METHISLAB S.P.A.

CORPORATE GOVERNANCE – D.L.VO 231/2001

MODELLO ORGANIZZATIVO E DI GESTIONE

PARTE I

Approvato il **25/07/2022.**

INTRODUZIONE

IL D.L.VO 231/2001

Il D.L.vo 231/2001 è stato emanato per effetto della delega al Governo prevista dalla L. 29/9/2000 n. 300 di recepimento, tra gli altri, della Convenzione relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità europee o degli Stati membri dell'Unione europea, fatta a Bruxelles il 26/5/1997 e della Convenzione OCSE sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali fatta a Parigi il 17/12/1997.

Tale norma ha innovato il principio secondo cui le persone giuridiche non potevano delinquere e, conseguentemente, non potevano essere punite.

I fatti dimostravano che un sistema concernente la criminalità delle imprese, basato e limitato esclusivamente attorno alle persone fisiche, comportava una perdita di garanzia.

La mancata espressa previsione di una forma di responsabilità della persona giuridica, per effetto di comportamenti illeciti commessi dalle persone fisiche, in linea o comunque dipendenti dalla politica aziendale, infatti, determinava, di fatto, l'insensibilità delle persone giuridiche ai deterrenti contenuti nelle norme penali.

Dal 2001 il D.L.vo 231/2001 si è comportato come un "contenitore" ove sono stati collocati, nel tempo, reati socialmente rilevanti, così accanto agli originari reati in danno alle Pubbliche Amministrazioni (malversazione, indebita percezione, truffa, concussione, corruzione), si sono aggiunti i reati di falso nummario, i reati societari, i reati con finalità di terrorismo od eversione dell'ordine democratico …

La responsabilità dell'ente nasce da difetti di organizzazione, tanto che si semplifica definendo la responsabilità dell'ente come l'effetto della deficienza organizzativa.

L'art. 5 della norma definisce l'ambito di responsabilità dell'ente:

"*1. L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:*

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; (Soggetti Apicali)

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a) (Sottoposti).

2. L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi."

Il successivo articolo 6 precisa:

"*1. Se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a)* (Soggetti Apicali), *l'ente non risponde se prova che:*

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 di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;

c) le persone hanno commesso il reato 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)."

Riguardo, poi, i soggetti sottoposti il successivo articolo 7 stabilisce:

"1. Nel caso previsto dall'articolo 5, comma 1, lettera b) (Sottoposti), *l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza.*

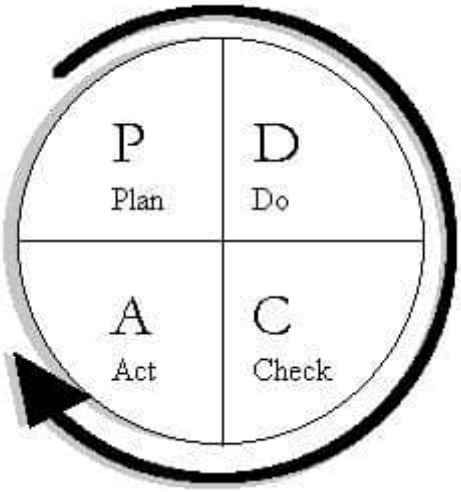
2. In ogni caso, è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.".

L'ente, dunque, per non assumere la responsabilità prevista dalla norma, deve dotarsi di un sistema organizzativo che sia in grado di prevenire e ridurre al minimo la possibilità che siano commessi i reati previsti dalla norma da soggetti Apicali o da sottoposti, deve efficacemente attuarlo, controllarlo ed essere in grado di darne prova.

IL PROCESSO "231"

Col termine "processo 231" si intende il complesso di attività, conoscenze e risorse che sono organizzate tra loro in modo da soddisfare quanto previsto dal D.L.vo 231/2001 onde sollevare l'ente dalla relativa responsabilità.

Si tratta di un processo ciclico che deve essere avviato dall'organo dirigente (Art.6 comma1 lett.a) e, quindi, mantenuto aggiornato ed efficacemente attuato sotto il controllo dell'Organismo di Vigilanza – OdV – (Art.6 comma 1 lett.b).
Il funzionamento del processo può ben essere descritto attraverso il noto ciclo di Deming (che, peraltro, è alla base degli standard di risk management).



Nella tabella che segue sono sintetizzate le macro-attività previste dal processo 231, raggruppate secondo i quattro momenti del Pianificare (Plan), Agire (Do), Controllare (Check) e Reagire (Act) (colonne "fase" e "descrizione"), collegate, attraverso la colonna "chi" al segmento gerarchico dell'ente.

