MODELLO DI ORGANIZZAZIONE E GESTIONE

PARTE GENERALE

Sintax S.r.l. - Società Unipersonale soggetta a Direzione e Coordinamento da parte di PA Digitale S.p.A.

SEDE LEGALE: Via Giuseppe Verdi 9, 87036 Rende (CS)

Approvato dal Consiglio di Amministrazione il 12 Ottobre 2023

SOMMARIO

INTRODUZIONE

Premessa

SINTAX, società a responsabilità limitata, è una software house costituita nel 2000 come spin-off del reparto informatico di una società operante nel settore dei servizi tributari.

Da allora SINTAX si è focalizzata sullo sviluppo di servizi e tecnologie per la Fiscalità Locale puntando su creatività, passione qualità e competenza per dare vita a soluzioni software e servizi sempre più innovativi e avanzati.

Ad oggi in azienda opera un team di professionisti, quasi tutti laureati e con un elevato livello di specializzazione nel settore, sia con molteplici e pluriennali esperienze nell'analisi e realizzazione di sistemi informativi aziendali dedicati alla riscossione dei tributi locali, sia nell'erogazione di servizi professionali e post-vendita.

La ricerca e l'utilizzo di tecnologie sempre più all'avanguardia, unitamente alla costante valutazione del mutamento delle esigenze dei propri clienti, ha portato nel tempo SINTAX a divenire società leader nella progettazione e conduzione di soluzioni informatiche specialistiche proprietarie applicate alla fiscalità locale che sono esercite sia in modalità hosting che SaaS.

Al core business dell'outsourcing della piattaforma IT proprietaria si è abbinata nel tempo una crescente offerta di attività di servizi professionali EDP a supporto dei propri clienti.

Le caratteristiche intrinseche della missione di SINTAX ed il contesto di mercato in cui opera, caratterizzato nei rapporti con clienti pubblici e privati dalla necessità di accesso diretto a informazioni tributarie relative ai cittadini, implicano un elevata attenzione alla prevenzione proattiva di qualsiasi fenomeno di illegalità, istituendo una governance aziendale che adotti appropriati controlli sulle aree e attività aziendali comportanti rischio di attività illecite.

A tal fine SINTAX ha aderito ad un Modello di Organizzazione Gestione e Controllo (di seguito MOG) ai sensi del decreto legislativo 8 giugno 2001 n. 231 "Disciplina della Responsabilità amministrativa degli enti" (di seguito, il "D. Lgs. 231/2001") al fine perseguire le finalità di: promuovere in misura sempre maggiore una cultura aziendale orientata all'eticità, correttezza e trasparenza delle attività; adeguarsi alla normativa sulla responsabilità amministrativa degli enti, verificando e valorizzando i presidi già in essere, atti a prevenire la realizzazione di condotte illecite.

Struttura del Documento e Definizioni

Nella stesura del MOG, SINTAX si è ispirata alle Linee Guida emanate da Confindustria e approvate dal Ministero della Giustizia. In particolare, seguendo i seguenti principi fondamentali:

- l'individuazione delle aree di rischio (attività sensibili), ove sia possibile il verificarsi dei reati previsti dal D. Lgs. 231/2001;
- la mappatura dei processi e sub processi coinvolti dalle attività sensibili (area/settore aziendale/processo)
- la definizione di protocolli generali per l'attuazione delle decisioni atti a stabilire meccanismi di prevenzione e controllo di rischi di avvenimento dei reati previsi dal D. Lgs. 231/2001;
- l'individuazione delle macro-componenti più rilevanti che caratterizzano l'attuazione dei protocolli e l'istituzione efficace di un Sistema di Controllo preventivo quali:
    - l'adozione di un Codice etico;
    - il sistema organizzativo ed i relativi poteri autorizzativi e di firma;
    - la Governance del Sistema di Gestione Aziendale ispirato alle norme ISO;
    - il controllo di gestione;
    - la comunicazione al personale e sua formazione;

  - l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel MOG;
  - La costituzione di un Organismo di Vigilanza con individuazione dei poteri e delle modalità di funzionamento dello stesso;
- l'individuazione dei principi generali di controllo applicabili quali:
  - la verificabilità, documentazione, coerenza e congruenza di ogni operazione;
  - l'applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo);
  - la documentazione dei controlli;
  - la previsione di un adeguato sistema sanzionatorio per la violazione delle norme interne e delle procedure previste dal MOG;
  - la nomina di una funzione interna di Assurance & Compliance avente il compito di vigilare sull'applicazione del MOG.
  - il soddisfacimento degli obblighi di informazione da e verso l'Organismo di Vigilanza.

Nel documento sono utilizzate le seguenti definizioni

Attività sensibili	Singole attività primarie o strumentali, che presentano rischi (astratti) di commissione di uno dei reati che presuppone la responsabilità amministrativa della Società ai sensi del D.Lgs 231/01.
Personale	Contratti di lavoro di qualsiasi tipologia e natura, inclusi quelli che riguardano i dirigenti, il personale a progetto, part-time, gli interinali, gli stage e i contratti di collaborazione rientranti nella para-subordinazione
Collaboratori	Coloro che, in forza di un contratto o di un mandato, agiscono in nome e per conto della società (consulenti, intermediari, procuratori speciali).
Parti Terze	Coloro che intrattengono relazioni commerciali con la Società, quali fornitori, clienti, partner, investitori, e i beneficiari di iniziative sociali, donazioni e sponsorizzazioni
P.A.	La Pubblica Amministrazione e, con riferimento ai reati nei confronti della pubblica amministrazione, i pubblici ufficiali e gli incaricati di un pubblico servizio a norma degli artt. 357, 358 c.p.
Destinatari	Sono i soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione all'interno della Società, le persone che esercitano, anche di fatto, la gestione e il controllo, nonché le persone sottoposte alla direzione o alla vigilanza di uno dei predetti soggetti (ai sensi dell'art. 5 del D.Lgs. 231/2001). A titolo esemplificativo, sono Destinatari i componenti degli organi Sociali e tutto il personale quando svolgono attività per la Società. Allo stesso modo, sono Destinatari i consulenti e le parti terze che operano nell'ambito delle Attività Sensibili in nome o per conto della Società.
Controllo Preventivo	Attività di verifica sistematica sulle attività sensibili aziendali idonee a mitigare, rendendolo accettabile, il rischio di accadimenti di reati sia di natura colposa che dolosa.
Accettabilità del rischio del reato doloso	Solidità del sistema di prevenzione del rischio reato tale da non poter essere aggirata se non attraverso "elusione fraudolenta" del modello organizzativo intesa come esimente dal D. Lgs 231/2001 ai fini dell'esclusione della responsabilità amministrativa dell'ente (art. 6, comma 1, lett. c).

Organismo di vigilanza	l'organismo esterno di controllo, preposto alla vigilanza sul funzionamento e sull'osservanza del Modello, nonché al relativo aggiornamento, ai sensi dell'art. 6 del D.Lgs. 231/2001.

Destinatari del MOG

Le regole e le disposizioni contenute nel MOG si applicano e devono essere rispettate da coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo della Società, dai dipendenti, nonché da coloro i quali, pur non appartenendo alla Società, operano su mandato della medesima.

Sono quindi "Destinatari" del presente MOG:

- i titolari di qualifiche formali (di direzione, gestione e controllo della Società o di una sua unità organizzativa) riconducibili alla definizione di "soggetti apicali";
- i soggetti che esercitano tali funzioni (di direzione, gestione e controllo) anche solo di fatto;
- tutto il personale della Società, in forza di qualsiasi tipo di rapporto contrattuale (compresi stagisti, collaboratori legati da contratti a termine e collaboratori a progetto);
- i membri degli organi di controllo sia interni che esterni;
- chiunque agisca in nome e per conto della Società a prescindere dal vincolo di subordinazione.

Ai collaboratori esterni, consulenti, fornitori, partner commerciali e altre controparti contrattuali in genere, la Società richiede il rispetto delle prescrizioni dettate dal Decreto e dei principi etici adottati dalla Società, tramite, laddove necessario, la sottoscrizione di specifiche clausole contrattuali che assicurino l'impegno al rispetto delle norme di cui al D. Lgs. 231/2001, dei principi etici e delle linee di condotta adottati dalla Società.

