversi Business (Public Sector, Health, Manufacturing, Financial Services, Energy & Utility).

La Società ha privilegiato un sistema di *corporate governance* tradizionale che si fonda su:

- Un organo amministrativo - il Consiglio di amministrazione - composto da 4 amministratori, cui spettano tutti i poteri di ordinaria e straordinaria amministrazione per il raggiungimento dello scopo sociale, esclusi i poteri che la legge riserva al Socio Unico (DGS S.p.A.).

  La rappresentanza della Società, di fronte ai terzi ed in giudizio, spetta al Presidente del Consiglio di amministrazione e agli Amministratori Delegati. Le persone cui spetta o sia stata delegata la rappresentanza della Società potranno nominare e revocare avvocati e procuratori alle liti nonché procuratori speciali per singoli negozi o categorie di negozi, nei limiti dei loro poteri e/o di quelli delegati.

Il Socio Unico ha affidato ad una società di revisione, iscritta all'Albo Speciale, l'incarico di revisione legale dei conti della Società.

Come si avrà modo di chiarire nel prosieguo, si precisa che la Società riceve alcuni servizi di staff dalla Controllante, sulla base di contratti infragruppo.

3.2.2 I Principi ispiratori del Modello

Il presente Modello è stato predisposto nel rispetto delle peculiarità dell'attività della Società e della sua struttura organizzativa e, pertanto, perfeziona ed integra gli specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni aziendali e ad effettuare i controlli sulle attività aziendali, e specificamente dei seguenti:

- Strumenti di Governance
- Sistema di controllo interno

3.2.2.1 Gli strumenti di *governance*

Nella costruzione del Modello di VISTA TECHNOLOGY si è tenuto conto degli strumenti di governo dell'organizzazione della Società che ne garantiscono il funzionamento, che possono essere così riassunti:

- Statuto - che, in conformità con le disposizioni di legge vigenti, contempla diverse previsioni relative al governo societario volte ad assicurare il corretto svolgimento dell'attività di gestione.

- Sistema delle deleghe e delle procure - che stabilisce i poteri per rappresentare o impegnare la società e, attraverso il sistema di deleghe interne, le responsabilità per quanto concerne gli aspetti in tema di ambiente e sicurezza sul lavoro.
- Organigramma aziendale del gruppo DGS.
- Contratti di prestazioni infragruppo (di seguito, anche “contratti intercompany”).
- Codice Etico di gruppo.
- Corpo procedurale interno e policy di gruppo - costituito da procedure, manuali e comunicazioni interne volte a regolamentare in modo chiaro ed efficace i processi rilevanti della Società.

Tali politiche adottate dalla Società sono necessarie a garantire la qualità del servizio/prodotto fornito, il suo continuo miglioramento, la soddisfazione del cliente, la protezione del patrimonio informativo dell’azienda e la salute e sicurezza sui luoghi di lavoro.

Le regole, le procedure e i principi contenuti nella documentazione sopra elencata, pur non essendo riportati dettagliatamente nel presente Modello, costituiscono un prezioso strumento a presidio di comportamenti illeciti in generale, inclusi quelli di cui al D.lgs. 231/2001; esse fanno parte del più ampio sistema di organizzazione, gestione e controllo che il Modello intende integrare e che tutti i soggetti destinatari sono tenuti a rispettare, in relazione al tipo di rapporto in essere con la Società.

3.2.2.2 Il Sistema di controllo interno

Il sistema di controllo interno di VISTA TECHNOLOGY è l’insieme delle attività, prassi consolidate, procedure, regole comportamentali e strutture organizzative volto a consentire, attraverso il presidiare continuo dei rischi della Società, una conduzione dell’impresa sana, corretta e coerente con gli obiettivi prefissati e nel rispetto di leggi e regolamenti, ivi compreso il Decreto stesso.

Questo sistema di regole e controlli, sia internamente alla Società che a livello del gruppo DGS, coinvolge diversi attori aziendali:

- Il Consiglio di amministrazione (ente di indirizzo), che definisce le linee guida e la visione del funzionamento del globale per il Sistema di Controllo Interno.
- La Società di Revisione (ente di supervisione), la quale vigila - con indipendenza e imparzialità - sulla regolare tenuta dei libri contabili, sulla regolarità delle dichiarazioni fiscali e, in generale, sulla correttezza della rappresentazione delle voci economiche inserite nel bilancio d’esercizio.
- Il Comitato di Sicurezza, (composto da CISO, DPO, Compliance Officer, Privacy Officer e QHSE Officer), incaricato di definire gli indirizzi strategici, supervisionare e coordinare le attività connesse alla sicurezza delle informazioni, alla conformità normativa in materia di privacy e alla gestione integrata degli standard certificati per tutto il gruppo DGS.
- La Funzione Compliance di gruppo, la quale assicura conformità alle normative di riferimento interne (es, Policy, Procedure), esterne (es. D.lgs. 231/2001) e agli standard internazionali di certificazione.
- Il Gestore delle segnalazioni whistleblowing di gruppo, nominato ai sensi dell’art.4 del D.lgs. 231/2001, incaricato di ricevere e dare seguito alle segnalazioni effettuate ai sensi del D.lgs. 24/2023, svolgendo (ove necessario) attività di approfondimento e istruttoria per l’accertamento dei fatti oggetto di segnalazione.
- L’Internal Audit di gruppo, a cui è affidata la funzione di procedere ad una valutazione indipendente e obiettiva dell’adeguatezza, dell’efficacia e della resilienza del sistema di controllo interno, della gestione dei rischi e dei processi di governance del gruppo.
- Il Responsabile per la prevenzione della corruzione (RAC) di gruppo, a cui è affidata la funzione di garantire il rispetto e il continuo miglioramento del Sistema di Gestione del rischio ai sensi della ISO 37001:2016 (Sistema di Gestione per la prevenzione della corruzione).
- Tutti i soggetti o le funzioni che definiscono e gestiscono i controlli cosiddetti di linea, insiti nei processi operativi, ovvero quei controlli procedurali, informatici, finanziari, comportamentali, svolti sia da chi mette in atto una determinata attività, sia da chi ne ha la

responsabilità di supervisione, che richiedono competenze specifiche del business, dei rischi e/o delle normative pertinenti.

Il Sistema di controllo interno della Società si basa, oltre che sugli strumenti di governance di cui al precedente paragrafo 2.1, sui seguenti elementi qualificanti:

- sistema di pianificazione, controllo di gestione e *reporting*, che ha lo scopo di guidare la gestione aziendale al conseguimento degli obiettivi pianificati, evidenziando gli scostamenti tra questi ultimi ed i risultati effettivi della gestione, mettendo così in grado i responsabili, di predisporre, decidere ed attuare le opportune azioni correttive;
- sistemi informatici già orientati alla segregazione delle funzioni e regolati da procedure interne che garantiscono sicurezza, privacy e corretto utilizzo da parte degli utenti;
- Sistema di Gestione Integrato (cfr. ***AI-06*** *Elenco delle certificazioni attive*).

I principali obiettivi del sistema dei controlli interni della Società si sostanziano nel garantire con ragionevole sicurezza il raggiungimento di obiettivi strategici, operativi, d'informazione interna e verso il mercato e di conformità alle leggi e regolamenti applicabili.

Alla base di questi obiettivi vi sono i seguenti principi generali:

- ogni operazione, transazione, azione deve essere verificabile, documentata, coerente e congrua: per ciascuna operazione, vi deve essere un adeguato supporto documentale che consenta di poter procedere, in ogni momento, all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione ed individuino chi ha autorizzato, effettuato, registrato e verificato l'operazione stessa. Al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle norme di legge, sono adottate misure di sicurezza adeguate;
- nessuno può gestire in autonomia un intero processo: l'osservanza di tale principio è garantito dall'applicazione del principio di separazione delle funzioni e dei compiti applicato all'interno della Società, in base al quale persone e funzioni diverse hanno la responsabilità di autorizzare un'operazione, di contabilizzarla, di attuarla e/o di controllarla. Inoltre, a nessuno sono attribuiti poteri illimitati, i poteri e le responsabilità sono definiti e diffusi all'interno della Società, i poteri autorizzativi e di firma sono coerenti con le responsabilità organizzative;
- il sistema di controllo deve poter documentare l'effettuazione dei controlli, anche di supervisione.

3.2.2.3 La costruzione del modello

La scelta del Consiglio di amministrazione di VISTA TECHNOLOGY S.r.l. di dotarsi di un Modello si inserisce nella più ampia politica d'impresa della Società che si esplicita in interventi ed iniziative volte a sensibilizzare tutto il personale alla gestione trasparente e corretta della Società, al rispetto delle norme giuridiche vigenti e dei fondamentali principi di etica degli affari nel perseguimento dell'oggetto sociale.

La "costruzione" del presente Modello ha preso l'avvio dall'analisi del sistema di governance, della struttura organizzativa e di tutti i principi ispiratori di cui al precedente paragrafo 2.1 e ha tenuto in espressa considerazione le indicazioni ad oggi rilevate dalla giurisprudenza e dai pronunciamenti anche provvisori dell'Autorità Giudiziaria, unitamente a quelle espresse dalle Associazioni di Categoria (tipicamente Linee Guida Confindustria).

Il processo di costruzione del Modello si è dunque sviluppato in diverse fasi, basate sul rispetto dei principi di tracciabilità e verificabilità delle attività svolte.

Il punto di partenza è stato l'individuazione della **mappa delle aree a rischio 231** ovvero delle attività svolte dalla Società nel cui ambito possono essere commessi i Reati, secondo quanto espressamente previsto dall'art. 6, c. 2, lett. a) del Decreto.

Si è quindi provveduto alla valutazione del sistema di controllo interno a presidio dei rischi individuati ed alla redazione di specifici **Protocolli**, finalizzati a governare i profili di rischio enucleati a seguito

dell'attività di mappatura delle attività societarie, secondo quanto richiesto dall'art. 6 c. 2 lett. b) del D.lgs. 231/2001.

Inoltre, la Società agisce nel rispetto di valori e principi di comportamento definiti all'interno del **Codice Etico di gruppo**.

In conformità a quanto richiesto dagli artt. 6 c. 2 lett. d) e lett. e) e lettera c.2 ter del Decreto, si è provveduto quindi:

- a definire le caratteristiche, i ruoli e i compiti dell'**Organismo di Vigilanza** (così come riportato nel successivo par. 3), espressamente preposto al presidio dell'effettiva applicazione del Modello ed alla sua verifica in termini di adeguatezza ed efficacia;
- a delineare un apparato sanzionatorio (riportato nel successivo par. 4) avverso a tutte le violazioni del Modello e del D.lgs. 231/2001;
- a definire le modalità di diffusione del Modello e di relativa formazione del personale (così come indicato nel successivo par. 5);
- a definire le modalità di aggiornamento del Modello stesso (riportato nel successivo par. 6);
- a definire le modalità di nomina del difensore di fiducia dell'Ente in conformità a quanto previsto dall'art. 39 del Decreto;
- a definire le modalità di gestione delle segnalazioni (riportato nel paragrafo 3 della Sezione Prima);
- a prevedere un sistema per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro.