FASE	DESCRIZIONE	CHI
PLAN	PIANIFICARE, ovvero individuare e definire gli obiettivi, elaborare la strategia per il loro conseguimento, organizzare le risorse per darne attuazione.	Questa fase appartiene ai vertici amministrativi e alle dirigenze al loro livello più alto.
DO	FARE, ovvero definire i programmi tattici e curarne l'esecuzione.	Questa fase interessa i livelli gestionali (management) per quanto attiene l'attuazione delle direttive dei vertici (tattica). I livelli più operativi sono infine coinvolti per la concreta attuazione.
CHECK	CONTROLLARE, ovvero verificare il corretto funzionamento dell'ente, monitorare l'osservanza dei modelli (attuazione ed applicazione), controllare l'efficienza, l'adeguatezza, l'attualità e coerenza dei modelli.	Questa fase interessa tutti i livelli per le rispettive aree di competenza: gli operativi per il controllo del rispetto delle procedure, i gestionali per il controllo delle disposizioni tattiche, i vertici per il controllo delle strategie. Partecipano a questa fase l'Organismo di Vigilanza per le specifiche competenze ed il Collegio Sindacale in generale.
ACT	REAGIRE, ovvero adottare tutte le iniziative ed azioni opportune e necessarie sulla base delle verifiche svolte ivi inclusi i provvedimenti disciplinari. Aggiornare i modelli, individuare gli elementi di aggiornamento od aggiustamento di obiettivi, strategie e tattiche.	Questa fase coinvolge, oltre ai vertici ed alle alte dirigenze, anche l'Organismo di Vigilanza in veste meramente consultiva.

IL MODELLO DI ORGANIZZAZIONE E GESTIONE - MOG

Lo schema che segue illustra sinteticamente, relativamente al processo 231, la gerarchia delle fonti ed il sistema documentale adottato dall'ente.

SCHEMA GERARCHIA DELLE FONTI

Il documento che segue è il Modello di Organizzazione e Gestione predisposto ed approvato da Methis Lab S.p.a. in ottemperanza ed in conformità al D.L.vo 231/2001.

Esso si compone delle seguenti parti:

I) la prima parte contiene le enunciazioni di carattere generale e di contenuto programmatico. Essa si divide in due sezioni: la prima sezione è intitolata "Dichiarazioni" in essa sono contenute le informazioni che descrivono l'ambiente in cui è stato sviluppato il MOG, la seconda parte si intitola "Principi" e contiene i principi generali che guidano l'organizzazione dell'ente coerentemente a quanto stabilito nel Codice Etico, e nel rispetto dell'ordinamento giuridico italiano.

II) La seconda parte contiene la parte di analisi e si divide in due sezioni:
   a. la prima intitolata "Ricognizione", contiene i dati, forniti dall'ente, sui quali è stata svolta l'analisi dei rischi.
   b. La seconda sezione, intitolata "Analisi", contiene la parte di analisi dei rischi inclusi gli scenari che individuano la collocazione del rischio all'interno dell'ente.

III) La terza parte contiene gli allegati, ovvero la documentazione rilevante in materia di supporto ad una corretta organizzazione dell'ente e si divide nelle seguenti sezioni:
   a. ETICA, ove sono contenuti i documenti che definiscono i principi etici che guidano in ogni attività l'ente, tra essi il Codice Etico e gli eventuali Codici di Comportamento.
   b. PROCESSO 231, ove sono contenuti i documenti attuativi per la gestione e mantenimento del processo "231", nonché i Rimedi "231" atti a ridurre i rischi individuati.
   c. PROCEDURE DI ATTUAZIONE, ove sono contenute le procedure e la documentazione a livello di gestione ed operativo, rilevanti per la corretta ed efficace attuazione del Modello di Organizzazione e Gestione.

d. SISTEMA DI VIGILANZA, ove sono contenute le disposizioni che regolano la costituzione ed il funzionamento dell'Organismo di vigilanza, con particolare riferimento all'autonomia dell'organismo rispetto gli altri organismi dell'ente.
e. SISTEMA DISCIPLINARE, ove sono contenute le disposizioni rilevanti ai fini del processo "231".

DEFINIZIONI

Qui sono riepilogate, in ordine alfabetico, le definizioni dei termini più significativi utilizzati nel presente documento.

AUTENTICITA', si intende il requisito di sicurezza del Sistema informativo secondo il quale le informazioni devono essere riconducibili a chi le produce o le approva.

DANNO, si intende l'impatto prodotto dall'avveramento di un rischio sull'ente ed i suoi stakeholders.

DATI, si intende ogni informazione nella sua accezione più ampia, indipendentemente dal formato o dal supporto su cui essa è contenuta, sia in forma sciolta che aggregata.

DISPONIBILITA', si intende il requisito di sicurezza del Sistema informativo secondo il quale le informazioni, quando occorrono, devono essere a disposizione di chi ne ha diritto.