DISPOSIZIONI GENERALI

Il Decreto Legislativo n 231/2001

Il D. Lgs. 231/2001, emanato in attuazione della delega conferita al Governo con l'art. 11 della Legge 29 settembre 2000, n. 300, disciplina la "responsabilità degli enti per gli illeciti amministrativi dipendenti da reato".

La disciplina si applica agli enti dotati di personalità giuridica, nonché alle società e associazioni anche prive di personalità giuridica.

Il D. Lgs. 231/2001 trova la sua genesi in alcune convenzioni internazionali e comunitarie ratificate dall'Italia che impongono di prevedere forme di responsabilità degli enti collettivi per talune fattispecie di reato.

Secondo la disciplina introdotta dal D. Lgs. 231/2001 un ente/società può essere ritenuto "responsabile" per alcuni reati commessi o tentati, nell'interesse o a vantaggio della società stessa, da (Art 5):

- soggetti apicali, ossia coloro i quali rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente/società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché coloro che esercitano, anche di fatto, la gestione e il controllo delle stesse;
- soggetti sottoposti alla direzione o alla vigilanza di soggetti apicali.

Per quanto attiene alla nozione di "interesse", esso si concretizza ogni qualvolta la condotta illecita sia posta in essere con l'esclusivo intento di conseguire un beneficio all'ente/società, indipendentemente dalla circostanza che tale obiettivo sia stato conseguito.

Del pari la responsabilità incombe sull'ente/società ogniqualvolta l'autore dell'illecito, pur non avendo agito al fine di beneficiare l'ente, abbia comunque fatto conseguire un "vantaggio" alla persona giuridica, di tipo economico o meno.

La responsabilità amministrativa dell'ente/società è autonoma rispetto alla responsabilità penale della persona fisica che ha commesso il reato e si affianca a quest'ultima.

L'art. 6, comma 2, del D. Lgs 231/2001 indica le caratteristiche essenziali per la costruzione di un modello di organizzazione, gestione e controllo. In particolare, le lettere a) e b) della disposizione si riferiscono espressamente ad alcune attività correlate ad un processo di sana e prudente gestione dei rischi di avverarsi di reati sia di natura dolosa che colposa.

Un concetto nodale nella costruzione di un sistema di controllo preventivo è quello di "**rischio accettabile**".

Nel caso dei reati di natura dolosa la soglia concettuale di accettabilità è rappresentata da un: sistema di prevenzione tale da non poter essere aggirato se non attraverso "**elusione fraudolenta**" del modello organizzativo intesa come esimente dal D. Lgs 231/2001 ai fini dell'esclusione della responsabilità amministrativa dell'ente (art. 6, comma 1, lett. c).

Un "elusione fraudolenta" presuppone, dunque, che la violazione del soggetto sia determinata comunque da un aggiramento delle "misure di sicurezza", idoneo a forzarne l'efficacia.

Diverso il caso di reati di natura colposa, che si differenziano da quelli dolosi nel caso in cui, pur essendoci la volontà dell'atto, il soggetto non ha voluto che si verificasse un determinato evento, ovvero l'evento si verifica a causa di imperizia, negligenza ecc., per cui si parlerà di "colpa".

In tal caso la soglia concettuale di accettabilità, che abbia effetti esimenti ai sensi del D. Lgs 231/2001, va diversamente modulata in relazione ai reati di omicidio colposo e lesioni personali colpose commessi con violazione delle norme in materia di salute e sicurezza sul lavoro, nonché ai reati ambientali punibili per colpa.

L'elusione fraudolenta dei modelli organizzativi, infatti, appare incompatibile con l'elemento soggettivo dei reati colposi, in cui manca la volontà dell'evento lesivo della integrità fisica dei lavoratori o dell'ambiente.

In queste ipotesi la soglia di rischio accettabile è rappresentata quindi dalla realizzazione di una condotta in violazione del modello organizzativo di prevenzione (caso, ad esempio, dei reati commessi in violazione degli adempimenti obbligatori prescritti dalle norme prevenzionistiche in materia di salute e sicurezza), nonostante la puntuale osservanza degli obblighi di vigilanza previsti dal D. Lgs 231/2001 da parte dell'Organismo di Vigilanza.

Il Modello di Organizzazione, Gestione e Controllo

Il D. Lgs 231/2021, prevede una forma specifica di esonero da responsabilità qualora la Società dimostri di aver adottato tutte le misure organizzative necessarie al fine di prevenire la commissione di reati da parte di soggetti che operino per suo conto. La presenza di un'adeguata organizzazione è, dunque, misura e segno della diligenza della Società nello svolgere le proprie attività, con particolare riferimento a quelle in cui si manifesta il rischio di commissione dei reati previsti dal Decreto: l'accertata esistenza di un'efficiente ed efficace organizzazione esclude, dunque, la "colpa" della Società e fa venir meno la necessità di applicare ad esso le previste sanzioni.

In caso di reato commesso da un soggetto in posizione apicale, infatti, la Società non risponde se prova che (art. 6):

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

Il Modello di Organizzazione, Gestione e Controllo adottato da SINTAX ai sensi del D. Lgs. 231/2001 (di seguito anche "MOG") si compone di:

- **Codice Etico** [ALL 1] che definisce l'insieme dei principi e delle regole di condotta fondamentali a cui SINTAX si attiene. Tali principi e regole, con l'ulteriore orientamento fornito da altre Politiche di Qualità, Trasparenza, Legalità e Sostenibilità [ALL 2] e [ALL 3], adottate e periodicamente aggiornate, guidano il progetto di impresa contribuendo alla creazione di valore condiviso nel lungo periodo;
- **Parte Generale** (il presente documento), che partendo dalla descrizione dei contenuti del D. Lgs. 231/2001, illustra sinteticamente i modelli di governo societario e di organizzazione e gestione della Società, la funzione ed i principi generali di funzionamento del Modello nonché i meccanismi di concreta attuazione dello stesso;
- **Parte Speciale**, sviluppata a seguito di una fase di analisi di accettabilità del rischio, che descrive o correla ad altri documenti aziendali (Disposizioni organizzative, Procedure, Regolamenti etc.), per ciascuna area di attività sensibile, le fattispecie di reato rilevanti, i processi coinvolti, i principi comportamentali da rispettare nonché i presidi di controllo da assicurare per la prevenzione dei rischi.

Il MOG sviluppato sul contesto aziendale tiene conto dei seguenti documenti, che ne costituiscono parte integrante:

- Struttura Organizzativa Aziendale [ALL 4]
- Catalogo reati presupposto ai Sensi del D. Lgs 231/2001 [ALL 5]
- Mappatura rischi reato e attività sensibili catalogo dei reati e delle fattispecie [ALL 6];

Diffusione del modello

L'adeguata formazione e la costante informazione dei Destinatari in ordine ai principi ed alle prescrizioni contenute nel MOG rappresentano fattori di grande importanza per la corretta ed efficace attuazione dello stesso.

Tutti i Destinatari del MOG sono tenuti ad avere piena conoscenza degli obiettivi di correttezza e di trasparenza che si intendono perseguire con il MOG e delle modalità attraverso le quali la Società ha inteso perseguirli, approntando un adeguato sistema di procedure e controlli.

La comunicazione e la formazione sui principi e contenuti del MOG sono garantite da SINTAX che identifica, di concerto con l'Organismo di Vigilanza, la migliore modalità di fruizione di tali servizi.

L'attività di comunicazione e formazione è supervisionata dall'Organismo di Vigilanza che potrà proporre eventuali integrazioni ritenute utili.

L'adozione del MOG e del Codice Etico (ALL 1) (e di ogni loro versione aggiornata) è comunicata a tutto il personale dirigente e non dirigente in forza in azienda nonché ai collaboratori più stretti al momento dell'adozione stessa, rendendola disponibile sulla bacheca elettronica aziendale e pubblicandola sul sito internet aziendale.

La consegna è presa visione è assicurata al nuovo personale come parte integrante del percorso di "on-boarding" in azienda.

Al fine di agevolare la comprensione della normativa di cui al D. Lgs 231/2001 e del MOG, i dipendenti ed i collaboratori più stretti, con modalità diversificate secondo il loro ruolo e grado di coinvolgimento nelle attività sensibili, sono tenuti a partecipare alle specifiche attività formative promosse dalla Società con frequenza e contenuti idonei a garantire una conoscenza adeguata.

La partecipazione ai programmi di formazione è obbligatoria rispetto a tutti i destinatari della formazione stessa e deve essere documentata. Sono inoltre previsti controlli di frequenza e verifiche dell'apprendimento.