3.2.2.4 La Mappa delle aree a rischio 231

Il Modello di VISTA TECHNOLOGY si basa sulla individuazione della mappa delle aree a rischio 231, ovvero delle attività nel cui ambito può essere commesso uno dei reati presupposto, secondo quanto espressamente previsto dall'art. 6, c. II, lett. a) del Decreto.

La mappatura delle aree a rischio 231 è stata realizzata valutando gli specifici ambiti operativi e la struttura organizzativa della Società, con riferimento ai rischi di reato in concreto prospettabili.

Nell'ambito di tale attività, le aree a rischio 231 della Società sono state differenziate a seconda che esse rientrino nell'ambito di processi le cui attività:

a) sono svolte internamente dalla Società mediante le proprie risorse aziendali;
b) sono realizzate dalla Controllante in favore di VISTA TECHNOLOGY.

Il presente paragrafo descrive le modalità di mappatura delle aree a rischio 231 rientranti nell'ambito di processi svolti internamente dalla Società, approfondendo - inoltre - le relative modalità di valutazione del rischio.

Diversamente, le modalità di mappatura delle aree a rischio 231 rientranti nell'ambito di processi svolti in *outsourcing* da parte della Controllante in favore della Società – così come le relative modalità di valutazione del rischio – saranno oggetto di approfondimento nel successivo § 3.2.2.5.

La metodologia seguita ha visto il coinvolgimento di un gruppo di lavoro integrato composto da professionisti esterni - con competenze di risk management e controllo interno -, risorse interne della Società e la Funzione Compliance di gruppo.

Di seguito sono esposte le metodologie seguite e i criteri adottati nelle varie fasi.

I fase: raccolta e analisi di tutta la documentazione rilevante

Propedeutica all'individuazione delle attività a rischio è stata l'analisi documentale: si è innanzitutto proceduto a raccogliere la documentazione ufficiale rilevante, messa a disposizione dalla Società, al fine di meglio comprendere l'attività da questa svolta e identificare le aree aziendali oggetto d'analisi.

A titolo esemplificativo e non esaustivo è stata analizzata la seguente documentazione:

- Visura;
- Statuto;
- Organigramma del gruppo DGS;

- Policy e procedure aziendali del gruppo DGS;
- Documentazione relativa al sistema di deleghe e procure;
- Documentazione relativa al Sistema di Gestione Integrato;
- Elementi relativi alle sanzioni disciplinari previste dai C.C.N.L. applicabili;
- Contratti di prestazioni intercompany;
- Contratti significativi con terze parti.

II fase: risk assessment

Scopo della fase in oggetto è stata la preventiva identificazione dei processi ed attività aziendali e quindi l'individuazione delle aree a rischio ovvero delle aree aziendali nel cui ambito possono essere commessi i reati.

Tenuto conto tanto delle attività svolte in outsourcing dalla Controllante (in forza di appositi contratti intercompany in essere tra quest'ultima e la Società), quanto di quelle svolte internamente dalla Società stessa, le attività aziendali sono quindi state suddivise nei seguenti principali processi di riferimento:

- Risorse Umane;
- Acquisti;
- Amministrazione, Finanza e Controllo;
- Mergers & Acquisitions;
- Legale;
- Societario;
- Compliance;
- Marketing e Comunicazione;
- Information Technology;
- Salute e Sicurezza sul Lavoro e Ambiente;
- Operation;
- Business.

A fronte di tale classificazione, per i soli processi aziendali le cui attività sono svolte internamente dalla Società, sono state quindi identificate le risorse aziendali con una conoscenza approfondita dei citati processi aziendali e dei meccanismi di controllo esistenti, che sono state intervistate dal gruppo di lavoro al fine di costruire un Modello il più possibile aderente agli specifici ambiti operativi e alla struttura organizzativa della società, con riferimento ai rischi di reato in concreto prospettabili.

Le interviste, infatti, finalizzate altresì ad avviare il processo di sensibilizzazione rispetto alle previsioni di cui al D.lgs. 231/2001, alle attività di adeguamento della Società al predetto Decreto, all'importanza del rispetto delle regole interne adottate dalla Società per la prevenzione dei reati, sono state condotte con l'obiettivo di individuare i processi e le attività potenzialmente a rischio di commissione dei reati previsti dal Decreto nonché i presidi già esistenti atti a mitigare i predetti rischi.

È stata così effettuata una mappatura di tutti i processi della Società e delle relative attività, con evidenza delle Strutture aziendali a vario titolo coinvolte. Per ogni attività è stato quindi evidenziato il profilo di rischio attraverso l'indicazione dei potenziali Reati associabili e l'esemplificazione delle possibili modalità di realizzazione dei reati stessi. I risultati di tale attività sono stati formalizzati in specifico documento denominato "**Mappa delle aree a rischio 231**" che rimane a disposizione dell'Organismo di Vigilanza per l'attività istituzionale ad esso demandata.

È importante evidenziare che la mappa delle attività a rischio 231 fotografa la situazione esistente alla data di redazione del presente Modello. L'evolvere delle attività aziendali richiederà il necessario aggiornamento della mappatura, al fine di ricomprendere gli eventuali rischi associabili alle nuove attività.

Conformemente a quanto previsto dall'art. 6, comma 2, lett. a) D.Lgs. 231/2001 si riportano le aree di attività aziendali individuate come a rischio ai sensi del D.Lgs. 231/2001, ovvero nel cui ambito

potrebbero verificarsi le condizioni, gli strumenti e/o i mezzi per la commissione delle fattispecie di reato previste dal Decreto.

In particolare, sono state identificate le seguenti **aree a rischio 231**:

- Selezione, assunzione e gestione del personale;
- Approvvigionamento di beni e servizi;
- Acquisizione di Consulenze e incarichi professionali;
- Flussi monetari e finanziari;
- Amministrazione, Contabilità, Bilancio e Operazioni sul Capitale;
- Operazioni Straordinarie;
- Rapporti infragruppo;
- Contenziosi ed accordi transattivi;
- Acquisizione e gestione Commessa;
- Adempimenti con la Pubblica Amministrazione e le Autorità di Vigilanza;
- Richiesta e gestione dei finanziamenti pubblici;
- Relazioni istituzionali;
- Rapporti con i soci e gli organi sociali;
- Gestione della Fiscalità;
- Omaggi, sponsorizzazioni, liberalità ed eventi di co-marketing;
- Rimborso Spese e Spese di Rappresentanza;
- Marketing e Comunicazione;
- Adempimenti in materia di salute e sicurezza sul lavoro e ambientali;
- Sistemi informativi.

In tali aree si sono ritenuti maggiormente rilevanti i rischi di commissione di alcune fattispecie di reato indicati negli artt. 24, 24-*bis*, 24-*ter*, 25, 25-*bis*.1, 25-*ter*, 25-*quater*, 25-*quinquies*, 25-*sexies*, 25-*septies*, 25-*octies*, 25-*octies*.1, 25-*novies*, 25-*decies*, 25-*undecies*, 25-*duodecies*, 25-*terdecies*, 25-*quinquiesdecies*, 25-*sexiesdecies* e dall'art. 10, Legge 16 marzo 2006, n.146, del Decreto.

Relativamente agli altri reati ed illeciti (e tipicamente i *reati in materia di pratiche di mutilazione degli organi genitali femminili, i reati di market abuse, la Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati e delitti contro il patrimonio culturale*) si è ritenuto, anche sulla scorta del *Risk Assessment* effettuato, che la specifica attività svolta dalla Società non presenti profili di rischio tali da rendere ragionevolmente fondata la possibilità della loro commissione nell'interesse o a vantaggio della stessa. Si è pertanto stimato esaustivo il richiamo ai principi contenuti sia nel presente Modello che nel Codice Etico di gruppo, ove si vincolano gli esponenti aziendali, i collaboratori ed i partners commerciali al rispetto dei valori di solidarietà, tutela della personalità individuale, correttezza, moralità e rispetto delle leggi.

III fase: Gap Analysis

Scopo di tale fase è consistito nell'individuazione, per ciascuna area di rischio, dei presidi organizzativi, di controllo e comportamento esistenti a presidio delle specifiche fattispecie di reato richiamate dal Decreto, nella valutazione della loro idoneità a prevenire i rischi evidenziati nella precedente fase di *risk assessment* e quindi nelle azioni di miglioramento da apportare.

È stata fatta quindi un'analisi comparativa tra il Modello di organizzazione gestione e controllo esistente ("*as is*") ed un Modello di riferimento a tendere valutato sulla base del contenuto del Decreto, delle indicazioni dell'ampia giurisprudenza e delle linee guida di Confindustria ("*to be*").

In particolare, l'analisi è stata condotta con l'obiettivo di verificare:

- l'esistenza di regole comportamentali di carattere generale a presidio delle attività svolte;
- l'esistenza e l'adeguatezza di procedure che regolino lo svolgimento delle attività nel rispetto dei principi di controllo;

- il rispetto e l'attuazione concreta del generale principio di separazione dei compiti;
- l'esistenza di livelli autorizzativi a garanzia di un adeguato controllo del processo decisionale;
- l'esistenza di specifiche attività di controllo e di monitoraggio sulle attività a rischio.

Da tale confronto sono state identificate le aree di miglioramento del sistema di controllo interno esistente che, condivise con i responsabili delle Funzioni aziendali interessate, sono state implementate nei Protocolli.

3.2.2.5 Mappatura delle aree a rischio 231 nell'ambito di processi svolti in *outsourcing*

Come già illustrato, l'attività di mappatura e di valutazione del rischio ai sensi del D.Lgs. 231/2001 ha considerato la distinzione tra le attività operative svolte direttamente dalla Società e quelle affidate, in forza di specifici contratti intercompany, alla Capogruppo, che le esegue in outsourcing nell'interesse di VISTA TECHNOLOGY.

L'individuazione dei processi e delle attività sensibili svolti in outsourcing dalla Capogruppo si fonda sui contratti intercompany vigenti al momento dell'analisi, ai quali si fa rinvio per il dettaglio delle prestazioni oggetto di esternalizzazione.

Tale differenziazione è stata debitamente considerata sia nella mappatura delle attività a rischio 231 rientranti nel perimetro operativo della Società, sia nella metodologia di valutazione del relativo rischio.

In relazione alla mappatura, sono state escluse dal perimetro del rischio 231 a cui è direttamente esposta la Società le attività interamente esternalizzate alla Capogruppo, ritenendo che le stesse non integrino, in capo a VISTA TECHNOLOGY, un'esposizione diretta alla possibile commissione di illeciti. Per contro, nella valutazione del rischio è stata tenuta in considerazione l'esternalizzazione di tali attività, facendo riferimento alle attività di *risk assessment* e della *gap analysis* condotti da DGS S.p.A., con il supporto della Funzione Compliance di gruppo.

Tale approccio metodologico riflette una logica di corretta allocazione del rischio, basata sul criterio della prossimità operativa alla fonte di rischio.

Si evidenzia, inoltre, che:

- la metodologia di valutazione del rischio ai sensi del D.Lgs. 231/2001 è adottata in modo uniforme all'interno del gruppo (cfr. § 3.2.2.4);
- la Funzione Compliance opera a livello di gruppo, garantendo una visione integrata e trasversale dei sistemi di gestione del rischio di commissione dei reati delle singole società.