INTEGRITA', si intende il requisito di sicurezza del Sistema informativo secondo il quale le informazioni devono essere integre, esatte ed aggiornate.

MINACCIA, si intendono quegli eventi che, associati a debolezze (vulnerabilità) dell'ente, permettono l'avverarsi di un rischio; la minaccia si esprime in probabilità di accadimento.

MODELLO DI ORGANIZZAZIONE E GESTIONE (MOG), si intende il documento che definisce e formalizza gli obiettivi, i principi, i presupposti e le attività organizzative che l'ente, in conformità all'art.6 del D.L.vo 231/2001 adotta ed attua al fine di ridurre al minimo il rischio che soggetti da esso dipendenti (sia Apicali che Sottoposti)

possano commettere reati delle specie previste dal D.L.vo 231/2001 nell'interesse od a vantaggio dell'ente medesimo.

ORGANISMO DI VIGILANZA (OdV), si intende l'organismo dell'ente, dotato di autonomi poteri di iniziativa e controllo, cui l'organo dirigente ha affidato il compito di vigilare sul funzionamento e l'osservanza del MOG e di curarne l'aggiornamento in conformità a quanto previsto dall'art.6 comma 1 lett.b) del D.L.vo 231/2001.

PROCESSO, si intende il complesso di attività e risorse tra loro organizzate al fine di produrre un determinato output partendo da un determinato input.

QUOTE, si tratta del sistema sanzionatorio previsto dall'art. 10 del D.L.vo 231/2001.

RISCHIO, si intende la possibilità che un evento non desiderato si attui arrecando un danno all'ente.

RISERVATEZZA, si intende il requisito di sicurezza del Sistema informativo secondo il quale le informazioni devono essere conosciute solo da coloro che ne hanno diritto.

SISTEMA INFORMATIVO (SI), il complesso delle risorse (risorse umane, tecnologia, applicazioni, infrastrutture, dati) organizzate dall' azienda per il trattamento delle informazioni in genere e dei dati personali in modo specifico.

SISTEMA INFORMATIVO DI VIGILANZA (SIV), il documento che definisce il contenuto delle informazioni che obbligatoriamente devono essere trasmesse all'organismo di vigilanza, individuando compiti e responsabilità.

SOGGETTI APICALI, si intendono le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché le persone che

esercitano, anche di fatto, la gestione ed il controllo dell'ente medesimo, secondo quanto previsto dall'art. 5 comma 1 lett. a) del D.L.vo 231/2001.

SOGGETTI SOTTOPOSTI, si intendono le persone sottoposte alla direzione o alla vigilanza di un soggetto apicale, così come definito dall'art.5 comma 1 lett. b) del D.L.vo 231/2001.

VULNERABILITA', si intende la debolezza dell'ente rispetto specifiche ipotesi di rischio; attraverso tali debolezze le minacce determinano l'avverarsi dei rischi.

PARTE I

SEZIONE I - DICHIARAZIONI

I dati che seguono sono stati ricavati dalle interviste con le persone messe a disposizione dall'ente nonché da documenti forniti dalle stesse sino alla data del **15/04/2022** (data ricognizione)

I.1. ENTE

Methis Lab S.p.a. formalmente adotta e si impegna ad efficacemente attuare il presente Modello di Organizzazione; di seguito è altresì più brevemente denominato "Methis Lab", o genericamente "ente".

Methis Lab S.p.a. ha sede legale in via di Turati 7, Milano (IT) C.F.-P. IVA: 12622421001.

I.2. RAPPRESENTANZA LEGALE

La rappresentanza dell'ente di fronte ai terzi ed in giudizio spetta all' Amministratore Unico la cui carica è attualmente ricoperta dalla Sig.ra Delli Roberta.

I.3. NATURA E DESCRIZIONE

Methis Lab S.p.a. si occupa della prestazione di servizi tecnici, informativi e commerciali in particolare nel settore assicurativo, ovvero della prestazione di servizi di assistenza nella stipula di polizze assicurative e nella gestione delle stesse, elaborazione e controllo dati e documenti tecnici, assuntivi, liquidativi.

Si occupa altresì di intermediazione assicurativa, nel rispetto della normativa vigente e di consulenza tecnica e progettuale per la pianificazione, realizzazione e fornitura di sistemi informatici e telematici finalizzati all'erogazione e allo sviluppo di strategie legate al mondo internet. La società fornisce consulenza e servizi su collegamenti telematici, sia via cavo che via etere, attraverso reti ad-hoc/dedicate o di altri operatori; offre consulenza. progettazione, realizzazione, installazione, gestione, manutenzione, commercializzazione

relativamente a prodotti software, propri o di terzi, e in genere di prodotti telematici e informatici e appliance in qualsiasi moto applicativo; si occupa inoltre di consulenza progettazione, realizzazione di siti internet e portali e del commercio di software e hardware, ivi inclusi supporti, componenti e servizi connessi alle attività precedenti, in tutte le forme consentite dalla legge.