Le eventuali modifiche apportate al MOG, nonché ogni rilevante cambiamento procedurale, normativo o organizzativo ad esso correlato sono comunicate ai destinatari mediante idonei strumenti di comunicazione.

Le parti terze (partner commerciali, fornitori, consulenti e collaboratori esterni) sono informati, all'atto dell'avvio della collaborazione, dell'adozione, da parte della Società, del MOG e del Codice Etico [ALL 1] e dell'esigenza che il loro comportamento sia conforme alle inerenti prescrizioni adottate da SINTAX.

Aggiornamento ed adeguamento del modello

Il Consiglio di Amministrazione di SINTAX delibera in merito all'aggiornamento del MOG e al suo adeguamento in relazione a modifiche e/o integrazioni che si dovessero rendere necessarie in conseguenza ad esempio di:

- modifiche dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa;
- cambiamenti delle aree di business;
- modifiche normative;
- risultanze dei controlli;
- esiti degli Audit interni o esterni e delle attività di risk management.
- eventi di significative violazioni delle prescrizioni del MOG.
- Altre modifiche di natura formale (es. chiarimenti e precisazioni nel testo)

In ogni caso, eventuali accadimenti che rendano necessaria la modifica o l'aggiornamento del MOG devono essere segnalati in forma scritta dall'Organismo di Vigilanza al Consiglio di Amministrazione, affinché lo stesso possa effettuare le delibere di propria competenza.

L'Organismo di Vigilanza è costantemente informato dell'aggiornamento e dell'implementazione di eventuali nuove norme e procedure aziendali ed ha facoltà di esprimere il proprio parere sulle proposte di modifica.

ATTIVITA' A RISCHIO DI COMMISSIONE DI REATI

Premessa

Ai sensi dell'Art 6 del D. Lgs 231/2001, la mera adozione del MOG da parte dell'organo amministrativo della Società non è misura sufficiente a determinare l'esonero da responsabilità della Società stessa, essendo necessario che esso sia anche efficace ed effettivo.

In questo senso, all'art. 6 comma 2, il Legislatore stabilisce che il MOG deve soddisfare le seguenti esigenze:

a) individuare le attività nel cui ambito possono essere commessi reati (cosiddetta "mappatura" delle attività a rischio);
b) prevedere specifici protocolli/procedure dirette a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai reati da prevenire;
c) individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate dal MOG.

Nel caso di reati commessi da soggetti apicali, la Società dovrà dunque essere in grado di dimostrare la sua estraneità ai fatti contestati provando la sussistenza dei sopra elencati requisiti tra loro concorrenti e, di riflesso, la circostanza che la commissione del reato non derivi da una propria "colpa organizzativa".

Nel caso di reati commessi da soggetti sottoposti, la Società risponde se la commissione del reato è stata resa possibile dalla violazione degli obblighi di direzione o vigilanza alla cui osservanza la società stessa è tenuta (art. 7 comma 1).

Fattispecie di reato previste dal D. Lgs 231/2001

Il D. Lgs 231/2001 riguarda esclusivamente alcune particolari fattispecie di illecito penale, esplicitamente richiamate negli articoli 24 e 25 del decreto medesimo, attualmente aggiornati a marzo 2023.

Sono di seguito indicati gli ambiti di reato valutati come applicabili nel contesto SINTAX, il cui dettaglio inclusivo dei relativi riferimenti legislativi e delle sanzioni amministrative e penali previste è riportato nell' ALL 5, includendo le razionali motivazioni per la non applicabilità di alcuni reati in quanto la Società non svolge attività in cui gli stessi possano essere commessi, né appaiono configurabili, in caso di loro commissione, l'interesse o il vantaggio della stessa.

Art 24	Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture
Art 24bis	Delitti informatici e trattamento illecito di dati
Art 24ter	Delitti di criminalità organizzata
Art 25	Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio
25bis1	Delitti contro l'industria e il commercio
25ter	Reati societari (inclusa la corruzione tra privati)
25quinques	Delitti contro la personalità individuale
25sexies	Abusi di mercato
25septies	Omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro
25octies	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio
25octies.1	Delitti in materia di strumenti di pagamento diversi dai contanti
25novies	Delitti in materia di violazione del diritto d'autore
25decies	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
25undecies	Reati ambientali
25duodecies	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare
25terdecies	Razzismo e xenofobia
25quinquiesdecies	Reati tributari

Individuazione delle attività sensibili di commissione di reati

In relazione alle attività svolte da SINTAX, sono individuate le seguenti aree funzionali nel cui ambito si possono manifestare fattori di rischio relativi alla commissione di reati presupposto del Dlgs. n. 231/2001 o, in generale, di violazione del Codice Etico dell'Impresa. Le "attività sensibili" rilevate, sono le seguenti e ad esse sono associate le fattispecie di reato previste dal D. Lgs 231/2001:

Attività Sensibile	Descrizione	Fattispecie di Reato
Mercato - Acquisizione commesse da privati	Fattori di rischio riferiti alle attività che presuppongono la sottoscrizione di contratti con privati fattori di rischio riferiti al rapporto con il committente privato e con i fornitori.	Art 24ter, Art 25, Art 25bis.1, Art 25ter
Mercato - Partecipazioni ad Appalti Pubblici	Nella partecipazione a pubbliche gare o trattative per l'affidamento di lavori pubblici in appalto o in concessione, fattori di rischio relativi alle fasi delle procedure di gara, di autorizzazione del subappalto, di gestione dell'eventuale contenzioso con il committente, di collaudo dei servizi erogati.	Art 24ter, Art 25, Art 25bis.1, Art 25ter
Mercato - Rapporti con la Pubblica Amministrazione	fattori di rischio relativi a tutte le attività che implicano un rapporto diretto con pubblici uffici, organi ispettivi, enti pubblici erogatori di contributi o titolari di poteri autorizzativi, concessori od abilitativi.	Art 24ter, Art 25, Art 25bis.1, Art 25ter
Produzione - Erogazione di servizi	Fattori di rischio di frode informatica nel corso della gestione massiva di banche dati di proprietà della pubblica amministrazione con elevate implicazioni sulla privacy dei contribuenti.	Art 24bis
Produzione - Sviluppo di Piattaforme Informatiche	Fattori di rischio di frode informatica nel corso del processamento di banche dati di proprietà della pubblica amministrazione con elevate implicazioni sulla privacy dei contribuenti. Fattori di rischio di illecito nella violazione del copyright e di uso di prodotti non licenziati.	Art 24bis, Art 25novies
Produzione - Conduzione piattaforme Informatiche	Fattori di rischio di reati dolosi o colposi di tipo "cybercrime" e conseguenti in una distruzione o compromissione di banche dati di proprietà della pubblica amministrazione.	Art 24bis, Art. 25quinques
Governance - Comunicazioni sociali e controlli	Fattori di rischio relativi alla scorretta o incompleta rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nei bilanci e nei documenti ad uso informativo, sia interno che esterno Fattori di rischio relativi a comportamenti idonei ad ostacolare da parte dei soggetti e delle autorità competenti i controlli preventivi sulla attività e sulla rappresentazione contabile dell'attività d'impresa.	Art. 24, Art 24bis, Art 24ter, Art. 25, Art 25ter, Art 25sexies, Art 25octies, Art 25octies.1, Art 25decies, Art 25quinquiesdecies,
Governance - Rapporti con soci creditori e terzi	Fattori di rischio di comportamenti anche solo potenzialmente pregiudizievoli dell'interesse dei soci, dei creditori e dei terzi. In caso di situazioni di conflitto di interessi, fattori di rischio relativi alla attuazione di operazioni di gestione o organizzative interne a condizioni svantaggiose per la Società od alla omissione di decisioni vantaggiose per la Società.	Art 24bis, Art 24ter, Art 25, Art 25ter, Art 25sexies, Art 25octies, Art 25octies.1, Art 25decies, Art 25quinquiesdecies,

Attività Sensibile	Descrizione	Fattispecie di Reato
Governance - Gestione del Personale	Fattori di rischio relativi alle modalità di reclutamento del personale e al rispetto delle corrette condizioni di concorrenza.	Art 25quinquies, Art 25septies, Art 25duodecies, Art 25terdecies
Governance - Amministrazione e contabilità	Fattori di rischio derivanti dalla gestione dei flussi monetari attivi e passivi	Art 24, Art 25octies, A Art 25octies.1, Art 25quinquiesdecies
Governance - Sicurezza e Salute dei Lavoratori	Fattori di rischio relativi a comportamenti che costituiscono violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.	Art 25septies
Governance - Gestione Ambientale	Fattori di rischio relativi alle attività che possono comportare inquinamento, danno ambientale o alterazione del patrimonio naturale, della flora e della fauna.	Art 25undecies

Processi a rischio reato relativi alle attività sensibili

Il MOG SINTAX è basato sull'approccio per processi già delineato nel modello di Sistema di Gestione conforme alle norme ISO 9001, ISO/IEC 27001 e ISO 37001.