Si evidenzia, infine, che la mappa delle attività a rischio 231 svolte in outsourcing rappresenta la fotografia della situazione esistente alla data di adozione del presente Modello, sulla base degli accordi contrattuali intercompany vigenti. Ogni evoluzione organizzativa, modifica dei contratti o cambiamento nelle modalità esecutive delle attività esternalizzate dovrà essere oggetto di aggiornamento della mappatura, al fine di garantire un presidio costante ed efficace dei rischi potenzialmente rilevanti per la Società, in coerenza con il modello organizzativo e il Sistema di Gestione Integrato del gruppo DGS.

3.2.2.6 I Protocolli

A seguito della identificazione delle aree a rischio e in base al relativo sistema di controllo esistente, la Società ha elaborato specifici Protocolli, in conformità a quanto prescritto dall'art. 6 c. 2 lett. b) D.lgs. 231/2001, che contengono un insieme di regole e di principi di controllo e di comportamento ritenuti idonei a governare il profilo di rischio individuato.

Tenuto conto dell'appartenenza della Società al gruppo DGS e dell'esistenza di contratti *intercompany* tra controllate e holding, il presente Modello recepisce, all'interno della Parte Speciale, i principi di condotta e controllo già previsti nei Protocolli del Modello adottato da DGS S.p.A.

Conformemente a quanto precisato dalle più aggiornate Linee Guida di settore (Confindustria), nei Protocolli sono stati previsti specifici presidi di controllo relativi: (i) ai rapporti contrattuali infragruppo; (ii) alle autorizzazioni relative agli *input* forniti e ai controlli sugli *output* ottenuti; (iii) alla gestione dei

rapporti e della fatturazione *intercompany*; (iv) alle transazioni infragruppo; (v) ad ogni ulteriore operazione infragruppo che presenti uno specifico rischio di commissione di un reato presupposto.

Per ciascuna area a rischio 231 è stato creato un Protocollo, ispirato alla regola di rendere documentate e verificabili le varie fasi del processo decisionale, onde sia possibile risalire alla motivazione che ha guidato la decisione.

I principi di controllo riportati nei Protocolli fanno riferimento a:

- livelli autorizzativi;
- segregazione funzionale delle attività autorizzative, operative e di controllo;
- controlli specifici;
- tracciabilità del processo decisionale e archiviazione della documentazione a supporto.

I Protocolli sono stati sottoposti all'esame dei soggetti aventi la responsabilità della gestione delle attività a rischio per la loro valutazione e approvazione, rendendo così ufficiali ed obbligatorie le regole di condotta ivi contenute nei confronti di tutti coloro che si trovino a compiere l'attività nell'ambito della quale è stato individuato un profilo di rischio.

Per le attività svolte interamente in outsourcing dalla Controllante, sono considerati immediatamente applicabili e precettivi i Protocolli definiti nell'ambito del relativo Modello 231.

Laddove esistente, i Protocolli richiamano il corpo procedurale pro tempore vigente della Società e di tutto il gruppo DGS.

3.2.2.7 Il Codice Etico di gruppo

La definizione dei Protocolli si completa e si integra con il Codice Etico di gruppo che racchiude principi generali che sono il fondamento della cultura aziendale e rappresentano gli standard di comportamento quotidiano all'interno e all'esterno del gruppo DGS.

Il gruppo ha ritenuto che un numero ridotto di principi semplici ma saldi possa servire da guida per risolvere dilemmi e conflitti, partendo dal presupposto che si agisca in modo responsabile e che si faccia uso di buonsenso.

Precisamente:

- agire con integrità e senso di responsabilità;
- rispettare leggi e regolamenti;
- rispettare la dignità e i diritti di ciascuno;
- reagire con flessibilità, rapidità e intraprendenza ai cambiamenti del mercato;
- porre attenzione alle esigenze ed aspettative degli Stakeholder garantendo completezza, attendibilità, uniformità e tempestività di informazioni;
- tutelare la riservatezza e confidenzialità delle informazioni apprese in ragione della propria funzione lavorativa;
- creare un valore sostenibile nel tempo per tutti gli stakeholder;
- promuovere la ricerca e l'innovazione;
- valorizzare e sviluppare le capacità e competenza di ognuno;
- porre la massima attenzione e cura al servizio reso;
- agire nel rispetto dell'ambiente naturale;
- utilizzare beni e risorse dell'azienda nel rispetto dell'interesse del gruppo e degli azionisti.

La Società ha adottato un Codice Etico di gruppo, la cui applicabilità è valida per tutte le società del gruppo DGS, attraverso cui intende uniformare la gestione delle proprie attività in relazione ai comportamenti che possono integrare le fattispecie di reato disciplinate dal D.lgs. 231/2001.

Il Codice Etico di gruppo costituisce parte integrante del Modello organizzativo (Allegato II), pur avendo portata e finalità differenti.

Sotto tale profilo, infatti, è opportuno precisare che:

- il Codice Etico di gruppo riveste una rilevanza generale in quanto contiene una serie di principi e valori di "deontologia aziendale", che tutte le società del gruppo riconoscono come propri e sui quali intendono richiamare l'osservanza di tutti i suoi dipendenti e di tutti coloro che, anche all'esterno di ciascuna società, cooperano al perseguimento degli obiettivi aziendali;
- il Modello e i Protocolli di Decisione rispondono e soddisfano, invece, conformemente a quanto previsto nel Decreto, l'esigenza di predisporre un sistema di regole interne diretto a prevenire la commissione di particolari tipologie di reati (per fatti che, commessi nell'interesse o a vantaggio della Società, possono comportare una responsabilità amministrativa in base alle disposizioni del Decreto medesimo).

Il Codice Etico di gruppo viene distribuito a tutti i dipendenti delle società facenti parte del gruppo DGS. Viene inoltre reso disponibile ai Terzi, ai quali viene richiesto il rispetto dei principi in esso contenuti, mediante sottoscrizione di apposite clausole nei contratti con i terzi.

È inoltre disponibile sul sito internet della Società all'indirizzo www.vistatech.it nella sezione **Governance e Compliance**.

3.2.3 Organismo di Vigilanza

3.2.3.1 Le caratteristiche dell'Organismo di Vigilanza

L'esenzione dalla responsabilità amministrativa – come disciplinata dall'art. 6 comma 1 D.lgs. 231/2001 – prevede anche l'obbligatoria istituzione di un Organismo dell'Ente, dotato di autonomi poteri di controllo e di iniziativa, che consentano di vigilare sul funzionamento e sull'osservanza del Modello, e tenuto a curarne l'aggiornamento.

La caratteristica dell'**autonomia dei poteri di iniziativa e controllo** in capo all'OdV è rispettata se:

- è garantita all'OdV l'indipendenza gerarchica rispetto a tutti gli organi e le funzioni della Società sui quali è chiamato a vigilare facendo in modo che lo stesso riporti direttamente al Consiglio di amministrazione;
- i suoi componenti non siano direttamente coinvolti in attività gestionali che risultino oggetto del controllo da parte del medesimo Organismo;
- sia dotato di autonomia finanziaria per il corretto svolgimento delle proprie attività.

Oltre all'indipendenza e all'autonomia dei poteri prevista dallo stesso Decreto, la Società ha ritenuto di allinearsi anche alle Linee Guida di Confindustria nonché alle pronunce della magistratura in materia, che hanno indicato come necessari anche i requisiti di professionalità e di continuità di azione.

Per quanto attiene al requisito della **professionalità**, è necessario che l'OdV sia dotato degli strumenti e tecniche necessari allo svolgimento dell'attività assegnata, sia di carattere ispettivo che consulenziale. La professionalità è assicurata anche dalla previsione della facoltà dell'Organismo di avvalersi, al fine dello svolgimento del suo incarico e con assoluta autonomia di spesa (all'interno del budget ad esso assegnato), delle specifiche professionalità sia dei responsabili di varie funzioni aziendali, che di consulenti esterni.

Quanto, infine, alla **continuità di azione**, l'OdV dovrà garantire un'efficace e costante attuazione del Modello, e rappresentare un referente per i Destinatari del Modello. La continuità di azione è inoltre garantita dalla circostanza che l'Organismo opera stabilmente avvalendosi dell'ausilio delle funzioni interne per lo svolgimento dell'incarico assegnatogli, nonché dal fatto di ricevere costanti informazioni da parte delle strutture individuate come potenziali aree a rischio.

3.2.3.2 L'identificazione dell'Organismo di Vigilanza

Per quanto concerne la possibile composizione dell'OdV, la dottrina e la prassi hanno elaborato diverse soluzioni, in ragione delle caratteristiche dimensionali ed operative dell'Ente, delle relative regole di corporate *governance* e della necessità di realizzare un equo bilanciamento tra costi e benefici. Sono pertanto ritenute percorribili sia ipotesi di definizione di strutture appositamente create

nell'Ente, che l'attribuzione dei compiti dell'OdV ad organi già esistenti. Del pari, possono prescegliersi sia strutture a composizione collegiale che monosoggettiva. Infine, nell'enucleazione dei componenti dell'OdV, è possibile affidare detta qualifica a soggetti esterni, che posseggano le specifiche competenze necessarie per la migliore esecuzione dell'incarico.

Da ultimo ai sensi dell'art. 6 comma 4 *bis* del Decreto, introdotto dall'art. 14 comma 12, della Legge 12 novembre 2011, n. 183, nelle società di capitali la funzione di Organismo di Vigilanza può essere svolta dal Collegio Sindacale.

Salvo il caso in cui l'Ente decida di affidare l'incarico di Organismo di Vigilanza ad uno dei soggetti indicati all'art. 6 comma 4 *bis* del D.lgs. 231/2001, la concreta costituzione di tale organismo è rimessa all'iniziativa organizzativa dell'Ente, sempre in funzione del quadro delineato dal Decreto.

In considerazione di quanto sopra, nel caso di specie, la Società, tenuto conto della sua struttura e delle attività che vengono svolte, ha scelto di dotarsi di un organismo costituito ad hoc, plurisoggettivo.

Ad eccezione del Presidente, che deve necessariamente essere soggetto esterno all'organizzazione, i restanti componenti dell'Organismo di vigilanza, pur sempre nel rispetto dei requisiti di professionalità, indipendenza, autorevolezza e autonomia dei poteri di iniziativa e controllo, possono essere individuati in soggetti sia interni sia esterni all'organizzazione garantendo in tal modo l'apporto di competenze diversificate.

L'OdV è nominato con delibera del Consiglio di amministrazione. La nomina quale componente dell'Organismo di Vigilanza è condizionata dalla presenza dei requisiti soggettivi di eleggibilità, la cui ricorrenza e permanenza verranno di volta in volta accertate dal Consiglio di amministrazione.