Methis Lab offre servizi di manutenzione hardware, e-commerce di prodotti e servizi e servizi di consulenza anche con riguardo alla formazione, l'addestramento e la riqualificazione professionale, ivi inclusa la modalità e-learning. Si occupa inoltre della organizzazione di seminari, corsi e convegni specializzati e dello studio e della ricerca nell'ambito dei servizi informatici e telematici.

I.4. LA MISSIONE

Methis Lab è costituita da un team di professionisti specializzati nella cessione del quinto e opera come Third Party Administrator per le compagnie di assicurazione che si muovono in questa nicchia.

I valori che contraddistinguono la società sono:

- eccellenza operativa: è l'unica società in Italia verticalizzata nel settore della gestione delle polizze assicurative abbinate ai finanziamenti erogati tramite cessione del quinto. In questi anni ha collaborato con le più grandi compagnie, le ha guidate fornendo loro un supporto costante e competenze specialistiche. Ciò che serve per guadagnare terreno in un settore così di nicchia.
- Competenza del personale: il team lavora insieme da quasi vent'anni, è una squadra coesa, formata da professionisti esperti nell'assunzione e nella gestione del rischio, con una profonda conoscenza del mercato. E' presente una grande passione, altra caratteristica che anima la società.
- Innovazione tecnica: il team IT interno ha sviluppato QuintoHUB, il primo software interamente dedicato alla gestione della cessione del quinto. La piattaforma, di uso esclusivo, garantisce ai clienti un servizio innovativo e accurato.

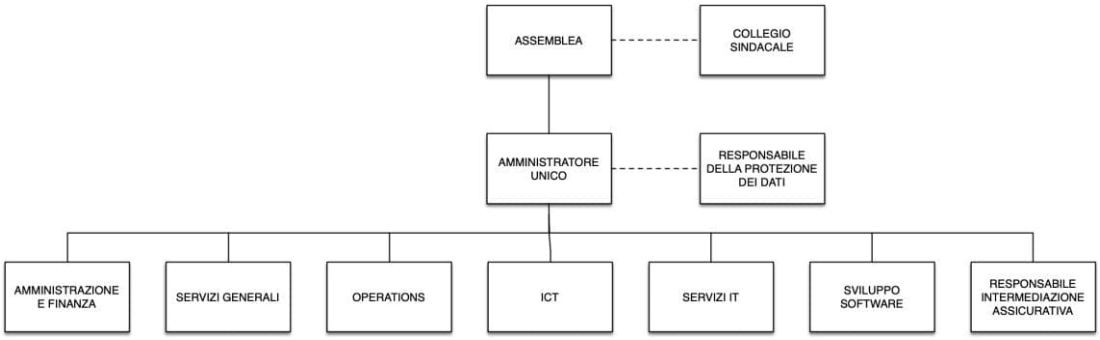
- Centralità del cliente: sono fornite soluzioni che incontrano le singole esigenze delle compagnie. QuintoHUB è progettato per essere utilizzato e gestito non solo dal team di Methis Lab, ma anche dai clienti e dalle banche, che possono monitorare in tempo reale il proprio business. Per questo si è voluto un software che, oltre a garantire soluzioni personalizzate e sicurezza nel trattamento dei dati, fosse anche semplice da utilizzare.

La squadra di Methis Lab garantisce un servizio qualificato ed evoluto, capace di trovare sempre una soluzione su misura.

I.5. AMMINISTRAZIONE

La società è amministrata da un Amministratore Unico che detta le linee di programmazione economica e politica della azienda ed è investito dei più ampi poteri di ordinaria e straordinaria amministrazione.

I.6. MAPPA ORGANIZZATIVA



I.7. CONDIZIONI

L'ente è vincolato all'osservanza, oltre che della vigente normativa europea ed italiana, dello statuto, del codice etico e dei regolamenti interni.

I.8. NORMATIVA

Questo Modello di Organizzazione e Gestione è stato sviluppato e revisionato in conformità al D.L.vo 231/2001 e successive modificazioni ed integrazioni alla data del 31 ottobre 2021.

I.9. STANDARDS DI RIFERIMENTO

Di seguito sono riportati gli standard di riferimento utilizzati per lo sviluppo della presente documentazione:

- Linee guida per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) – UNI-INAIL 2001.
- Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.L.vo 231/2001 – Confindustria 2004.
- ISO/EC 19600:2014 (Compliance management systems -Guidelines) per quanto riguarda i principi di governo del sistema di conformità, base del Modello.
- UNI ISO 31000:2010 (Principi e Linee Guida per la Gestione del Rischio).
- ISO 26000:2010 (Guidance on Social Responsibility).
- ISO/IEC 27001:2013 (Information technology - Security techniques - Information security management systems - Requirements).