In base ai suddetti Standard Internazionali ogni modello organizzativo richiede che tutti i processi aziendali sono definiti, adeguatamente descritti (ovvero documentati e/o procedurizzati) anche nelle loro interrelazioni e che all'interno di ciascun processo vengano chiaramente definite ed assegnate responsabilità e autorità.

L'analisi svolta alla base del MOG identifica i seguenti processi a rischio reato rispetto alle attività sensibili

Attività Sensibile	Processi a rischio	Fattispecie di Reato
Mercato - Acquisizione commesse da privati	• Responsabilità della direzione • Organizzazione e Gestione • Studio offerte e Gestione Gare	Art 24ter, Art 25, Art 25 bis.1, Art 25ter
Mercato - Partecipazioni ad Appalti Pubblici	• Responsabilità della direzione • Organizzazione e Gestione • Studio offerte e Gestione Gare	Art 24ter, Art 25, Art 25 bis.1, Art 25ter
Mercato - Rapporti con la Pubblica Amministrazione	• Responsabilità della direzione • Organizzazione e Gestione • Studio offerte e Gestione Gare	Art 24ter, Art 25, Art 25 bis.1, Art 25ter
Produzione - Erogazione di servizi	• Assistenza Clienti • Data Protection & Incident Management • Sistemi Informativi Interni	Art 24bis

Attività Sensibile	Processi a rischio	Fattispecie di Reato
Produzione - Sviluppo di Piattaforme Informatiche	• Progettazione e sviluppo • Data Protection & Incident Management • Sistemi Informativi Interni	Art 24bis, Art 25 bis1, Art 25ter, Art 25novies
Produzione - Conduzione piattaforme Informatiche	• Cloud IT Operation • Gestione servizi erogati da terze parti • Data Protection & Incident Management • Sistemi Informativi Interni	Art 24bis, Art 25novies
Governance - Comunicazioni sociali e controlli	• Responsabilità della direzione • Organizzazione e Gestione • Amministrazione finanza e controllo • Valutazione Performance	Art 24bis, Art 25quinques
Governance - Rapporti con soci creditori e terzi	• Responsabilità della direzione • Organizzazione e Gestione • Amministrazione finanza e controllo • Partner e fornitori strategici • Valutazione Performance	Art. 24, Art 24bis, Art 24ter, Art 25, Art 25ter, Art 25sexies, Art 25octies, Art 25octies.1, Art 25decies, Art 25quinquiesdecies
Governance - Gestione del Personale	• Responsabilità della direzione • Gestione del Personale • Comunicazione Interna e Formazione • Sistemi Informativi Interni	Art 25quinquies, Art 25septies, Art 25decies, Art 25duodecies, Art 25terdecies
Governance - Amministrazione e contabilità	• Responsabilità della direzione • Organizzazione e Gestione • Amministrazione finanza e controllo • Partner e fornitori strategici	Art 24, Art 25octies, Art 25octies.1, Art 25decies, Art 25quinquiesdecies
Governance - Sicurezza e Salute dei Lavoratori	• Compliance S&SL e Ambiente	Art 25septies
Governance - Gestione Ambientale	• Compliance S&SL e Ambiente	Art 25undecies

Mappatura del rischio reato

Nella mappatura del rischio reato [ALL 6] vengono considerate nel dettaglio tutte le possibili occorrenze dei reati presupposto nell'ambito delle attività operative rispetto ai processi considerati, evidenziando i fattori di controllo procedurali e le relative frequenze che ne prevengono il verificarsi per "colpa organizzativa" o per "omessa vigilanza".

Esito finale della mappatura di rischio è la ponderazione del livello di adeguatezza delle misure di controllo esistenti, e la proposizione di azioni specifiche di trattamento dei rischi nel caso in cui tali misure presentino ancora dei margini di miglioramento.

La mappatura dei rischi del MOG può essere di input ad altre Analisi di Rischio previste dagli Standard Internazionali ISO precedentemente riferiti, condividendone i risultati per la conferma di affidabilità della ponderazione quantitativa.

Essa va riverificata almeno una volta all'anno per conferma di adeguatezza e ogni qualvolta siano rilevate necessità di aggiornamento, ovvero quando sono scoperte significative violazioni delle prescrizioni oppure quando intervengono mutamenti nell'organizzazione o nei processi di business.

I risultati della mappatura dei rischi sono sottoposti al Consiglio di Amministrazione e all'Organismo di Vigilanza per valutazioni di merito sulla sua adeguatezza.

Protocolli di controllo

Alla base della confidenza di adeguatezza del MOG vi è il rispetto di definiti protocolli generali di conformità che devono essere contemplati, rispettati e resi verificabili nel modello organizzativo aziendale e nei singoli processi impattati dalle aree a rischio reato.

Macroarea	Protocollo	Descrizione
Leadership e governance	Mansioni e responsabilità	Mansioni e responsabilità di tutto il personale debbono essere definite e rese note a tutta l'azienda; la catena gerarchica deve essere nota e rispettata.
	Recruiting	I processi di selezione del nuovo personale devono essere trasparenti e basati sulla obiettività di valutazione delle reali capacità dei candidati rispetto alle esigenze di assunzione. Le scelte di assunzione non devono essere influenzate da pregiudizi sulle differenze di genere.
	Deleghe e procure	Le deleghe e le procure conferite al personale o a terzi debbono essere chiare, giuridicamente valide e formalmente accettate dall'interessato.
Standard di comportamento	Codice etico	Deve essere definito uno standard di comportamento aziendale con riferimento agli aspetti etici e di prevenzione dei reati; tale standard deve essere formalizzato, diffuso ed aggiornato quando necessario.
	Procedure	Le procedure aziendali debbono coprire almeno i processi considerati critici e, quando necessario, essere aggiornate nel tempo.
Comunicazione e formazione	Comunicazione	Debbono essere previste modalità di comunicazione con il personale adeguate alle dimensioni dell'impresa (ordini di servizio, riunioni periodiche, e-mail, intranet, etc); tali modalità debbono essere rese operative in modo da

Macroarea	Protocollo	Descrizione
		essere riconosciute efficaci dallo stesso personale dell'impresa.
	Formazione	La pianificazione dell'attività di formazione deve prevedere che tutto il personale dell'azienda venga formato sulle tematiche etiche e sui contenuti delle procedure aziendali; una specifica formazione deve essere riservata ai neoassunti.
Controllo e Valutazione delle performances	Retribuzione correlata agli obiettivi	Nel caso di componenti di retribuzione variabile legati al raggiungimento di specifici obiettivi da parte di una funzione, è necessario che gli stessi obiettivi siano quantificabili, raggiungibili ed accettati dalla funzione interessata.
	Responsabilità per i controlli	Per quanto consentito dalle dimensioni dell'impresa, debbono essere sempre separate le responsabilità di chi agisce e quelle di chi controlla. Le procedure debbono identificare chi è responsabile dei controlli necessari e come debbono essere documentati i controlli effettuati. Le operazioni rilevanti debbono essere sempre verificabili e deve essere prevista attività di controllo (anche a campione) almeno sulle operazioni considerate critiche.
Reazione alle violazioni	Sistema sanzionatorio	Per il personale dipendente, deve essere implementato uno specifico sistema sanzionatorio (disciplinare), congruente con quello previsto dal Contratto Collettivo Nazionale applicabile, finalizzato al rispetto delle procedure operative aziendali e a dissuadere chiunque dall'agire illecitamente. Tale sistema sanzionatorio è applicabile anche a chi, all'interno dell'organizzazione, viola le misure di tutela dell'identità di chi segnala condotte illecite o violazioni del modello di organizzazione e gestione dell'ente ovvero commette atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione. Per collaboratori e fornitori devono essere previste contrattualmente clausole aventi la stessa finalità. Per violazioni commesse dall'organismo amministrativo (amministratori) deve essere prevista la segnalazione al Consiglio di Amministrazione al Collegio Sindacale o ad altro organo equivalente. Eventuali violazioni commesse dall'Organismo di Vigilanza costituiscono giusta causa per la revoca dell'incarico.