In *primis*, i componenti dell'Organismo di Vigilanza, ai fini della valutazione del **requisito di indipendenza**, dal momento della nomina e per tutta la durata della carica, non dovranno:

- trovarsi in una posizione, neppure potenziale, di conflitto di interessi con VISTA TECHNOLOGY;
- rivestire incarichi esecutivi o delegati nel Consiglio di amministrazione della Società o di altra società facente parte del gruppo DGS;
- svolgere, all'interno della Società o di altra società del gruppo DGS, funzioni di tipo esecutivo direttamente connesse al business e/o attività di gestione operativa della Società, con poteri di firma singola. Qualora i componenti dell'Organismo di Vigilanza siano soggetti interni alla struttura aziendale, essi devono godere di una posizione organizzativa adeguatamente elevata e, comunque, tale da non poterli configurare come dipendenti da organi esecutivi;
- avere rapporti di parentela, coniugio o affinità entro il quarto grado con i componenti degli organi sociali, con persone che rivestono funzioni di rappresentanza con firma singola, di amministrazione o di direzione di VISTA TECHNOLOGY o di una sua struttura organizzativa dotata di autonomia finanziaria e funzionale o di un'altra società del gruppo DGS, nonché con persone che esercitano – anche di fatto – la gestione e il controllo di VISTA TECHNOLOGY, e la società di revisione.

Inoltre, la Società ha stabilito che i componenti dell'OdV devono essere in possesso dei **requisiti di professionalità e di onorabilità** di cui all'art. 109 del D.lgs. 1° settembre 1993, n. 385. In particolare, i componenti dell'Organismo di Vigilanza devono essere nominati tra soggetti con professionalità adeguata in materia giuridica e di controllo e gestione dei rischi aziendali e non devono (condizioni di ineleggibilità):

- trovarsi in stato di interdizione temporanea o di sospensione dagli uffici direttivi delle persone giuridiche e delle imprese;
- trovarsi in una delle condizioni di ineleggibilità o decadenza previste dall'art. 2382 del Codice civile;
- essere stati sottoposti a misure di prevenzione ai sensi D. Lgs. 6 settembre 2011, n. 159 e successive modificazioni e integrazioni, salvi gli effetti della riabilitazione;
- aver riportato sentenza di condanna o patteggiamento, ancorché non definitiva, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione, per un tempo non inferiore a un anno:

1. per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267 (legge fallimentare);
2. per uno dei delitti previsti dal titolo XI del Libro V del Codice civile (società e consorzi);
3. per un delitto non colposo, per un tempo non inferiore a un anno;
4. per un delitto contro la Pubblica Amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica ovvero per un delitto in materia tributaria;
5. per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;
6. per un reato che importi e abbia importato la condanna ad una pena da cui derivi l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

- essere stati destinatari a titolo personale di un decreto che dispone il giudizio per tutti gli illeciti previsti dal D.lgs. 231/2001;
- aver svolto funzioni di amministratore esecutivo nei tre esercizi precedenti alla nomina quale membro dell'Organismo di Vigilanza, in imprese:
  - sottoposte a fallimento, liquidazione coatta amministrativa o procedure equiparate;
  - operanti nel settore creditizio, finanziario, mobiliare e assicurativo sottoposte a procedure di amministrazione straordinaria.
- trovarsi in una delle situazioni contemplate nell'art. 2399 c.c. comma 1 lett. a), b) e c) e nello specifico:
  a) coloro che si trovano nelle condizioni previste dall'articolo 2382 c.c. (l'interdetto, l'inabilitato, il fallito, o chi è stato condannato ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità ad esercitare uffici direttivi);
  b) il coniuge, i parenti e gli affini entro il quarto grado degli amministratori della Società, gli amministratori, il coniuge, i parenti e gli affini entro il quarto grado degli amministratori delle società da questa controllate, delle società che la controllano e di quelle sottoposte a comune controllo;
  c) coloro che sono legati alla società o alle società da questa controllate o alle Società che la controllano o a quelle sottoposte a comune controllo da un rapporto di lavoro o da un rapporto continuativo di consulenza o di prestazione d'opera retribuita, ovvero da altri rapporti di natura patrimoniale che ne compromettano l'indipendenza.

L'eventuale **revoca** dei componenti dell'Organismo di Vigilanza potrà esclusivamente disporsi per ragioni connesse a gravi inadempimenti rispetto al mandato assunto, ivi comprese le violazioni degli obblighi di riservatezza e le intervenute cause di ineleggibilità sopra riportate.

Costituiscono giusta causa di revoca dei componenti dell'OdV:

- una grave negligenza nell'assolvimento dei compiti connessi con l'incarico;
- la violazione dei doveri di riservatezza;
- l'"omessa o insufficiente vigilanza" da parte dell'Organismo di Vigilanza – secondo quanto previsto dall'art. 6, comma 1, lett. d), D.lgs. 231/2001 gravi e accertati motivi di incompatibilità che ne vanifichino l'indipendenza e l'autonomia;
- assenza ingiustificata a due o più riunioni consecutive dell'OdV, a seguito di rituale convocazione.

La revoca del mandato dovrà, in ogni caso, essere deliberata dal Consiglio di amministrazione della Società con atto che specifichi chiaramente i motivi della decisione intrapresa.

I componenti dell'Organismo di Vigilanza decadono dalla carica nel momento in cui vengano a trovarsi successivamente alla loro nomina:

- in una delle situazioni contemplate nell'art. 2399 c.c. comma 1 lett. a), b) e c)
- condannati con sentenza definitiva (intendendosi per sentenza di condanna anche quella pronunciata *ex* art. 444 c.p.p.) per un tempo non inferiore a un anno, per uno dei reati indicati ai numeri 1, 2, 3, 4, 5, 6 delle condizioni di ineleggibilità innanzi indicate.

Costituiscono inoltre cause di **decadenza** dalla funzione di componente dell'Organismo di Vigilanza:

- la condanna con sentenza non definitiva per uno dei reati dei numeri da 1 a 6 delle condizioni di ineleggibilità innanzi indicate;
- l'applicazione di una delle pene per i reati di cui ai numeri da 1 a 6 delle condizioni di ineleggibilità innanzi indicate;
- l'applicazione di una misura cautelare personale;
- l'applicazione provvisoria di una delle misure di prevenzione previste dal libro I, titolo I, capo II del D. Lgs. settembre 2011, n. 159 e successive modificazioni e integrazioni e delle sanzioni amministrative accessorie previste dall'art. 187-*quater* del Decreto Legislativo n. 58/1998 (TUF).

Costituiscono infine ulteriori cause di decadenza per i membri dell'OdV rispetto a quelle precedentemente delineate l'esser indagati o condannati, anche con sentenza non definitiva o emessa *ex* artt. 444 e ss c.p.p. (patteggiamento) o anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione, per uno o più illeciti tra quelli tassativamente previsti dal D.lgs. 231/2001.

Per i componenti dell'OdV legati alla Società da rapporto di lavoro subordinato, lo scioglimento del rapporto di lavoro, per qualsiasi causa ciò avvenga, determina la decadenza automatica dall'ufficio.

Si precisa infine che la decadenza dalla carica di componente dell'OdV opera automaticamente sin dal momento della sopravvenienza della causa che l'ha prodotta, fermi restando gli ulteriori obblighi sotto descritti.

La nomina dei membri dell'Organismo di Vigilanza da parte del Consiglio di amministrazione diviene efficace solo in seguito al rilascio da parte di ciascun membro di una formale accettazione per iscritto dell'incarico che contenga altresì una dichiarazione circa la sussistenza dei requisiti prescritti dal Modello ed in particolare quelli di eleggibilità, professionalità, autonomia e indipendenza.

Ciascun componente dell'Organismo di Vigilanza può rinunciare alla carica in qualsiasi momento, previa comunicazione da presentarsi per iscritto al Consiglio di amministrazione ed in copia conoscenza agli altri componenti.

In caso di sopravvenuta causa di decadenza dalla carica, il membro dell'OdV interessato deve darne immediata comunicazione per iscritto al Consiglio di amministrazione e per conoscenza al Collegio sindacale ed agli altri membri dell'Organismo di Vigilanza medesimo. Anche in assenza della suddetta comunicazione, ciascun membro dell'Organismo di Vigilanza che venga a conoscenza dell'esistenza di una causa di decadenza in capo ad un altro componente, deve darne tempestiva comunicazione per iscritto al Consiglio di amministrazione e per conoscenza al Collegio sindacale per consentire al medesimo di adottare i necessari provvedimenti del caso.

In caso di rinuncia, sopravvenuta incapacità, morte, revoca o decadenza di un membro dell'OdV, il Consiglio di amministrazione provvede a deliberare la nomina del sostituto, senza ritardo.

In caso di rinuncia, sopravvenuta incapacità, morte, revoca o decadenza del Presidente, subentra a questi il membro più anziano, il quale rimane in carica fino alla data in cui il CdA abbia deliberato la nomina del nuovo Presidente dell'OdV.

Durante l'eventuale periodo di *vacatio* per il verificarsi di uno degli eventi sopra delineati, i restanti membri dell'Organismo di Vigilanza restano in carica con l'onere di richiedere al Consiglio di amministrazione di procedere tempestivamente alla nomina del membro mancante.

3.2.3.3 La definizione dei compiti e dei poteri dell'Organismo di Vigilanza

La disposizione di cui all'art. 6, comma 1, lett. b) del Decreto stabilisce espressamente che i compiti dell'OdV sono la vigilanza sul funzionamento e sull'osservanza del Modello, nonché la cura del suo aggiornamento.

In particolare, l'OdV dovrà svolgere i seguenti specifici compiti:

a) **vigilare sul funzionamento del Modello e sull'osservanza delle prescrizioni ivi contenute** da parte dei Destinatari, verificando - anche tramite verifiche ispettive effettuate dalle funzioni di controllo interno aziendali o tramite terzi verificatori - la coerenza tra i comportamenti concreti ed

il Modello definito, proponendo l'adozione degli interventi correttivi e l'avvio dei procedimenti disciplinari nei confronti dei soggetti interessati. Più precisamente dovrà:

- verificare l'adeguatezza delle soluzioni organizzative adottate per l'attuazione del Modello (definizione delle clausole standard, formazione degli amministratori e dei procuratori, provvedimenti disciplinari, etc.), avvalendosi delle competenti strutture aziendali e/o di gruppo;
- predisporre il piano periodico delle verifiche sull'adeguatezza e funzionamento del Modello;
- effettuare verifiche periodiche, nell'ambito del piano approvato, sulle attività od operazioni individuate nelle aree a rischio, tramite le funzioni di controllo interne;
- effettuare verifiche mirate su determinate operazioni o su atti specifici e rilevanti posti in essere dalla Società nelle aree di rischio nonché sul sistema dei poteri al fine di garantire la costante efficacia del Modello, anche tramite le funzioni di controllo interne;
- promuovere incontri periodici (con cadenza almeno annuale) con il Collegio Sindacale, la Società di Revisione e l'OdV della Controllante per consentire lo scambio di informazioni rilevanti ai fini della vigilanza sul funzionamento del Modello;
- promuovere idonee iniziative per la diffusione della conoscenza e della comprensione dei principi del Modello e monitorarne l'attuazione;
- disciplinare adeguati meccanismi informativi prevedendo una casella di posta elettronica ed identificando le informazioni che devono essere trasmesse all'OdV o messe a sua disposizione;
- raccogliere, esaminare, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello;
- approfondire le segnalazioni di violazioni del Modello che dovessero arrivare attraverso i canali dedicati;
- segnalare tempestivamente all'organo dirigente (Consiglio di amministrazione), per gli opportuni provvedimenti disciplinari da irrogare con il supporto delle funzioni competenti, le violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo alla Società e proporre le eventuali sanzioni di cui al par. 4 del Modello;
- verificare che le violazioni del Modello siano effettivamente ed adeguatamente sanzionate nel rispetto del sistema sanzionatorio adottato da DGS.