I.10. OBIETTIVI DEL MODELLO

La società si propone di ridurre al minimo il rischio che soggetti da esso dipendenti (sia Apicali che Sottoposti) possano commettere reati delle specie previste dal D.L.vo 231/2001, nell'interesse od a vantaggio dell'ente medesimo; ciò al fine di rispettare i principi etici che lo ispirano e lo guidano ed al fine di essere sollevato dalla responsabilità prevista dal citato D.L.vo 231/2001.

I.11. SCOPO DEL DOCUMENTO

Questo documento ha lo scopo di definire e formalizzare i principi, i presupposti, le attività ed i progetti organizzativi, che l'ente intende adottare ed attuare al fine di raggiungere l'obiettivo sopra enunciato.

I.12. ESTENSORI

Questo documento è adottato dall'Amministratore Unico ed è stato predisposto con l'assistenza e consulenza dell'avvocato Alessandro Frillici.

I.13. DATE E TERMINI

Questo Modello Organizzativo e di Gestione è stato sviluppato sulla base delle informazioni alla data del **15/04/2022** (data ricognizione).

Esso è stato approvato dall'Amministratore Unico il **25/07/2022** (Data approvazione) che ne ha disposto l'immediata adozione.

SEZIONE II – PRINCIPI

Questa sezione contiene i principi, che guidano ed ispirano il presente Modello di organizzazione e gestione.

I principi qui elencati devono essere rispettati da tutti coloro i quali operano per conto di Methis Lab S.p.a.

II.1. - ETICITA'

L'adozione di principi etici rilevanti ai fini della prevenzione dei reati previsti dal D.L.vo 231/2001 costituisce elemento essenziale del processo "231".

Methis Lab S.p.a. riconosce l'importanza della responsabilità etico-sociale nella conduzione degli affari e delle attività aziendali impegnandosi al rispetto dei legittimi interessi dei propri stakeholder e della collettività in cui opera.

Non sono etici, e favoriscono l'assunzione di atteggiamenti ostili nei confronti dell'ente, i comportamenti di chiunque, singolo o organizzazione, cerchi di appropriarsi dei benefici della collaborazione altrui, sfruttando posizioni di forza.

In ogni caso il perseguimento dell'interesse dell'ente non può mai giustificare una condotta contraria ai principi di correttezza ed onestà.

II.2. - LEGALITA'

II.2.1. RISPETTO DELLE LEGGI

È condizione imprescindibile di ogni attività dell'ente il rispetto della normativa vigente ed applicabile all'ente. Per normativa si intendono la Costituzione e le Leggi italiane, le disposizioni di pari rango dell'Unione Europea, le Leggi nazionali dei Paesi in cui l'ente opera.

II.2.2. RISPETTO DEGLI OBBLIGHI DI NATURA NEGOZIALE

Methis Lab S.p.a. si obbliga altresì a rispettare scrupolosamente tutti gli obblighi derivatigli da contratti od altri strumenti negoziali di cui è parte. Come pure a rispettare gli altri obblighi legati dal contesto sociale in cui essa opera.

II.2.3. RISPETTO DEL D.l.vo 231/2001

Methis Lab S.p.a. si impegna a ridurre i rischi di commissione dei reati previsti dal D.L.vo 231/2001. La riduzione dei rischi deve essere più bassa possibile ritenendo il rispetto della legge obiettivo prioritario. La revisione ed aggiornamento periodici hanno il fine di restringere il livello di rischio accettabile al più basso possibile e conferire la massima efficacia al Modello di Organizzazione e Gestione.

Il processo "231" è dettagliatamente descritto nella III Parte di questo documento.

II.3. - RIGORE

Le disposizioni del presente documento, come pure le disposizioni di legge o di altra natura che sono vincolanti per l'ente devono essere interpretate in maniera rigorosa avendo come guida i fini primari del presente documento che sono il rispetto dei principi etici e delle leggi.

II.4. - GESTIONE DEI RISCHI

Le attività dell'ente e le scelte conseguenti devono essere condotte con consapevolezza secondo le migliori prassi quali ad esempio lo standard ISO 31000 (Principi e Linee Guida per la Gestione del Rischio).

Nel gestire i rischi deve essere garantito il rispetto oltre che delle leggi degli interessi degli stakeholders[1] E comunque e i rischi devono essere gestiti assegnando chiari e specifici poteri e responsabilità.

[1] Col termine stakeholder si individuano i soggetti sostenitori nei confronti di una iniziativa economica.