Macroarea	Protocollo	Descrizione
Information Security Governance	Organizzazione	Sono fornite dalla società politiche e indirizzi chiari per la sicurezza delle informazioni in conformità ai requisiti del business e alle leggi e regolamenti pertinenti, assicurandone la consapevolezza e condivisione da parte del personale e ove applicabile delle parti terze interessate. Sono attuate procedure e metodi di controllo efficaci che vigilano sugli adempimenti di tali indirizzi rilevando e sanzionando eventuali violazioni.
	Sicurezza delle persone	Tutti i dipendenti, i collaboratori e gli utenti di terze parti, sono resi consapevoli delle minacce e delle preoccupazioni relative alla sicurezza delle informazioni, delle loro responsabilità verso l'organizzazione e verso la legge, e che siano messi in grado di supportare la politica per la sicurezza dell'organizzazione durante lo svolgimento della loro normale attività lavorativa. Tale responsabilità, per quanto applicabile è estesa anche dopo la cessazione del rapporto di lavoro. I diritti di accesso alle informazioni sono controllati, assicurando l'accesso ai sistemi informativi ai soli utenti autorizzati e prevenendo accessi non autorizzati, con particolare riguardo ai diritti di accesso privilegiati (Amministratori di Sistemi). Assicurare che per i dipendenti, i collaboratori e gli utenti di terze parti che interrompono o variano il rapporto di lavoro sia garantita la pronta ed efficace rimozione dei diritti di accesso.
Cyber Security	Controlli tecnologici	Sono stabiliti mezzi e tecnologie efficaci e sempre aggiornati per la protezione dei beni, delle informazioni e dei dati aziendali assicurandone le proprietà attese di Riservatezza Integrità e Disponibilità necessarie alla prevenzione di eventi avversi di compromissione e comportamenti fraudolentemente dolosi sia da sorgenti esterne che interne (cyber crime).

Nella Parte Speciale del MOG è descritta in dettaglio la relazione tra Aree Sensibili, Reati presupposto, Processi impattati, Procedure e metodi di controllo dimostrando nel dettaglio il soddisfacimento dei protocolli.

L'ORGANISMO DI VIGILANZA

Istituzione dell'OdV

Secondo quanto previsto dall'art. 6, lett. b) del D. Lgs. 231/2001, l'ente può essere esonerato dalla responsabilità amministrativa prevista dal Decreto stesso, se l'organo dirigente ha, fra l'altro, affidato il compito di vigilare sul funzionamento e l'osservanza del MOG e di curarne l'aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

L'affidamento dei suddetti compiti ad un organismo dotato di autonomi poteri di iniziativa e controllo, unitamente al corretto ed efficace svolgimento degli stessi, rappresentano, quindi, presupposti indispensabili per l'esonero dalla responsabilità prevista dal D. Lgs. 231/2001.

I requisiti principali dell'Organismo di Vigilanza (di seguito anche "OdV"), così come proposti dalle linee guida emanate da Confindustria e fatti propri anche dagli organi giudicanti nelle diverse pronunce giurisprudenziali pubblicate, possono essere così identificati:

- autonomia ed indipendenza;
- professionalità;
- continuità di azione.

L'autonomia e l'indipendenza dell'OdV si traducono nell'autonomia dell'iniziativa di controllo rispetto ad ogni forma d'interferenza o di condizionamento da parte di qualunque esponente della persona giuridica e, in particolare, dell'organo amministrativo.

Al fine di assicurare tali requisiti, l'OdV riporta esclusivamente al Consiglio di Amministrazione nel suo complesso. L'OdV deve altresì godere di garanzie tali da impedire che lo stesso possa essere rimosso o penalizzato in conseguenza dell'espletamento dei propri compiti.

Il requisito della professionalità si traduce nella capacità dell'OdV di assolvere alle proprie funzioni ispettive, rispetto all'effettiva applicazione del MOG, nonché nelle necessarie qualità per garantire la dinamicità del MOG medesimo, attraverso proposte di aggiornamento da indirizzare al Vertice aziendale.

Con riferimento, infine, alla continuità di azione, l'OdV deve vigilare costantemente sul rispetto del MOG, verificare l'effettività e l'efficacia dello stesso, promuoverne il continuo aggiornamento e rappresentare un referente costante per ogni soggetto che presti attività lavorativa per la Società.

Il D. Lgs. 231/2001 non fornisce indicazioni specifiche circa la composizione dell'Organismo di Vigilanza. In assenza di tali indicazioni, la Società ha optato per una soluzione che, tenuto conto delle finalità perseguite dalla legge e dagli indirizzi ricavabili dalla giurisprudenza pubblicata, sia in grado di assicurare, in relazione alle proprie dimensioni ed alla propria complessità organizzativa, l'effettività dei controlli cui l'Organismo di Vigilanza è preposto.

SINTAX, tenuto conto delle proprie caratteristiche, della sua organizzazione e dell'esposizione ai rischi reato come emerso dalle attività di analisi e valutazione, ha optato in questa prima fase di attuazione del MOG per una nomina monocratica e pro tempore di un professionista esterno già esperto nella materia di facente funzione di OdV, attribuendogli i poteri per soddisfare i propri compiti in modo efficace ed efficiente.

La nomina del facente funzione dell'Organismo di Vigilanza avviene con delibera del Consiglio di Amministrazione ed è condizionata alla presenza dei requisiti soggettivi di eleggibilità.

In particolare, costituisce causa di ineleggibilità o di decadenza dalla carica di componente dell'OdV:

- la titolarità, diretta o indiretta, di partecipazioni azionarie in società;
- rapporto di dipendenza rispetto alla società;
- l'esistenza di conflitti di interesse, anche potenziali, con la Società tali da pregiudicare l'indipendenza richiesta dal ruolo e dai compiti propri dell'OdV;

- l'aver svolto funzioni di amministrazione - nei tre esercizi precedenti alla nomina quale membro dell'OdV ovvero all'instaurazione del rapporto di consulenza/collaborazione con la Società;
- l'aver riportato una sentenza di condanna anche non passata in giudicato ovvero sentenza di applicazione della pena su richiesta (il c.d. patteggiamento), in Italia o all'estero, per i delitti dolosi richiamati dal Decreto.

All'atto dell'accettazione della nomina, il componente rilascia una dichiarazione in cui attesta l'assenza delle sopra indicate cause di ineleggibilità. Laddove alcuno dei sopra richiamati motivi di ineleggibilità dovesse configurarsi in capo ad un soggetto già nominato, l'interessato comunica tempestivamente la notizia alla Società affinché questi disponga gli opportuni provvedimenti.

Il facente funzione dell'Organismo di Vigilanza potrà giovarsi, sotto la sua diretta sorveglianza e responsabilità, nello svolgimento dei compiti affidatigli, della collaborazione di tutte le direzioni, funzioni e strutture della Società ovvero di consulenti esterni, avvalendosi delle rispettive competenze e professionalità. Tale facoltà consente al facente funzione di assicurare un elevato livello di professionalità e la necessaria continuità di azione.

A tal fine il Consiglio di Amministrazione ha facoltà di assegnare, ogni anno, un budget di spesa al facente funzione dell'Organismo di Vigilanza tenuto conto delle richieste di quest'ultimo che dovranno essere formalmente presentate al Consiglio di Amministrazione.

Al fine di garantire la necessaria stabilità, la revoca dei poteri propri del facente funzione dell'Organismo di Vigilanza e l'attribuzione di tali poteri ad altro soggetto potrà avvenire soltanto per giusta causa, anche legata ad interventi di ristrutturazione organizzativa della Società, mediante un'apposita delibera del Consiglio di Amministrazione.