b) **Vigilare sull'opportunità di aggiornamento del Modello**, informando il Consiglio di amministrazione, laddove si riscontrino esigenze di adeguamento in relazione all'ampliamento del novero dei Reati che comportano l'applicazione del Decreto, evidenze di violazione del medesimo da parte dei Destinatari, ovvero significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa. In particolare, l'Organismo di Vigilanza dovrà:

- monitorare l'evoluzione della normativa di riferimento e verificare l'adeguatezza del Modello a tali prescrizioni normative segnalando al Consiglio di amministrazione le possibili aree di intervento;
- predisporre attività idonee a mantenere aggiornata la mappatura delle aree a rischio, secondo le modalità e i principi seguiti nell'adozione del presente Modello;
- vigilare sull'adeguatezza e sull'aggiornamento dei Protocolli rispetto alle esigenze di prevenzione dei Reati e verificare che ogni parte che concorre a realizzare il Modello sia e resti rispondente e adeguata alle finalità del Modello come individuate dalla legge, a tal fine potendosi avvalere delle informazioni e della collaborazione da parte delle strutture aziendali competenti;
- valutare, nel caso di effettiva commissione di Reati e di significative violazioni del Modello, l'opportunità di introdurre modifiche allo stesso;
- presentare al Consiglio di amministrazione le proposte di adeguamento e modifica del Modello. L'adozione di eventuali modifiche è infatti di competenza dell'organo dirigente, il

quale appunto, a mente dell'art. 6 comma 1 lett. a), ha la responsabilità diretta dell'adozione e dell'efficace attuazione del Modello stesso;

- verificare l'effettività e la funzionalità delle modifiche del Modello adottate dal Consiglio di amministrazione.

Nello svolgimento delle proprie attività di vigilanza e controllo l'OdV, senza la necessità di alcuna preventiva autorizzazione:

- avrà libero accesso a tutte le strutture e uffici della Società, potrà interloquire con qualsiasi soggetto operante nelle suddette strutture ed uffici ed accedere ed acquisire liberamente tutte le informazioni, i documenti e i dati che ritiene rilevanti. In caso di diniego motivato da parte dei referenti destinatari delle richieste, l'OdV predisporrà un'apposita relazione da trasmettersi al Consiglio di amministrazione;
- potrà richiedere l'accesso a dati ed informazioni nonché l'esibizione di documenti ai componenti degli organi sociali, alla società di revisione, ai Soggetti Terzi ed in generale a tutti i Destinatari del Modello. Con specifico riferimento ai Soggetti Terzi, l'obbligo ad ottemperare alle richieste dell'OdV deve essere espressamente previsto nei singoli contratti stipulati dalla Società;
- potrà effettuare ispezioni periodiche nelle varie direzioni e funzioni aziendali, anche con riferimento a specifiche operazioni (anche in corso di svolgimento) attuate dalla Società.

Laddove ne ravvisi la necessità, in funzione della specificità degli argomenti trattati, l'OdV può avvalersi del supporto delle strutture aziendali istituzionalmente dotate di competenze tecniche e risorse, umane e operative, idonee a garantire lo svolgimento su base continuativa delle verifiche, delle analisi e degli altri adempimenti necessari ovvero di consulenti esterni.

Ai fini di un pieno e autonomo adempimento dei propri compiti, all'OdV è assegnato un budget annuo adeguato, proposto dall'Organismo stesso e approvato con delibera dal Consiglio di amministrazione, che dovrà consentire all'OdV di poter svolgere i suoi compiti in piena autonomia, senza limitazioni che possano derivare da insufficienza delle risorse finanziarie in sua dotazione. Resta ferma la possibilità per l'OdV di oltrepassare i limiti del budget in caso di necessità, con l'obbligo di fornirne successiva rendicontazione.

Per tutti gli altri aspetti, l'OdV, al fine di preservare la propria autonomia ed imparzialità, provvederà ad autoregolamentarsi attraverso la formalizzazione, nell'ambito di un regolamento, di una serie di norme che ne garantiscano il miglior funzionamento (quali la calendarizzazione dell'attività e dei controlli, la verbalizzazione delle riunioni e la disciplina dei flussi informativi) e disciplinino nel dettaglio le attività di propria competenza. L'OdV trasmetterà, per informazione, copia del regolamento citato al Consiglio di amministrazione della Società.

3.2.3.4 I flussi informativi nei confronti dell'Organismo di Vigilanza

A norma dell'art. 6, comma 2, lettera d), del D.lgs. 231/2001, tra le esigenze cui deve rispondere il Modello è specificata la previsione di "*obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli*".

L'OdV deve essere informato da parte dei Destinatari del Modello in merito ad eventi che potrebbero ingenerare responsabilità ai sensi dal Decreto o che comunque rappresentano infrazioni alle regole societarie. Del pari, all'OdV deve essere trasmesso ogni documento che denunci tali circostanze.

In particolare, al fine di una più efficace e concreta attuazione di quanto previsto nel Modello, i Responsabili delle Differenti Direzioni aziendali, sono tenuti a:

- garantire personalmente e da parte dei Destinatari sottoposti alla loro direzione e vigilanza, il rispetto e l'applicazione dei principi e delle regole di condotta definiti nel Modello;
- supportare l'OdV nell'esercizio dei compiti e delle attività connesse alla responsabilità ad esso attribuite interfacciandosi con il medesimo e assicurando flussi informativi periodici che evidenziano anomalie, eccezioni e deroghe riscontrate nell'ambito delle proprie attività di verifica e controllo.

È stato pertanto istituito un obbligo di informativa verso l'OdV, che si concretizza in flussi informativi periodici e segnalazioni occasionali:

a) **Flussi informativi periodici**: informazioni, dati e notizie circa l'aderenza ai principi di controllo e comportamento sanciti dal Modello e dal Codice Etico di gruppo e trasmesse all'OdV dai Responsabili di Funzione, nei tempi e nei modi che saranno definiti e comunicati dall'OdV medesimo.

   Con cadenza almeno semestrale i Responsabili di Funzione, mediante un processo di autodiagnosi complessivo sull'attività svolta, attestano il livello di attuazione del Modello con particolare attenzione al rispetto dei principi di controllo e comportamento identificati negli specifici Protocolli di competenza.

   Attraverso questa formale attività di autovalutazione, evidenziano le eventuali criticità nei processi gestiti, gli eventuali scostamenti rispetto alle indicazioni dettate dal Modello e/o dai Protocolli, con l'evidenziazione delle azioni e delle iniziative adottate o al piano per la soluzione.

   Sono inoltre previsti flussi di rendicontazione ordinari verso l'Organismo di Vigilanza da parte del Datore di lavoro ai sensi del D.lgs. 81/2008, incentrati su relazioni periodiche in materia di salute e sicurezza sul lavoro.

b) **Segnalazioni occasionali**: informazioni, dati e notizie rilevanti per il rispetto e il funzionamento del Modello e precisamente:
   - i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, fatti comunque salvi gli obblighi di segreto imposti dalla legge, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per gli illeciti per i quali è applicabile il D.lgs. 231/2001, qualora tali indagini coinvolgano la Società o comunque i Destinatari del Modello;
   - i provvedimenti e/o le notizie aventi ad oggetto l'esistenza di procedimenti amministrativi o controversie civili di rilievo, fatti comunque salvi gli obblighi di segreto imposti dalla legge, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, relativi a richieste o iniziative di Autorità indipendenti, dell'amministrazione finanziaria, di amministrazioni locali, ai contratti con la Pubblica Amministrazione, alle richieste e/o gestione di finanziamenti pubblici;
   - le richieste di assistenza legale inoltrate alla Società dal personale in caso di avvio di procedimenti penali o civili nei loro confronti per i Reati di cui al Decreto 231;
   - le notizie relative alle violazioni del Modello con evidenza delle iniziative sanzionatorie assunte ovvero dei provvedimenti di archiviazione dei procedimenti con le relative motivazioni;
   - i rapporti e le relazioni preparati dai responsabili delle varie Direzioni/Funzioni aziendali nonché dalla Società di Revisione da cui emergono o possano emergere carenze nel sistema dei controlli interni, fatti censurabili, osservazioni sul bilancio della Società o comunque comportamenti non conformi alle norme di cui al Decreto 231 e che incidano sull'osservanza del Modello;
   - infortuni gravi (qualsiasi infortunio con prognosi superiore a 40 giorni) occorsi a dipendenti, collaboratori della Società e a tutti coloro che abbiano accesso alle strutture della Società;
   - tutte quelle informazioni, anche se non ritenute critiche, che siano previste dalle singole procedure aziendali e dai protocolli di decisione.

   I Flussi informativi periodici e occasionali potranno essere inviati all'OdV di VISTA TECHNOLOGY:
   - tramite indirizzo di posta elettronica: odv@vistatech.it
   - a mezzo posta tramite raccomandata, all'attenzione di: Organismo di Vigilanza di VISTA TECHNOLOGY, Via Paolo di Dono, 73 - 00142 Roma (RM).

L'Organismo di Vigilanza potrà richiedere, su base periodica o al verificarsi di determinati eventi, dati e informazioni sulle attività svolte (c.d. "informazioni specifiche") a tutti i Destinatari del presente Modello.

c) **Segnalazioni whistleblowing**: informazioni relative alla violazione del D.lgs. 231/2001, del Modello e/o del Codice Etico di gruppo, come previsto dalla recente normativa *ex* Decreto Legislativo n. 24/2023, che recepisce la Direttiva UE 2019/1937 in materia di «Protezione degli individui che segnalano violazioni delle norme comunitarie».

Tale disposto normativo ha previsto l'obbligo per la Società di prevedere dei canali che consentano la segnalazione di illeciti aventi ad oggetto violazioni di disposizioni normative nazionali e/o europee, che ledono gli interessi e/o l'integrità dell'organizzazione di appartenenza, garantendo la massima riservatezza in merito all'identità del segnalante.

Tutti i dipendenti delle Società o terze parti connesse ad essa che vengono a conoscenza di condotte illecite, rilevanti ai sensi del D.lgs. 24/2023, in ragione delle funzioni svolte, devono quindi tempestivamente segnalare tali comportamenti mediante diversi canali di comunicazione.

In considerazione di quanto sopra indicato, la Società ha istituito un sistema di gestione delle segnalazioni (Whistleblowing) che prevede l'utilizzo di una piattaforma al fine di garantire la massima tutela e riservatezza sia delle persone segnalanti che dell'oggetto delle segnalazioni.

In particolare, le segnalazioni inerenti VISTA TECHNOLOGY potranno essere inviate attraverso:

- la piattaforma whistleblowing, accessibile attraverso il seguente link: https://report.whistleb.com/it/dgsspa;
- per iscritto mediante raccomandata, riservata e personale, indirizzata al Ricevente, presso l'indirizzo della Società (Via Paolo di Dono, 73 – 00142 Roma (RM)).

Tutte le eventuali segnalazioni rilevanti ai sensi del Decreto 231 saranno analizzate e veicolate dalla funzione che le ha ricevute all'OdV.