II.4.1. ANALISI DEI RISCHI

Ogni attività rilevante dell'ente deve essere preceduta da analisi dei rischi. L'analisi dei rischi deve individuare e descrivere gli scenari di rischio in relazione alla commissione dei reati previsti dal D.L.vo 231/2001 con riferimento alla attività in esame. I ruoli, poteri e responsabilità per le analisi dei rischi devono essere chiaramente e specificamente allocate.

II.4.2. VALUTAZIONE DEI RISCHI

Nella valutazione dei rischi deve essere seguito il massimo rigore, ovvero in caso di indecisione deve essere scelta la soluzione di maggior garanzia tenuto conto dei principi etici e della legge. Il danno deve essere considerato sempre massimo indipendente dai criteri di valutazione qualitativi o quantitativi, poiché la commissione di un reato, seppure lieve, non può essere tollerata. La scelta delle contromisure deve essere effettuata in coerenza preferendo tra le misure quelle che offrono le maggiori protezioni e non secondo criteri di mera economicità.

Il "Rischio accettabile" deve essere valutato conformemente ai superiori principi considerando che il sistema di prevenzione deve essere tale da non poter essere aggirato se non fraudolentemente.

II.5. – CORRETTEZZA E TRASPARENZA

Le informazioni che vengono diffuse dall'ente sono complete, trasparenti, comprensibili ed accurate, in considerazione di coloro che sono i destinatari, in modo che questi ultimi possano assumere decisioni consapevoli.

Le informazioni, in considerazione della propria natura, devono soddisfare adeguati livelli di integrità e di disponibilità; alle informazioni destinate a diffusione o che possono avere impatti rilevanti sull'ente, sulle risorse umane, sugli stakeholder deve essere garantito un idoneo livello di autenticità.

Tutte le azioni e le operazioni compiute ed i comportamenti tenuti coloro che operano per l'ente, nello svolgimento del proprio incarico o funzione, devono pertanto essere

ispirate a trasparenza, correttezza e reciproco rispetto, nonché alla legittimità sotto l'aspetto sia formale che sostanziale, secondo le norme vigenti e le procedure e regolamenti interni e di gruppo.
L'ente ha adottato i principi della Responsabilità Sociale d'Impresa come indicate dallo standard ISO 26000:2011 (Guidance on Social Responsibility).

II.6. – RISERVATEZZA

L'ente, in conformità alle disposizioni di legge, garantisce la riservatezza delle informazioni in proprio possesso, ivi inclusi i dati personali.
A coloro che operano per conto dell'ente è fatto espresso divieto di utilizzare informazioni riservate per scopi non connessi all'esercizio della propria attività professionale anche successivamente alla cessazione del rapporto che li lega all'ente.

II.7. - PROTEZIONE DEI DATI PERSONALI

L'ente, in conformità alla vigente normativa europea e nazionale in materia di protezione dei dati personali, tutela i diritti e le libertà delle persone fisiche interessate dal trattamento dei dati uniformando le proprie attività di trattamento dei dati personali ai principi previsti dal Regolamento Europeo 679/2016.

II.8. – RISORSE UMANE

Il fattore umano costituisce allo stesso tempo la risorsa chiave dell'ente ed è la fonte da cui possono essere commessi i reati da prevenire. Ne consegue che l'ente pone massima attenzione nella gestione delle risorse umane selezionando e mantenendo personale particolarmente qualificato. Particolare attenzione è prestata agli aspetti motivazionali ed alle specifiche esigenze formative, tenendo conto delle potenzialità degli individui e favorendo le condizioni per un ambiente di lavoro propositivo, collaborativo, gratificante e non conflittuale. Ciò nella convinzione che un sano ambiente di lavoro irrobustisce l'ente riguardo le minacce di commissione di reato.

Coloro che operano in nome e/o per conto dell'ente devono svolgere la propria attività lavorativa ed il proprio incarico con impegno professionale, diligenza, efficienza e correttezza, utilizzando al meglio gli strumenti ed il tempo a loro disposizione ed assumendo le responsabilità connesse agli impegni assunti.

L'ente garantisce un adeguato grado di professionalità nell'esecuzione dei compiti assegnati ai propri collaboratori, impegnandosi a valorizzare le competenze delle proprie risorse, mettendo a disposizione dei medesimi idonei strumenti di formazione, di aggiornamento professionale e di sviluppo.

Tutto il personale è assunto con regolare contratto di lavoro, non essendo tollerata alcuna forma di lavoro irregolare e di sfruttamento.

Qualsiasi forma di discriminazione è evitata sia in fase di selezione che in quelle di gestione e sviluppo di carriera del personale; la valutazione dei candidati è basata unicamente sul fine del perseguimento degli interessi aziendali.