A tale proposito, per "giusta causa" di revoca dei poteri connessi con l'incarico di Organismo di Vigilanza potrà intendersi, a titolo meramente esemplificativo:

- una sentenza di condanna definitiva della Società ai sensi del D. Lgs 231/2021 o una sentenza di patteggiamento, passata in giudicato, ove risulti dagli atti "l'omessa o insufficiente vigilanza" da parte del facente funzione dell'Organismo di Vigilanza, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;
- una sentenza di condanna o di patteggiamento emessa nei confronti del facente funzione dell'Organismo di Vigilanza per aver commesso uno dei reati o illeciti amministrativi previsti dal D. Lgs 231/2021 (o reati/illeciti amministrativi della stessa indole);
- la violazione degli obblighi di riservatezza a cui l'OdV è tenuto;
- una grave negligenza nell'adempimento dei propri compiti quale, ad esempio, l'omessa redazione della relazione informativa annuale al Consiglio di Amministrazione sull'attività svolta;
- l'attribuzione di funzioni e responsabilità operative all'interno dell'organizzazione aziendale incompatibili con i requisiti di "autonomia e indipendenza" e "continuità di azione" propri del facente funzione dell'Organismo di Vigilanza.

Funzioni e poteri dell'OdV

Al facente funzione dell'Organismo di Vigilanza sono conferiti i poteri di iniziativa e controllo necessari per assicurare un'effettiva ed efficiente vigilanza sul funzionamento e sull'osservanza del MOG secondo quanto stabilito dall'art. 6 del D. Lgs. 231/2001.

In particolare, l'OdV deve vigilare:

- sull'adeguatezza ed effettività del MOG rispetto all'esigenza di prevenire la commissione dei reati per cui trova applicazione il D. Lgs. 231/2001, tenendo conto anche delle dimensioni e della complessità organizzativa e operativa della Società;
- sulla permanenza nel tempo dei requisiti di adeguatezza ed effettività del MOG;

- sull'osservanza delle prescrizioni del MOG da parte dei Destinatari, rilevando eventuali violazioni e proponendo i relativi interventi correttivi e/o sanzionatori agli organi aziendali competenti;
- sull'aggiornamento del MOG nel caso in cui si riscontrassero esigenze di adeguamento in relazione alle mutate condizioni aziendali o normative, proponendo le eventuali azioni di adeguamento agli organi aziendali competenti e verificandone l'implementazione.

Per l'espletamento e l'esercizio delle proprie funzioni, all'OdV sono attribuiti i compiti e i poteri di:

- accedere a tutte le strutture della Società e a tutta la documentazione aziendale rilevante ai fini di verificare l'adeguatezza e il rispetto del MOG;
- effettuare verifiche a campione mirate su specifiche attività/operazioni a rischio e sul rispetto dei presidi di controllo e di comportamento adottati e richiamati dal MOG e da eventuali procedure aziendali;
- promuovere l'aggiornamento della mappatura dei rischi in caso di significative variazioni organizzative o di estensione della tipologia di reati presi in considerazione dal D. Lgs. 231/2001;
- coordinarsi con le funzioni aziendali di riferimento per valutare l'adeguatezza del corpo normativo interno adottato e definire eventuali proposte di adeguamento e miglioramento (regole interne, procedure, modalità operative e di controllo) verificandone, successivamente, l'attuazione;
- monitorare le iniziative di informazione/formazione finalizzate alla diffusione della conoscenza e della comprensione del MOG in ambito aziendale;
- richiedere ai responsabili aziendali, in particolare a coloro che operano in aree aziendali a potenziale rischio-reato, le informazioni ritenute rilevanti ai fini di verificare l'adeguatezza e l'effettività del MOG;
- raccogliere eventuali segnalazioni provenienti da qualunque Destinatario del MOG in merito a: eventuali criticità delle misure previste dal MOG; violazioni dello stesso; qualsiasi situazione che possa esporre la Società a rischio di reato;
- segnalare periodicamente all'Amministratore Unico e ai responsabili delle Direzioni/Funzioni interessate eventuali violazioni di presidi di controllo richiamati dal MOG o le carenze rilevate in occasione delle verifiche svolte, affinché questi possano adottare i necessari interventi di adeguamento coinvolgendo, ove necessario, il Consiglio di Amministrazione;
- vigilare sull'applicazione coerente delle sanzioni previste dalle normative interne nei casi di violazione del MOG, ferma restando la competenza dell'organo dirigente per l'applicazione dei provvedimenti sanzionatori;
- rilevare gli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i Destinatari del MOG.

Il facente funzione dell'OdV dispone la calendarizzazione e le modalità di svolgimento delle attività di sua pertinenza, nonché la procedura seguita per il trattamento delle segnalazioni.

Il facente funzione dell'OdV è tenuto al vincolo di riservatezza rispetto a tutte le informazioni di cui è a conoscenza a causa dello svolgimento del proprio incarico.

La divulgazione di tali informazioni potrà essere effettuata solo ai soggetti e con le modalità previste dal MOG stesso.

Obblighi di informazione nei confronti dell'OdV

Il facente funzione dell'Organismo di Vigilanza deve essere tempestivamente informato dai Destinatari del MOG, mediante apposite segnalazioni, in merito ad atti, comportamenti od eventi che possano determinare una violazione del MOG o che, più in generale, siano rilevanti ai fini del D. Lgs. 231/2001.

Più precisamente, tutti i Destinatari del MOG o hanno l'obbligo di segnalare tempestivamente all'OdV le seguenti informazioni ("segnalazioni"):

- la commissione, il tentativo di commissione o il ragionevole pericolo di commissione dei reati previsti dal D. Lgs 231/2001;
- eventuali presunte violazioni alle modalità comportamentali ed operative definite nel Codice Etico, nel MOG e/o nel corpo normativo e procedurale aziendale, di cui siano direttamente o indirettamente venuti a conoscenza;
- qualsiasi notizia, ancorché anonima, riguardante sospette/presunte violazioni della legge;
- in ogni caso, qualsiasi atto, fatto, evento od omissione rilevato od osservato nell'esercizio delle responsabilità e dei compiti assegnati, con profilo di criticità rispetto alle norme del D. Lgs 231/2001;
- osservazioni sull'adeguatezza del sistema di controllo;
- qualsiasi eccezione comportamentale o qualsiasi evento inusuale indicando le ragioni delle difformità e dando atto del diverso processo seguito.

I segnalanti in buona fede sono garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione ed in ogni caso è assicurata la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

Le segnalazioni devono essere effettuate in forma scritta e preferibilmente non anonima ai recapiti comunicati del facente funzione dell'OdV.

Il facente funzione dell'OdV valuta le segnalazioni ricevute e i casi in cui è necessario attivarsi.

Oltre alle segnalazioni di cui sopra, le Direzioni/Funzioni aziendali di volta in volta interessate devono trasmettere al facente funzione dell'Organismo di Vigilanza le informazioni concernenti (c.d. "informazioni generali"):

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini o di procedimenti penali, anche nei confronti di ignoti, relativi a fatti d'interesse e/o che possano coinvolgere la Società (relativi al D. Lgs. 231/2001 e non);
- i provvedimenti e/o notizie aventi ad oggetto l'esistenza di procedimenti amministrativi o civili di rilievo relativi a richieste o iniziative di Autorità pubbliche;
- ogni atto o citazione a testimoniare che veda coinvolti soggetti della Società o che collaborano con essa;
- le richieste di assistenza legale inoltrate dai dipendenti in caso di avvio di procedimento penali o civili nei loro confronti (non solo in relazione ai reati di cui al D. Lgs. 231/2001);
- le informazioni relative alle eventuali visite ispettive condotte da funzionari della Pubblica Amministrazione e comunicati da tutte le Direzioni/Funzioni aziendali;
- le notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate ovvero ai provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- le comunicazioni inerenti modifiche organizzative e societarie;
- anomalie o criticità riscontrate dai responsabili nello svolgimento delle attività sensibili per l'applicazione del D. Lgs. 231/2001.

In capo a ciascun Responsabile di Direzione/Funzione della Società, in qualità di soggetto preposto alla completa e corretta adozione delle regole aziendali a presidio dei rischi individuati nei settori di sua competenza, è altresì previsto l'obbligo di trasmettere al facente funzione dell'Organismo di Vigilanza, su base periodica o al verificarsi di determinati eventi, i dati e le informazioni da questi richiesti, anche sulla base di specifiche procedure adottate o comunicazioni inviate dal facente funzione dell'OdV stesso (c.d. "informazioni specifiche").

Le informazioni generali e le informazioni specifiche devono essere inviate al facente funzione dell'OdV in forma scritta utilizzando l'indirizzo di posta elettronica comunicato dallo stesso.