L'OdV valuta le segnalazioni e le informazioni ricevute rilevanti ai sensi del Decreto 231 e le eventuali conseguenti iniziative da attuare, in conformità a quanto previsto dal sistema disciplinare interno, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione, motivando per iscritto l'eventuale decisione e dando luogo a tutti gli accertamenti e le indagini che ritiene necessarie.

Per il dettaglio delle modalità operative di gestione delle segnalazioni si rimanda alla Politica ***PL-10-03*** *Segnalazioni, suggerimenti, reclami (Whistleblowing)*.

La Società non tollera alcuna conseguenza pregiudizievole nei confronti del segnalante in ambito disciplinare, tutelandolo in caso di adozione di «misure discriminatorie, dirette o indirette, aventi effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia». La predetta tutela non trova, quindi, applicazione nei casi in cui la segnalazione riporti informazioni false rese con dolo o colpa grave.

In caso di sospette discriminazioni o ritorsioni nei confronti del Segnalante, correlabili alla segnalazione, o di abusi dello strumento di segnalazione da parte dello stesso, la Società provvederà all'applicazione di sanzioni disciplinari sia nei confronti del Segnalante sia nei confronti dei Segnalati come descritto al capitolo 4 della sezione seconda della presente Parte Generale del Modello, cui si rimanda per maggiori dettagli.

Le segnalazioni di eventuali violazioni del D.lgs. 231 e/o del Modello e/o del Codice Etico di gruppo possono essere segnalate anche direttamente all'Organismo di Vigilanza. In tal caso, le stesse saranno trattate come segnalazioni "ordinarie" e il Segnalante non potrà godere delle tutele previste dal sistema di segnalazione whistleblowing.

Tutte le informazioni, documentazioni, segnalazioni, report, previsti nel presente Modello sono conservati dall'OdV per un periodo di 10 anni; l'OdV avrà cura di mantenere riservati i documenti e le informazioni acquisite, anche nel rispetto della normativa sulla privacy.

L'accesso a tale documentazione è consentito esclusivamente all'OdV.

3.2.3.5 L'attività di reporting dell'Organismo di Vigilanza

Come sopra già precisato, al fine di garantire la sua piena autonomia e indipendenza nello svolgimento delle proprie funzioni, l'Organismo di Vigilanza riporta i risultati della propria attività, in modo continuativo, al Presidente della Società e, periodicamente al Consiglio di amministrazione.

Segnatamente, semestralmente l'OdV trasmette al Consiglio di amministrazione una dettagliata relazione sui seguenti aspetti:

- una descrizione degli eventi significativi rilevanti ai fini del D.lgs. 231/2001;
- l'evoluzione della normativa riguardante il D.lgs. 231/2001;
- lo stato di fatto sull'aggiornamento del Modello;
- le segnalazioni ricevute dall'OdV;
- le evidenze contenute nei flussi informativi ricevuti dall'OdV in merito alle aree di rischio;
- le attività svolte;
- il piano delle attività che intende svolgere per adempiere ai compiti assegnategli;
- i rapporti con gli organi giudiziari rilevanti ai sensi del D.lgs. 231/2001;
- le conclusioni in merito al funzionamento, osservanza ed aggiornamento del Modello.

In caso di gravi anomalie nel funzionamento ed osservanza del Modello o di violazioni di prescrizioni dello stesso, l'OdV riferisce tempestivamente al Consiglio di amministrazione o al Presidente.

L'OdV potrà essere convocato in qualsiasi momento dal Consiglio di amministrazione o potrà, a sua volta, fare richiesta – qualora lo reputi opportuno o comunque ne ravvisi la necessità – di essere sentito da tale organo per riferire su particolari eventi o situazioni relative al funzionamento e al rispetto del Modello sollecitando, se del caso, un intervento da parte dello stesso. Inoltre, l'OdV, se ritenuto necessario ovvero opportuno, potrà chiedere di essere convocato anche dal Collegio Sindacale e dall'OdV della Controllante.

A garanzia di un corretto ed efficace flusso informativo, l'OdV ha inoltre la possibilità, di chiedere chiarimenti o informazioni direttamente al Presidente del CdA ed ai soggetti con le principali responsabilità operative.

Gli incontri con gli organi cui l'OdV riferisce devono essere verbalizzati e copia dei verbali deve essere custodita dall'OdV e dagli organismi di volta in volta coinvolti.

3.2.4 Sistema disciplinare

Ai fini della valutazione dell'efficacia e dell'idoneità del Modello a prevenire i reati indicati dal D.lgs. 231/2001, è opportuno che il Modello individui in via esemplificativa e sanzioni i comportamenti che possono favorire la commissione di reati.

Ciò in quanto l'art. 6, comma 2, D.lgs. 231/2001, nell'elencare gli elementi che si devono rinvenire all'interno dei modelli predisposti dagli Enti, alla lettera e) espressamente prevede che l'Ente ha l'onere di "introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate dal Modello".

Inoltre, in materia di *whistleblowing* si prevede l'integrazione del sistema disciplinare adottato ai sensi dell'art.6 del comma 2, lettera e), con sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

Resta comunque fermo che anche qualora un certo comportamento non sia previsto fra i comportamenti di seguito individuati, laddove risulti in violazione del Modello potrà comunque essere oggetto di sanzione.

3.2.4.1 Le funzioni del sistema disciplinare

La mancata osservanza del Modello, comprensivo di tutte le sue componenti e/o del Codice Etico di gruppo, configura, nel rispetto delle caratteristiche di status giuridico del soggetto nei cui confronti si procede, una violazione dei doveri di diligenza e di fedeltà e, nei casi più gravi, lede il rapporto di fiducia instaurato con la Società. Pertanto, la Società, al fine di indurre i soggetti che agiscono in nome o per conto di VISTA TECHNOLOGY ad operare nel rispetto del Modello, ha quindi istituito un Sistema Disciplinare specifico, volto a punire tutti quei comportamenti che integrino violazioni

delle prescrizioni Modello, attraverso l'applicazione di sanzioni specifiche derivanti da un raccordo tra le previsioni della normativa giuslavoristica ed i principi e le esigenze del Modello.

L'OdV, qualora rilevi nel corso delle sua attività di verifica e controllo una possibile violazione delle prescrizioni del Modello, comprensivo di tutte le sue componenti e/o del Codice Etico di gruppo, darà impulso al procedimento disciplinare, nel rispetto delle caratteristiche di status giuridico del soggetto nei cui confronti si procede, contro l'autore della potenziale infrazione, in misura autonoma rispetto ad eventuali azioni penali dell'autorità giudiziaria a carico dell'autore nonché in relazione a ogni altra eventuale azione che risulti opportuna o necessaria (es. azione risarcitoria).

L'accertamento dell'effettiva responsabilità derivante dalla violazione del Modello e del Codice Etico di gruppo, e l'irrogazione della relativa sanzione, avrà luogo nel rispetto delle disposizioni di legge vigenti, delle norme della contrattazione collettiva applicabile, delle procedure interne, delle disposizioni in materia di privacy e nella piena osservanza dei diritti fondamentali della dignità e della reputazione dei soggetti coinvolti.

L'eventuale irrogazione della sanzione disciplinare dovrà ispirarsi ai principi di tempestività, immediatezza e, per quanto possibile, di equità.

3.2.4.2 I destinatari del sistema disciplinare

Le previsioni del presente Sistema Disciplinare si rivolgono, in particolare, a tutti i Destinatari del Modello ovvero a coloro che rivestono – nell'ambito dell'organizzazione societaria - il ruolo di soggetti "apicali" o di "sottoposti" (secondo la definizione contenuta nell'art. 5 D.lgs. 231/2001) nonché a tutti coloro che – in qualità di Soggetti Terzi – agiscono su mandato o per conto della Società e che abbiano rapporti contrattuali con la Società che per tale motivo sono tenuti a rispettarne i principi generali di comportamento.

In particolare, sono da considerarsi Destinatari del presente Sistema Disciplinare – con le specificità ivi previste - tutti quei soggetti che collaborano a vario titolo con VISTA TECHNOLOGY e, segnatamente:

- i componenti degli organi sociali;
- i lavoratori dipendenti (Dirigenti, quadri, impiegati e operai), legati alla Società da un rapporto di lavoro subordinato, indipendentemente dal CCNL applicato, dalla loro qualifica e/o dal loro inquadramento aziendale riconosciuto;
- i lavoratori parasubordinati (collaboratori, prestatori di lavoro temporaneo, interinali) e i Soggetti Terzi (consulenti, fornitori, partner nonché più in generale tutti coloro che intrattengono rapporti di collaborazione con VISTA TECHNOLOGY per lo svolgimento di qualsiasi prestazione lavorativa).

3.2.4.3 Le condotte rilevanti

Rappresentano condotte oggetto di sanzione i comportamenti posti in essere in violazione del Modello di VISTA TECHNOLOGY, e segnatamente in violazione delle prescrizioni nella Parte Generale, nella Parte speciale e nei Protocolli, nelle Procedure del gruppo DGS ivi richiamate e nel Codice Etico di gruppo.

Costituiscono violazioni del Modello anche le condotte, comprese quelle omissive, attuate in violazione delle indicazioni e/o delle prescrizioni dell'OdV.

Per garantire il rispetto del principio costituzionale di legalità, nonché di quello di proporzionalità della sanzione, appare opportuno indicare di seguito, in via esemplificativa e non esaustiva, un elenco di possibili violazioni secondo un ordine crescente di gravità:

- violazioni connesse, in qualsiasi modo, alle attività indicate come "a rischio 231", violazioni di una o più regole procedurali e/o comportamentali previste nel Modello, configurabili come mancanze lievi, e sempre che non si ricorra in una delle violazioni previste di seguito;
- violazioni connesse, in qualsiasi modo, alle attività a rischio 231 indicate nel Modello, violazioni di una o più regole procedurali e/o comportamentali configurabili come mancanze più gravi se da esse non deriva pregiudizio alla normale attività della Società, violazioni di

cui al punto I se recidivanti, e sempre che non si ricorra in una delle violazioni previste di seguito;

- violazioni idonee a integrare l'elemento oggettivo di uno dei reati suscettibili di fondare, secondo quanto previsto nel Decreto, la responsabilità dell'Ente, violazioni di una o più regole procedurali e/o comportamentali previste nel Modello che determinano un danno patrimoniale alla Società o espongano la stessa a una situazione oggettiva di pericolo all'integrità dei beni aziendali;
- violazioni finalizzate alla commissione di uno dei reati idonei a fondare, secondo quanto previsto dal Decreto, la responsabilità dell'Ente o comunque idonee a ingenerare il pericolo che sia contestata la responsabilità della Società ai sensi del Decreto;
- violazioni di una o più regole procedurali e/o comportamentali previste nel Modello tali da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione del rapporto contrattuale.

3.2.4.4 Le sanzioni

Le sanzioni sono adottate nel rispetto delle normative vigenti in materia e, laddove applicabile, delle norme rinvenibili nella contrattazione collettiva di volta in volta applicabile e dall'art. 7 Legge 300/70 e sono commisurate alla gravità dell'infrazione e all'eventuale reiterazione della stessa.