Qualsiasi azione che possa configurare abuso d'autorità e, più in generale, che violi la dignità e l'integrità psico-fisica della persona non è tollerata dall'ente.

II.9. - WHISTLEBLOWING

L'ente riconosce il diritto per i soggetti apicali e sottoposti, che prestano la propria opera a suo favore, di segnalare comportamenti scorretti di cui siano venuti a conoscenza alle funzioni di vigilanza, attraverso idonei e sicuri canali di comunicazione che garantiscano la riservatezza delle segnalazioni e senza che ciò possa essere causa di pregiudizio per il segnalante.

In particolare l'ente adotta:

- uno o più canali che consentano a soggetti apicali e sottoposti, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;

- almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
- misure idonee a tutelare l'identità del segnalante e a mantenere la riservatezza dell'informazione in ogni contesto successivo alla segnalazione, nei limiti in cui l'anonimato e la riservatezza siano opponibili per legge.

II.10. - DOCUMENTAZIONE

Ogni operazione, transazione, azione, rilevanti ai fini del D.L.vo 231/2001 (quali ad esempio la documentazione contabile e di sicurezza) deve essere verificabile, documentata, coerente e congrua rispettando i principi di sicurezza del Sistema informativo di seguito meglio specificati.

Il sistema di controllo e vigilanza deve documentare l'effettuazione dei controlli, anche di supervisione; il sotto-processo "documentazione di vigilanza" è parte del processo "231".

La documentazione deve essere prodotta e mantenuta secondo idonei livelli di efficacia probatoria tenuto conto della vigente normativa.

II.11. SICUREZZA

II.11.1. SUL LAVORO

Methis Lab S.p.a. promuove e diffonde la cultura della sicurezza, sviluppando la consapevolezza dei rischi, promuovendo comportamenti responsabili da parte di tutti i dipendenti e collaboratori, al fine di preservarne la salute e la sicurezza.

Methis Lab S.p.a. garantisce un ambiente lavorativo conforme alle vigenti norme in materia di sicurezza e salute mediante il monitoraggio, la gestione e la prevenzione dei rischi connessi allo svolgimento delle attività professionali.

La gestione della salute e della sicurezza sul lavoro costituisce parte integrante della gestione generale dell'ente.

Methis Lab S.p.a. adotta un sistema di gestione della salute e della sicurezza sul lavoro (SGSL) conforme alle linee guida OHSAS 18001.

Il SGSL integra obiettivi e politiche per la salute e la sicurezza nella progettazione e gestione di sistemi di lavoro e di produzione di beni e servizi, definendo le modalità per individuare, all'interno dell'ente, le responsabilità, le procedure, i processi e le risorse per la realizzazione della politica aziendale di prevenzione, nel rispetto delle norme di salute e sicurezza vigenti (D.L.vo 81/2008).
Adeguate risorse sono specificamente allocate per la realizzazione dei principi sopra espressi.

II.11.2. DEL SISTEMA INFORMATIVO

Le informazioni e gli strumenti con cui sono trattate (elettronici e non, inclusi i programmi software) sono una risorsa chiave dell'ente ed allo stesso tempo sono uno dei principali strumenti per la commissione di alcuni dei reati contemplati dal D.L.vo 231/2001 (Reati ai danni delle P.A. Gr. 1 – Reati societari Gr. 3 – Delitti contro la personalità individuale Gr. 6 — Delitti informatici Gr. 10). Per Sistema informativo si intende il complesso delle risorse organizzate ed utilizzate dall'ente per il trattamento delle informazioni, ne consegue che l'ente ritiene prioritaria la protezione del Sistema informativo.
La protezione dei dati personali come prescritto dal Regolamento Europeo 679/2016 e dal Codice della Privacy (D.Lgs. 196/2003 e s.m.i.) è parte integrante della sicurezza del Sistema Informativo.

II.11.3. DELLE RISORSE FINANZIARIE

Le risorse finanziarie sono strategiche per l'ente ed allo stesso tempo sono uno degli strumenti maggiormente interessati dalla commissione di alcuni dei reati previsti dal D.L.vo 231/2001.
L'art. 6 co. 2 lett. c) del D.L.vo 231/2001 prescrive l'obbligo di individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati, a tal fine l'ente si attiene scrupolosamente al rispetto della vigente normativa di settore sottoponendo le suddette attività al controllo incrociato del collegio sindacale e dei revisori dei conti.

II.12 - VIGILANZA ED AGGIORNAMENTO

L'art. 6 co.1 lett. b) D.L.vo 231/2001 prevede l'obbligo di affidare ad un organismo dell'ente, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza del MOG e di curarne l'aggiornamento.

L'ente a tal scopo istituisce ed incarica uno specifico Organismo di Vigilanza, cui ha fornito attribuzioni di competenze e responsabilità in modo da essere dotato di autonomi poteri di iniziativa e di controllo in conformità alla legge.