Ogni informazione, segnalazione, report, relazione previsto nel Modello sono conservati dal facente funzione dell'OdV in un apposito archivio riservato (informatico o cartaceo).

In relazione alle attività della Società e al fine di garantire uno stabile collegamento operativo fra il facente funzione dell'OdV e le funzioni aziendali, con il benestare dell'Amministratore Unico, il referente della funzione **Assurance & Compliance**, anche responsabile del Sistema di Gestione Integrato ISO, assume il ruolo di referente dell'OdV per tutto ciò che concerne l'attività dell'OdV.

Relazione dell'OdV verso il Consiglio di Amministrazione

Al fine di garantire la sua piena autonomia e indipendenza nello svolgimento delle proprie funzioni, il facente funzione dell'OdV riferisce direttamente al Consiglio di Amministrazione della Società.

In particolare, l'OdV trasmette al Consiglio di Amministrazione:

- con cadenza annuale una relazione informativa, relativa all'attività svolta;
- al verificarsi di violazioni accertate del Modello, con presunta commissione di reati, una comunicazione per quanto di competenza.

Il facente funzione dell'Organismo di Vigilanza ha comunque la facoltà di richiedere la propria audizione al Consiglio di Amministrazione, qualora ne ravvisi la necessità.

Allo stesso modo, il Consiglio di Amministrazione ha facoltà di convocare il facente funzione dell'Organismo di Vigilanza qualora lo ritenga opportuno.

Nell'ambito della relazione informativa periodica vengono affrontati i seguenti aspetti:

- controlli e verifiche svolti ed esito degli stessi;
- eventuali criticità emerse;
- stato di avanzamento di eventuali interventi correttivi e migliorativi del MOG;
- eventuali innovazioni legislative o modifiche organizzative che richiedano aggiornamenti nell'identificazione dei rischi o variazioni del MOG;
- eventuali sanzioni disciplinari irrogate dagli organi competenti a seguito di violazioni del Modello;
- eventuali segnalazioni ricevute da soggetti interni ed esterni nel corso del periodo in ordine a presunte violazioni al MOG o al Codice Etico;
- il piano di attività previsto per il periodo successivo;
- altre informazioni ritenute significative

Gli incontri con gli organi societari devono essere documentati. Il facente funzione dell'Organismo di Vigilanza cura l'archiviazione della relativa documentazione.

IL SISTEMA DISCIPLINARE E SANZIONATORIO

Funzione del sistema disciplinare

L'art. 6, comma 2, lett. e) e l'art. 7, comma 4, lett. b) del D. Lgs. 231/2001 indicano, quale condizione per un'efficace attuazione del Modello di Organizzazione, Gestione e Controllo, l'introduzione di un sistema idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso.

Pertanto, la definizione di un adeguato sistema disciplinare, con sanzioni proporzionate alla gravità della violazione rispetto alle infrazioni delle regole di cui al presente MOG e relativi Allegati da parte dei Destinatari, costituisce un presupposto essenziale per l'efficacia del MOG stesso.

Le sanzioni previste saranno applicate ad ogni violazione delle disposizioni contenute nel MOG a prescindere dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria, nel caso in cui il comportamento da censurare integri gli estremi di una fattispecie di reato rilevante ai sensi del D. Lgs. 231/2001.

In ogni caso, la sanzione prescinde dalla commissione del reato e si attesta come reazione della Società al mancato rispetto di procedure o regole comportamentali richiamate dal MOG e dai relativi Allegati.

Misure nei confronti di lavoratori dipendenti non dirigenti

Le violazioni delle disposizioni e delle regole comportamentali previste dal MOG e dai suoi Allegati da parte dei dipendenti della Società costituiscono inadempimento contrattuale. Ne consegue che la violazione delle singole disposizioni e regole comportamentali previste dal Modello e dai suoi Allegati da parte dei dipendenti può comportare l'adozione di sanzioni disciplinari, nei limiti stabiliti dal Contratto Collettivo Nazionale Lavoro ("CCNL") applicabile. Per i dipendenti di livello non dirigenziale, tali provvedimenti sono quelli previsti dalle norme disciplinari di cui al CCNL, in particolare:

- richiamo/rimprovero verbale;
- rimprovero scritto;
- multa fino all'importo di 4 ore di retribuzione;
- sospensione dalla retribuzione e dal lavoro fino a 10 giorni;
- licenziamento senza preavviso.

I provvedimenti disciplinari sono irrogabili nei confronti dei lavoratori dipendenti in conformità a quanto previsto dall'art. 7 della legge 20 maggio 1970, n. 300. La tipologia e l'entità della sanzione è definita tenendo conto della gravità e/o recidività della violazione e del grado di colpa, più precisamente:

- intenzionalità del comportamento;
- presenza di circostanze aggravanti o attenuanti, con particolare riguardo alla professionalità, alle precedenti esperienze lavorative e alle circostanze in cui è stato commesso il fatto;
- rilevanza degli obblighi violati;
- entità del danno derivante alla Società;
- ruolo, livello di responsabilità gerarchica e autonomia del dipendente;
- eventuale condivisione di responsabilità con altri soggetti che abbiano concorso a determinare la mancanza;
- eventuali simili precedenti disciplinari.

Ad ogni notizia di violazione del MOG, verrà promossa un'azione disciplinare finalizzata all'accertamento della violazione stessa. In particolare, nella fase di accertamento verrà previamente contestato al dipendente l'addebito e gli sarà, altresì, garantito un congruo termine di replica in ordine alla sua difesa.

Una volta accertata la violazione, sarà comminata all'autore una sanzione disciplinare proporzionata alla gravità della violazione commessa ed all'eventuale recidiva. Resta inteso che saranno in ogni caso rispettate le procedure, le disposizioni e le garanzie previste dall'art. 7 dello Statuto dei Lavoratori e dalla normativa pattizia in materia di provvedimenti disciplinari. L'accertamento delle infrazioni (eventualmente su segnalazione dell'OdV e/o del Datore di Lavoro nel caso di infrazioni al sistema della salute e sicurezza sul lavoro), la gestione dei provvedimenti disciplinari e l'irrogazione delle sanzioni stesse sono di competenza della funzione "Gestione Del Personale". Ogni atto relativo al procedimento disciplinare dovrà essere comunicato all'OdV per le valutazioni ed il monitoraggio di sua competenza.

Misure nei confronti dei Dirigenti

I dipendenti con qualifica dirigenziale sono soggetti al Contratto Collettivo Nazionale di Lavoro per i Dirigenti. In caso di violazione del MOG e dei suoi Allegati da parte dei dirigenti, la Società provvederà ad applicare nei

confronti dei responsabili le misure più idonee in conformità a quanto previsto dalla vigente normativa e dal CCNL applicabile. L'accertamento delle infrazioni (eventualmente su segnalazione dell'OdV e/o del Datore di Lavoro nel caso di infrazioni al sistema della salute e sicurezza sul lavoro), la gestione dei provvedimenti disciplinari e l'irrogazione delle sanzioni stesse sono di competenza del vertice aziendale con il supporto dell'esperto in materia di gestione delle Risorse Umane. Ogni atto relativo al procedimento sanzionatorio dovrà essere comunicato all'OdV per le valutazioni ed il monitoraggio di sua competenza.

Misure nei confronti degli Amministratori

L'OdV, raccolta una notizia di violazione delle disposizioni e delle regole di comportamento del MOG da parte di membri del Consiglio di Amministrazione, dovrà tempestivamente informare dell'accaduto l'intero Consiglio di Amministrazione che, valutata la fondatezza della segnalazione ed effettuati i necessari accertamenti, potrà assumere gli opportuni provvedimenti previsti dalla Legge, sentito il parere del Collegio Sindacale. In particolare, il Consiglio di Amministrazione convocherà l'Assemblea dei Soci al fine di adottare le misure più idonee previste dalla legge, tra le quali l'eventuale revoca del mandato e/o la deliberazione di azioni di responsabilità nei confronti degli amministratori coinvolti nella violazione. Si specifica, a titolo esemplificativo, che costituisce violazione dei doveri degli amministratori:

- la commissione, anche sotto forma di tentativo, di un reato per cui è applicabile il D. Lgs. 231/2001 nell'espletamento delle proprie funzioni;
- l'inosservanza delle regole prescritte dal Modello o dal Codice Etico;
- la mancata vigilanza sui prestatori di lavoro o partner della Società circa il rispetto del Modello e delle regole da esso richiamate;
- l'inadempimento degli obblighi di "segnalazione" nei confronti dell'Organismo di Vigilanza;
- la tolleranza od omessa segnalazione di irregolarità commessa da altri prestatori di lavoro o partner della Società.