In ogni caso il tipo e l'entità della sanzione applicata deve tener conto dei principi di proporzionalità e adeguatezza rispetto alla violazione contestata.

In generale avranno rilievo, in via esemplificativa:

- la tipologia dell'illecito compiuto anche in considerazione della gravità dello stesso;
- le circostanze nel cui ambito si è sviluppata la condotta illecita;
- le modalità di commissione della condotta;
- la gravità della condotta;
- l'intenzionalità del comportamento o del grado di negligenza, imprudenza o imperizia anche con riguardo alla prevedibilità dell'evento;
- il comportamento complessivo del destinatario con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- il ruolo rivestito dal destinatario;
- la posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- altre particolari circostanze che accompagnano l'illecito disciplinare quali ad esempio l'eventuale commissione di più violazioni nell'ambito della medesima condotta, nel qual caso l'aggravamento sarà operato nel rispetto della sanzione prevista per la violazione più grave;
- il comportamento immediatamente susseguente al fatto;
- le circostanze aggravanti (o attenuanti) nel cui ambito si è sviluppata la condotta illecita, con particolare riguardo alla professionalità, alle precedenti prestazioni lavorative e/o ai precedenti rapporti contrattuali, ai precedenti disciplinari, alle circostanze in cui è stato commesso il fatto;
- l'eventuale concorso di più soggetti nella commissione della violazione;
- l'eventuale recidiva del suo autore.

L'applicazione delle sanzioni disciplinari non pregiudica in alcun modo il diritto della Società di agire nei confronti del soggetto responsabile al fine di ottenere il risarcimento di tutti i danni patiti a causa o in conseguenza della condotta accertata.

3.2.4.4.1 Misure nei confronti del personale non dirigente

Le violazioni delle regole comportamentali previste dal Modello e dai suoi Allegati commesse dai lavoratori dipendenti costituiscono inadempimento contrattuale e pertanto potranno comportare

l'adozione di sanzioni disciplinari, nei limiti stabiliti dal contratto collettivo applicabile al rapporto di lavoro.

In particolare, il C.C.N.L. per gli Addetti del Settore Metalmeccanico ("CCNL"), che disciplina il rapporto di lavoro tra VISTA TECHNOLOGY ed i suoi dipendenti, stabilisce all'articolo 8 del Titolo Settimo – Rapporti in Azienda l'applicazione dei seguenti provvedimenti disciplinari a fronte di inadempimenti contrattuali:

a) richiamo verbale;
b) ammonizione scritta;
c) multa non superiore a tre ore di retribuzione oraria calcolata sul minimo tabellare;
d) sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni;
e) licenziamento per mancanze ai sensi dell'art. 10.

Restano ferme, e si intendono qui richiamate, tutte le disposizioni di cui all'art. 7 della legge 20 maggio 1970, n. 300 (c.d. "Statuto dei Lavoratori") in relazione sia all'esposizione del codice disciplinare ed all'obbligo di preventiva contestazione dell'addebito al Dipendente, anche al fine di consentire allo stesso di approntare una idonea difesa e di fornire eventuali giustificazioni.

Le sanzioni disciplinari previste ai punti (a) e (b) sono comminate ai lavoratori Dipendenti che, per negligenza, violano le regole, i principi e le procedure previste dal Modello e dai suoi allegati o adottano comportamenti non conformi allo stesso o non adeguati, ma comunque tali da non minare l'efficacia del Modello stesso. Tali sanzioni disciplinari sono inoltre previste nel caso in cui i Dipendenti non rispettino gli obblighi previsti in materia di whistleblowing.

Più precisamente:

- la sanzione del richiamo verbale può essere attuata in caso di lieve inosservanza dei principi e delle procedure previste dal Modello e dal Codice Etico di gruppo dovuti a negligenza del Dipendente. A titolo esemplificativo e non esaustivo, è punibile con il rimprovero verbale il Dipendente che, per negligenza, trascuri di conservare in maniera accurata la documentazione di supporto necessaria per ricostruire l'operatività della Società nelle aree a rischio. Il richiamo verbale è inoltre previsto, nei casi in cui si verifichi un'inosservanza degli obblighi in materia di whistleblowing, ad esempio, nel caso in cui un Dipendente, effettui segnalazioni che si rivelano false e prive di fondamento nei confronti di un altro soggetto.
- la sanzione dell'ammonizione scritta viene adottata in ipotesi di ripetute mancanze punite con il richiamo verbale, o in caso di violazione colposa dei principi e dalle procedure previste dal Modello e Codice Etico di gruppo, attraverso un comportamento non conforme o non adeguato: ad esempio in caso di ritardata segnalazione all'OdV delle informazioni dovute ai sensi del Modello. Tale sanzione viene applicata anche nei casi in cui si verifichino una reiterata inosservanza colposa della normativa in materia di whistleblowing, ad esempio nel caso in cui il Dipendente effettui più segnalazioni che si rivelano false e prive di fondamento nei confronti di un altro soggetto, o qualora un Dipendente tenti di violare le norme in materia di tutela del segnalante.

Le sanzioni disciplinari di cui ai punti (c) e (d) sono comminate ai lavoratori dipendenti in caso di reiterate violazioni di cui ai precedenti punti o in caso di comportamenti colposi e/o negligenti posti in essere dal personale dipendente che opera in aree a rischio 231, che possono minare anche potenzialmente l'efficacia del Modello e del Codice Etico di gruppo.

E così in via esemplificativa:

- la multa non superiore a tre ore di retribuzione oraria calcolata sul minimo tabellare può essere applicata nel caso di inosservanza dei principi e delle regole di comportamento previste dal presente Modello, per un comportamento non conforme o non adeguato alle prescrizioni del Modello in misura tale da essere considerata di una certa gravità.

  A titolo esemplificativo e non esaustivo, tra tali comportamenti rientra la violazione degli obblighi di informazione nei confronti dell'OdV in ordine alla commissione dei Reati, ancorché

tentati, ovvero la mancata reiterata partecipazione, senza giustificato motivo alle sessioni formative che nel tempo verranno erogate dalla Società relative al D. Lgs. 231/2001, al Modello di organizzazione, gestione e controllo e del Codice Etico di gruppo adottato dalla Società o in ordine a tematiche relative. Tale sanzione è anche comminata nel caso in cui il Dipendente effettui, all'interno dell'ambito lavorativo e con colpa grave, una segnalazione di illecito nei confronti di un altro soggetto, qualora questa si riveli successivamente falsa ed infondata.

- la sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni sarà applicata in caso di gravi violazioni procedurali tali da esporre la Società a responsabilità nei confronti di terzi. A titolo esemplificativo e non esaustivo: l'inosservanza delle prescrizioni del Codice Etico di gruppo; l'omissione o il rilascio di false dichiarazioni relative al rispetto del Modello; l'inosservanza delle disposizioni dei poteri di firma e del sistema delle deleghe; l'omissione della vigilanza sul comportamento del personale operante all'interno della propria sfera di responsabilità al fine di verificare le loro azioni nelle aree di rischio; ogni e qualsiasi altra inosservanza contrattuale o di specifica disposizione comunicata al Dipendente. Inoltre, in materia di whistleblowing, tale sanzione è prevista, nei casi in cui un Dipendente effettui, all' interno dell'ambito lavorativo e con dolo, una segnalazione di illecito nei confronti di un altro soggetto che successivamente si riveli falsa ed infondata, o ancora nei casi in cui un Dipendente violi le misure volte alla tutela del segnalante illeciti (qualora lo stesso non sia coinvolto nel processo di valutazione della segnalazione).

Le sanzioni disciplinari di cui al punto e) sono inflitte al Dipendente che attui, nell'espletamento delle sue attività, un comportamento non conforme alle prescrizioni del Modello e diretto in modo univoco al compimento di un reato sanzionato dal Decreto e tale da poter determinare l'applicazione a carico della Società delle sanzioni amministrative derivanti da reato previste dal Decreto.

Più precisamente, il licenziamento per mancanze ai sensi dell'art. 10 è una sanzione inflitta in conseguenza di una mancanza così grave (per la dolosità del fatto, o per i riflessi penali o pecuniari o per la sua recidività) da non consentire la prosecuzione, anche provvisoria del rapporto di lavoro. Tra le violazioni passibili della predetta sanzione: comportamento fraudolento inequivocabilmente diretto alla commissione di uno dei Reati previsti dal Decreto tale da far venir meno il rapporto fiduciario con il datore di lavoro; redazione di documentazione incompleta o non veritiera dolosamente diretta ad impedire la trasparenza e verificabilità dell'attività svolta; violazione dolosa di procedure aventi rilevanza esterna; omessa redazione della documentazione prevista dal Modello; violazione o elusione dolosa del sistema di controllo previsto dal Modello in qualsiasi modo effettuata, incluse la sottrazione, distruzione o alterazione della documentazione inerente alla procedura, l'ostacolo ai controlli, l'impedimento di accesso alle informazioni e alla documentazione da parte dei soggetti preposti ai controlli o alle decisioni. Inoltre, in materia di whistleblowing, tale sanzione è prevista, ad esempio, nei casi in cui un dipendente effettui in maniera reiterata, all' interno dell'ambito lavorativo e con dolo, una segnalazione di illecito nei confronti di un altro soggetto che successivamente si riveli falsa ed infondata, o ancora nei casi in cui un dipendente violi ripetutamente gli obblighi di riservatezza di cui al decreto legislativo n. 24 del 2023 art.12

Alla notizia di violazione delle regole di comportamento del Modello da parte di un dipendente non dirigente, l'OdV informa la Funzione Human Resources per l'adozione delle opportune iniziative.

3.2.4.4.2 Misure nei confronti del personale dirigente

Con riguardo ai dirigenti, nei casi di violazione delle regole del presente Modello e in ragione della gravità di dette violazioni, si applicano le sanzioni più idonee conformemente a quanto previsto per legge e dalla contrattazione collettiva applicabile, sino alla misura del licenziamento, nel caso in cui venga meno il rapporto di fiducia.

Talune sanzioni disciplinari, in base alla gravosità dell'atto compiuto, sono inoltre previste nel caso in cui i dipendenti non rispettino gli obblighi previsti in materia di Whistleblowing, ad esempio, nei casi in cui un dipendente effettui, all'interno dell'ambito lavorativo e con dolo, una segnalazione di illecito nei confronti di un altro soggetto che successivamente si riveli falsa ed infondata.

L'esistenza di un sistema sanzionatorio connesso al mancato rispetto delle disposizioni contenute nel Modello, e nella documentazione che di esso forma parte, deve essere necessariamente portato a conoscenza del personale dipendente attraverso i mezzi ritenuti più idonei dalla Società.

3.2.4.4.3 Misure nei confronti degli amministratori

Con riguardo ai membri del Consiglio di Amministrazione, nel caso di violazioni delle prescrizioni contenute nel presente Modello, l'Organismo di Vigilanza informa l'intero Consiglio di Amministrazione, che procederà ai sensi di legge ad assumere le iniziative più opportune e adeguate in relazione alla gravità della violazione rilevata e conformemente ai poteri previsti dalla vigente normativa e dallo Statuto sociale, coinvolgendo, ove necessario, il Socio Unico.