All'Odv come sopra nominato spetta il compito di controllare il funzionamento e l'osservanza del MOG e di curarne l'aggiornamento.

Il processo "Vigilanza" è meglio definito nella III Parte di questo documento "Sistema di vigilanza" nel rispetto dei principi contenuti nella policy dell'Organismo di vigilanza.

Al fine di garantire l'efficacia ed efficienza del MOG, periodicamente, almeno una volta l'anno, ed anche prima qualora intervengano rilevanti mutamenti organizzativi dell'ente o legislativi, ad iniziativa di chi è incaricato della vigilanza (consiglieri od organismo autonomo) è promossa la revisione ed aggiornamento del MOG medesimo.

Il sotto-processo "Revisione" è parte del processo "231" descritto nella sezione b) della III Parte di questo documento.

II.13 - COMUNICAZIONI

L'art. 6 co. 2 lett. d) del D.L.vo 231/2001 prevede l'obbligo di organizzare un sistema di informazioni nei confronti di chi è tenuto alla vigilanza.

Tale sistema è definito nel sotto-processo "Sistema di informazioni di vigilanza" (SIV) che è parte del processo "231".

Il processo è assegnato ad un responsabile che ha l'onere di garantirne l'efficace attuazione e l'aggiornamento.

Il SIV definisce il contenuto delle informazioni che obbligatoriamente devono essere trasmesse all'Organismo di vigilanza, individuando coloro che devono effettuare le comunicazioni, le modalità ed i tempi.

Le informazioni trasmesse a chi effettua la vigilanza devono soddisfare alti livelli di

integrità, disponibilità, riservatezza ed autenticità.

Devono essere individuati e stabiliti idonei canali di comunicazione verso chi effettua la vigilanza, attraverso i quali tutti coloro che operano per l'ente possano segnalare fatti rilevanti ai fini del D.L.vo 231/2001 (quali ad esempio incidenti di sicurezza, violazioni o sospetto di violazioni delle norme previste dal MOG).

Nel caso in cui la vigilanza sia affidata ad un organismo autonomo deve essere parimenti garantito un efficace sistema di comunicazione verso i vertici dell'ente.

II.14 - FORMAZIONE

L'art. 6 co. 2 lett. b) prevede l'obbligo di definire specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire.

Tutti coloro che operano per conto dell'ente devono essere informati e ricevere formazione sugli aspetti rilevanti della norma, le regole decise dall'ente in materia, le responsabilità e le conseguenze per la mancata osservanza delle regole.

La formazione è elemento primario del sistema di sicurezza e prevenzione dei reati previsti dal D.L.vo 231/2001.

Le attività di formazione devono essere programmate e diversificate tenendo conto delle necessità specifiche dei destinatari.

L'attività di formazione deve essere misurata al fine di verificarne l'efficacia.

Le responsabilità per la formazione devono essere chiaramente attribuite.

La formazione deve essere aggiornata quando intervengono modifiche rilevanti del MOG ovvero quando da controlli sull'efficacia o sui livelli di consapevolezza dei destinatari ne emerga la necessità.

Il sotto-processo "formazione 231" è parte del processo "231" contenuto nella sezione b) della III Parte di questo documento.

II.15 - SISTEMA DISCIPLINARE

L'art. 6 co.2 lett. e) prevede l'obbligo di conformare il sistema disciplinare in modo da renderlo idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il Sistema Disciplinare prevede le azioni da assumere in caso di comportamenti scorretti

rilevanti ai fini del D.Lgs. 231/2001 tenuti da: dipendenti, collaboratori, amministratori e chiunque altro opera in nome o per conto dell'ente.

In particolare:

- per quanto riguarda i dipendenti, coerentemente a quanto previsto dall'art. 7 della L. 300/1970 (Statuto dei lavoratori), le conseguenze disciplinari per il mancato rispetto delle decisioni adottate dall'ente riguardo la conformità al D.L.vo 231/2001 devono essere chiaramente e specificamente formalizzate nel Sistema Disciplinare. Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia è stabilito da accordi e contratti di lavoro di riferimento. Il datore di lavoro non può adottare alcun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa. Le responsabilità per i controlli e per le contestazioni disciplinari devono essere chiaramente e specificamente definite e portate a conoscenza con idonei mezzi a tutti gli interessati.
- Per quanto riguarda gli altri prestatori d'opera, partners, collaboratori, il rispetto dei principi e delle disposizioni di questo modello costituisce grave inadempimento degli obblighi contrattuali e/o convenzionali.

Il Sistema Disciplinare rilevante ai fini del processo "231" è riportato nella III Parte di questo documento.

SOMMARIO