Ogni atto relativo al procedimento sanzionatorio dovrà essere comunicato all'Organismo di Vigilanza per le valutazioni ed il monitoraggio di sua competenza.

Misure nei confronti di partner commerciali, fornitori, consulenti e collaboratori esterni

L'adozione da parte di partner commerciali, fornitori, consulenti e collaboratori esterni, comunque denominati, o altri soggetti aventi rapporti contrattuali con la Società di comportamenti in contrasto con il D. Lgs. 231/2001 e con i principi ed i valori contenuti nel Codice Etico sarà sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti. Le violazioni gravi o reiterate dei principi contenuti nel Codice Etico (e, per i collaboratori più stretti, nel MOG) o l'adozione di comportamenti in contrasto con il D. Lgs. 231/2001 saranno considerate inadempimenti degli obblighi contrattuali e potrà dar luogo alla risoluzione del contratto. Il monitoraggio della costante idoneità delle clausole contrattuali è di competenza della funzione Amministratore Unico.

WHISTLEBLOWING

Definizione e normativa di riferimento

Il termine whistleblower identifica un individuo che denuncia pubblicamente o riferisca alle autorità attività illecite o fraudolente all'interno del governo, di un'organizzazione pubblica o privata o di un'azienda. Le rivelazioni o denunce possono essere di varia natura: violazione di una legge o regolamento, minaccia di un interesse pubblico come in caso di corruzione e frode, gravi e specifiche situazioni di pericolo per la salute e la sicurezza pubblica. La finalità primaria della segnalazione è quindi quella di portare all'attenzione dei

soggetti individuati i possibili rischi di irregolarità di cui si è venuti a conoscenza. La segnalazione, pertanto, si pone come un rilevante strumento di prevenzione.

La materia, già disciplinata in ambito pubblico per le amministrazioni ed enti equiparati (art. 54 bis Dlgs. 165/2001 sul pubblico impiego), è stata ulteriormente disciplinata, anche per il settore privato, dalla legge 179/2017, in vigore dal 29 dicembre 2017 e dalla successiva Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019, recepita dal D.Lgs. 24/2023.

Oltre alle modifiche al citato art. 54 bis, il quale trova applicazione anche ai lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica, l'aspetto più rilevante è l'estensione della tutela in questione anche nell'ambito dei soggetti privati.

Con l'articolo 2bis dell'art. 6 del Dlgs. 231/2001, si stabilisce che, a tutela dell'integrità dell'Ente, i modelli di organizzazione devono prevedere uno o più canali che consentano ai soggetti apicali e/o ai loro sottoposti, come definiti all'Art 5 comma 1 a) e b) del D.lgs 231/2001, di presentare "segnalazioni circostanziate di condotte illecite" rilevanti ai sensi della normativa di cui al Dlgs. 231/2001, "fondate su elementi di fatto precisi e concordanti", o "di violazioni del modello di organizzazione e gestione dell'Ente" di cui siano venuti a conoscenza in ragione delle funzioni svolte.

Tali canali devono garantire al segnalante:

- la presenza di almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
- la possibilità di seguire l'esito della gestione della segnalazione
- il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante stesso per motivi collegati, direttamente o indirettamente, alla segnalazione;

Il diritto alla segnalazione deve essere garantito

- ai soggetti apicali e/o ai loro sottoposti come definiti all'Art 5 comma 1 a) e b) del D.lgs 231/2001
- a qualsiasi persona che lavora sotto la supervisione e la direzione di appaltatori, subappaltatori e fornitori di cui si serve la società (art. 4, par. 1, lett. c) Dir. 2019/1937/UE);
- a chi segnala una violazione avvenuta nell'ambito di un rapporto di lavoro nel frattempo terminato o non ancora formalmente iniziato (art. 4, par. 2 e 3, Dir. 2019/1937/UE).

Nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sono previste 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.

Modalità operativa

Le segnalazioni possono essere presentate secondo diverse modalità.

- missiva cartacea inviata, con dicitura riservata/personale indirizzata all'OdV;
- mail all'indirizzo dell'OdV reso pubblico sul sito internet aziendale;
- funzionalità on line agganciata al sito internet della aziendale che garantisce al contempo l'adeguata gestione della segnalazione e la riservatezza e tutela del segnalante.

Possono essere presentate segnalazioni su:

- eventuali condotte illecite rilevanti ai sensi del D.lgs. 231/2001, basate su elementi di fatto precisi e concordanti;
- violazioni del MOG, ovvero delle procedure ad esso correlate o comunque comportamenti difformi dai principi etici a cui SINTAX si ispira.

Tutte le segnalazioni vengono inoltrate all'OdV. Ricevuta la segnalazione, l'OdV nell'esercizio dei suoi poteri condurrà la propria istruttoria coinvolgendo le funzioni della Società per gli opportuni approfondimenti.

Al termine dell'indagine l'OdV informerà l'Amministratore Delegato dell'esito mediante apposito verbale scritto per i relativi provvedimenti.

Nel caso in cui la segnalazione riguardi l'Amministratore Delegato, l'Organismo di Vigilanza informerà il Consiglio di Amministrazione.

Indipendentemente dal canale scelto. Il segnalante ha diritto all'avviso di ricevimento della segnalazione entro sette giorni dalla ricezione della stessa da parte dell'OdV (art. 9, par. 1, lett. b) Dir. 2019/1937/UE).

In ogni caso, l'OdV è tenuto a conservare tutta la documentazione inerente ad ogni segnalazione ricevuta per il tempo necessario e proporzionato al loro accertamento (art. 16, par. 1 Dir. 2019/1937/UE).

Qualunque sia il canale prescelto, nella gestione della segnalazione, sarà garantita da parte dell'OdV la riservatezza dell'identità del segnalante (art. 6, comma 2 bis, lett. a; art. 16, par. 1 Dir. 2019/1937/UE), nonché la protezione di eventuali terzi nominati all'interno della segnalazione e verrà inoltre impedito l'accesso a tali informazioni da parte di chi non è autorizzato (art. 9, par. 1, lett. a) Dir. 2019/1937/UE).

SINTAX vieta qualsiasi atto di ritorsione o discriminazione, diretto o indiretto, nei confronti del segnalante per motivi collegati direttamente o indirettamente alla segnalazione (art. 6, comma 2 bis, lett. b). Ai fini del MOG per «ritorsione» si intende «qualsiasi omissione o atto, diretto o indiretto, che si verifica in un contesto lavorativo in conseguenza della segnalazione [...] che provoca o può provocare danni ingiustificati alla persona segnalante» (definizione mutuata dall'art. 5 n. 11 Dir. 2019/1937/UE).

Infatti, ferme restando le disposizioni contenute all'art. 6, commi 2-bis, lett. d), 2-ter, del D. Lgs 231/2001 è sottoposto a sanzione disciplinare, chiunque violi l'impegno di riservatezza nella gestione della segnalazione e le cautele conseguentemente adottate, e si riservano altresì ogni opportuna azione disciplinare o legale nei confronti di chi ponga in essere azioni ritorsive o discriminatorie ai danni del segnalante in conseguenza della sua segnalazione (art. 6, comma 2-bis, lett. c)).

La normativa prevede, in particolare, che l'adozione di misure discriminatorie nei confronti del segnalante può essere segnalata all'Ispettorato Nazionale del Lavoro e l'eventuale licenziamento ritorsivo o discriminatorio a carico del segnalante è nullo con la conseguenza della reintegra che sarà disposta dal Giudice. Sono altresì nulli i mutamenti di mansioni, trasferimenti, provvedimenti disciplinari. Sarà onere del Datore di Lavoro dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

Nel caso in cui al termine dell'istruttoria la segnalazione si rivelasse pretestuosa o intenzionalmente falsa saranno presi provvedimenti disciplinari da parte del Datore di Lavoro nei confronti di chi ha avanzato la segnalazione, e, qualora configurasse reato (calunnia), verrà informata l'Autorità Giudiziaria.

Di contro sanziona a livello disciplinare chi, con dolo o colpa grave, effettui segnalazioni che si rivelino poi infondate (art. 6, comma 2-bis, lett. d).