3.2.4.4.4 Misure nei confronti dei Soggetti Terzi

I Soggetti Terzi quali, fornitori, consulenti, business partner sono destinatari del Modello e del Codice Etico di gruppo. Nei contratti stipulati dalla con detti Soggetti Terzi sono contenute apposite dichiarazioni di conoscenza dei contenuti del Modello, del Codice Etico di gruppo e dell'obbligo di attenervisi.

I contratti con tali soggetti contengono una specifica clausola di recesso e/o di risoluzione connesse all'inadempimento di tali obbligazioni, fermo restando il diritto della Società di rivalersi per gli eventuali danni verificatisi in conseguenza di dette condotte, ivi inclusi i danni causati dall'applicazione da parte del giudice delle misure previste dal Decreto.

3.2.5 Diffusione del Modello

Il regime della responsabilità amministrativa previsto dalla normativa di legge e l'adozione del Modello di organizzazione, gestione e controllo da parte di VISTA TECHNOLOGY formano un sistema che deve trovare nei comportamenti operativi dei destinatari una coerente ed efficace risposta.

Al riguardo è fondamentale un'attività di **comunicazione** e di **formazione** finalizzata a favorire la diffusione di quanto stabilito dal Decreto e dal Modello organizzativo adottato nelle sue diverse componenti, affinché la conoscenza della materia e il rispetto delle regole che dalla stessa discendono costituiscano parte integrante della cultura professionale di ciascun dipendente e collaboratore.

VISTA TECHNOLOGY ha quindi strutturato un piano di comunicazione interna, informazione e formazione rivolto a tutti i dipendenti aziendali ma diversificato a seconda dei destinatari cui si rivolge, che ha l'obiettivo di creare una conoscenza diffusa e una cultura aziendale adeguata alle tematiche in questione, mitigando così il rischio della commissione di illeciti.

Il piano è gestito dalle competenti funzioni aziendali, in coordinamento con l'Organismo di Vigilanza.

In particolare, per ciò che concerne la **comunicazione** si prevede:

- una comunicazione iniziale da parte del Presidente della Società a tutti i Dipendenti circa l'adozione del Modello;
- la pubblicazione del Modello e dei suoi Protocolli sulla intranet aziendale;
- la pubblicazione del Codice Etico di gruppo sulla intranet e sul sito internet aziendali;
- la pubblicazione della Parte Generale del Modello e del Codice sul sito internet aziendale;
- idonei strumenti di comunicazione saranno adottati per aggiornare i destinatari circa le eventuali modifiche al Modello e/o al Codice Etico di gruppo.

Relativamente ai meccanismi di **informazione**, si prevede che:

- i neoassunti ricevono, all'atto dell'assunzione, unitamente alla prevista restante documentazione, copia del Modello e del Codice Etico di gruppo di cui si chiede conoscenza e rispetto;
- siano fornite ai Soggetti Terzi, apposite informative sui principi e sulle politiche adottate da VISTA TECHNOLOGY - sulla base del presente Modello e del Codice Etico di gruppo -

nonché sulle conseguenze che comportamenti contrari alla normativa vigente ovvero ai principi etici adottati possano avere con riguardo ai rapporti contrattuali, al fine di sensibilizzarli all'esigenza della Società a che il loro comportamento sia conforme alla legge, con particolare riferimento a quanto disposto dal D.Lgs. 231/2001.

Per quanto infine concerne la **formazione**, sono previste attività formative periodiche e obbligatorie avente l'obiettivo di far conoscere a tutti i Dipendenti della Società i contenuti del Decreto, del Modello e del Codice Etico di gruppo, i poteri e i compiti dell'Organismo di Vigilanza nonché a sensibilizzare i Dipendenti sull'importanza dell'attuazione effettiva e concreta del Modello e a favorire il loro ruolo propulsivo e collaborativo nella diffusione e aggiornamento dello stesso.

Il piano di formazione, costruito e gestito dalla Funzione Human Resources della Capogruppo, in coordinamento con l'OdV e tiene in considerazione molteplici variabili, in particolare:

- i *target* (i destinatari degli interventi, il loro livello e ruolo organizzativo),
- i contenuti (gli argomenti attinenti al ruolo delle persone);
- gli strumenti di erogazione (aula, *e-learning*).

La partecipazione alle citate attività di formazione da parte di tutto il personale interessato è obbligatoria ed è monitorata dalla Funzione Human Resources della Capogruppo e dall'OdV.

È prevista la formalizzazione della partecipazione ai momenti formativi attraverso la richiesta della firma di presenza.

3.2.6 Aggiornamento del Modello

L'attività di aggiornamento, intesa sia come integrazione sia come modifica, è volta a garantire l'adeguatezza e l'idoneità del Modello, valutate rispetto alla funzione preventiva di commissione dei Reati indicati dal D.lgs. 231/2001.

Il Modello è adottato dal Consiglio di amministrazione della Società nella cui competenza rientrano le modifiche ed integrazioni dello stesso che si rendessero opportune o necessarie, in relazione a:

- significative violazioni delle prescrizioni del Modello adottato;
- modifiche normative che comportano l'estensione della responsabilità amministrativa degli enti ad altre tipologie di reato per le quali si reputi sussistente un rischio di commissione nell'interesse o a vantaggio della Società;
- significative modifiche intervenute nella struttura organizzativa, nel sistema dei poteri e nelle modalità operative di svolgimento delle attività a rischio e dei controlli a presidio delle stesse.

Le proposte di modifica ed integrazione del Modello e dei suoi allegati potranno essere presentate dall'Organismo di Vigilanza al Consiglio di amministrazione, sentite le competenti funzioni aziendali.

Al fine di apportare al Modello tutte quelle modifiche formali e non sostanziali che potranno rendersi necessarie nel tempo, è facoltà del Consiglio di amministrazione della Società, nella sua autonomia decisionale, attribuire ad uno dei suoi membri il potere di apportare le citate modifiche con obbligo per il Presidente di comunicare formalmente al Consiglio di amministrazione le modifiche apportate.

3.2.7 Modalità di nomina del difensore di fiducia dell'Ente

Come previsto dall'art.39 del Decreto, l'Ente partecipa al procedimento penale, instaurato nei suoi confronti, per mezzo del proprio rappresentante legale, salvo che questi sia imputato per il reato da cui dipende la responsabilità amministrativa dell'Ente stesso. Il Decreto individua una condizione di insanabile conflitto di interessi nel caso in cui l'Ente - nel procedimento penale - sia rappresentato dal rappresentante legale che, essendo imputato della commissione del reato presupposto, ha "dato causa" alla contestazione mossa nei confronti dell'Ente.

Per tale ragione, la giurisprudenza è costante nel ritenere che - stante la suddetta condizione di incompatibilità - il legale rappresentante dell'Ente, imputato per il reato presupposto, oltre a non poter rappresentare l'Ente in giudizio, non possa provvedere neanche alla nomina del difensore di

fiducia con cui l'Ente si costituirà nel procedimento. La nomina del difensore di fiducia dell'Ente effettuata dal legale rappresentante che versi in condizioni di conflitto di interessi è ritenuta invalida: ciò potrebbe rappresentare un grave pregiudizio per la tutela della posizione dell'Ente tanto nell'ambito del processo, quanto - in fase di indagini preliminari - soprattutto in relazione all'applicazione di eventuali misure cautelari di natura interdittiva o patrimoniale.

Per ovviare a tali condizioni, conformemente agli orientamenti giurisprudenziali attualmente maggioritari, la Società ha previsto delle regole cautelari interne tali per cui - anche laddove il legale rappresentante sia imputato per il reato presupposto - la nomina del difensore di fiducia dell'Ente può essere validamente effettuata da un altro soggetto, dotato dei relativi poteri per effetto di apposita procura, evitando possibili condizioni di conflitto di interessi.

4 Parte Speciale

4.1 Introduzione

La Parte Speciale del Modello ha lo scopo di definire le regole di organizzazione, gestione e controllo che devono guidare la Società e tutti i Destinatari del Modello nello svolgimento delle attività nell'ambito delle quali possono essere commessi i Reati presupposto del D.lgs. 231/2001.

Al fine di prevenire o di mitigare il rischio di commissione dei reati previsti dal D.lgs. 231/2001, la Società, oltre ad aver adottato un Codice Etico di gruppo, ha definito Protocolli specifici di prevenzione per ciascuna delle aree a rischio 231.

Con riferimento a ciascuna di dette aree a rischio sono stati individuati i profili di rischio di commissione delle specifiche fattispecie di reato presupposto, individuati i soggetti a vario titolo coinvolti nella realizzazione delle attività, formulati principi di comportamento e di controllo per presidiare i rischi in oggetto ed individuate le modalità che devono essere osservate dai Destinatari del Modello per garantire un costante flusso informativo verso l'Organismo di Vigilanza, affinché lo stesso possa efficacemente ed efficientemente svolgere la propria attività di controllo.

I principi su cui la Società si è basata nella redazione dei protocolli sono i seguenti:

- attribuzione formale delle responsabilità;
- poteri di firma e poteri autorizzativi interni devono essere assegnati sulla base di regole formalizzate, in coerenza con le responsabilità organizzative e gestionali e con una chiara indicazione dei limiti di spesa;
- separazione di compiti e funzioni: non deve esserci identità di soggetti tra chi autorizza l'operazione, chi la effettua e ne dà rendiconto e chi la controlla;
- tracciabilità: deve essere ricostruibile la formazione degli atti e le fonti informative/documentali utilizzate a supporto dell'attività svolta, a garanzia della trasparenza delle scelte effettuate; ogni operazione deve essere documentata in tutte le fasi di modo che sia sempre possibile l'attività di verifica e controllo. L'attività di verifica e controllo deve a sua volta essere documentata attraverso la redazione di verbali;
- archiviazione/tenuta dei documenti: i documenti riguardanti le attività dell'area a rischio 231 devono essere archiviati e conservati, a cura del Responsabile della Direzione/Funzione interessata o del soggetto da questi delegato, con modalità tali da non consentire l'accesso a terzi che non siano espressamente autorizzati. I documenti approvati ufficialmente dagli organi sociali e dai soggetti autorizzati a rappresentare la Società verso i terzi non possono essere modificati, se non nei casi eventualmente indicati dalle procedure e comunque in modo che risulti sempre traccia dell'avvenuta modifica.

Nell'ambito di ciascun Protocollo si rilevano:

- presupposti e obiettivi del documento
  - Obiettivo del Protocollo
  - Destinatari del Protocollo
  - Campo di applicazione e attività relative alle aree a rischio 231

    - Riferimenti
    - Fattispecie di reato
- principi di comportamento
- principi di controllo
- reporting all'Organismo di Vigilanza.

Per ciascun Protocollo di decisione deve essere individuato un responsabile che garantisca il rispetto e l'applicazione delle regole di condotta e dei controlli definiti nel documento, ne curi l'aggiornamento e informi l'Organismo di Vigilanza di fatti o circostanze significative riscontrate nell'esercizio delle attività a rischio di sua pertinenza, in conformità con quanto previsto nella Parte Generale. Tale soggetto, generalmente, coincide con il responsabile della Direzione/Funzione all'interno della quale si svolgono le attività di cui all'area a rischio 231 o, comunque, una parte significativa di queste.

FINE DEL DOCUMENTO