MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO D.Lgs 231

REVISIONE: **06 del 15/12/2025**
APPROVATO DA: **Legale Rappresentante**

Sommario

1. INTRODUZIONE

L'adeguamento della legislazione italiana ad alcune Convenzioni internazionali cui l'Italia ha aderito (Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri e Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali) ha portato all'approvazione del **D.Lgs. 8 giugno 2001, n. 231**, intitolato "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*".

Con questo decreto è stato introdotto nell'ordinamento italiano un regime di responsabilità amministrativa a carico degli Enti (S.r.l., cooperative, associazioni riconosciute, ecc.) per alcuni reati commessi nell'interesse o a vantaggio degli Enti stessi da soggetti che, anche di fatto, ne esercitino la gestione o il controllo, ovvero da loro sottoposti.

La responsabilità amministrativa dell'Ente, che rende possibile l'applicazione delle sanzioni sotto indicate, si basa su una colpa "di organizzazione": l'Ente è ritenuto ugualmente responsabile del reato commesso da un suo esponente se ha omesso di darsi un'organizzazione in grado di impedirne in maniera efficace la realizzazione; in particolare se ha omesso di dotarsi di un sistema di controllo interno e di adeguate procedure per lo svolgimento delle attività a maggior rischio di commissione di illeciti.

Nel decreto legislativo 231/2001, agli artt. 6 e 7 sono indicate le modalità con cui dotarsi di un simile sistema di controllo interno. In particolare, è prevista la realizzazione di un "**modello di organizzazione e gestione**" e la creazione di un **Organismo di Vigilanza** (di seguito anche denominato OdV) interno che provveda al controllo e alla costante verifica dell'efficacia preventiva del modello: tale strada rappresenta la sola condizione esimente dall'applicazione delle sanzioni previste dal decreto stesso.

A tale proposito, **MB Consulting Srl** ritenendo opportuno operare in un contesto di trasparenza e correttezza, ha deciso di dotarsi di un apposito modello che, oltre al rispetto delle prescrizioni del Decreto, tenga conto delle Linee guida emanate da Confindustria e di tutta la normativa successiva, applicabile al D. Lgs 231/2001.

Il presente documento, corredato di tutti i suoi allegati, è il Modello di Organizzazione, Gestione e Controllo (di seguito anche Modello Organizzativo) ai sensi del Decreto Legislativo 8 giugno 2001, n. 231 così come approvato dal Legale Rappresentante in data 04/11/2015, nella sua versione rev. 3 del 01/12/2024.

Aggiornamenti del Modello (successivi alla versione originaria):

- **rev. 1** in data 15.04.2021, a fronte delle modifiche integrative in merito ai reati fiscali ex art 25 quinquiesdecies apportate dall'art. 39 D.L. 124/2019 (decreto fiscale) e dal D.Lgs 75/2020, con ulteriore integrazione dell'art 25 quinquiesdecies D.Lgs. 231/2001, nuovo comma 1 bis in merito ai reati fiscali con sistemi fraudolenti transfrontalieri;
- **rev. 2** in data 16.12.2022, a fronte dell'integrazione degli ulteriori reati presupposto ex art 25 septiesdecies e art. 25-duodevicies ex Legge 9 marzo 2022 n. 22 (art.3).
- **rev. 3** in data 01.12.2023, (*nel rispetto ed applicazione della normativa Direttiva (UE) 2019/1937, D. Lgs 24/2023, Linee operative ANAC e guida operativa Confindustria*) a fronte dell'integrazione della disciplina del Whistleblowing ex D. Lgs 24/2023 che ha previsto l'obbligatoria integrazione nei Modelli ex D. Lgs 231/2001 di un sistema di whistleblowing.
  In fatto, l'Azienda ha adottato un sistema whistleblowing, attivando per tutti coloro i quali sono venuti a conoscenza nel contesto lavorativo di possibili violazioni, alcuni "canali di segnalazione interna" attraverso l'utilizzo della piattaforma digitale Whistlenet, personalizzata ad hoc per MB

Consulting srl (attraverso il link mbconsulting.whistlenet.it/whistle) e di seguito meglio descritta, nominando, al contempo, nella figura del Presidente dell'OdV, il soggetto responsabile della presa in carico e gestione delle varie ed eventuali segnalazioni che potranno essere fatte attraverso il medesimo "canale di segnalazione interna", di seguito anch'esso descritto nel dettaglio.

- **rev. 4 in data 10.12.2024**, con inserimento del sistema WHISTLEBLOWING per la tutela sulla riservatezza del soggetto segnalante introdotta dalla normativa D.Lgs 24/2023
- **rev. 5 in data 10.02.2025** a fronte degli aggiornamenti normativi (Cartabia, PIF, reati IT, contrabbando)

Modello attuale

- **rev. 6 in data 15.12.2025** a fronte della variazione piattaforma whistleblowing

2. IL REGIME DI RESPONSABILITA' AMMINISTRATIVA DELLE PERSONE GIURIDICHE

Si tratta di una responsabilità che, nonostante sia stata definita amministrativa dal legislatore e pur comportando sanzioni di tale natura, presenta i caratteri tipici della responsabilità penale, posto che consegue alla realizzazione di reati ed è accertata attraverso un procedimento penale.
In particolare, gli Enti possono essere considerati "responsabili" ogniqualvolta si realizzino i comportamenti illeciti tassativamente elencati nel D. Lgs. 231/01e ss.mm.ii. (di seguito i "Reati") nel loro interesse o vantaggio da:

- persone fisiche 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 degli stessi (cosiddetti soggetti apicali);
- persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati (cosiddetti soggetti subordinati).

Per quanto attiene alla nozione di "interesse", esso si concretizza ogniqualvolta la condotta illecita sia posta in essere con l'esclusivo intento di arrecare un beneficio alla società.
Parimenti, la "responsabilità amministrativa" incombe su quest'ultima tutte le volte che l'autore dell'illecito, pur non avendo agito al fine di beneficiare l'Ente, abbia comunque portato un vantaggio indiretto alla persona giuridica, sia di tipo economico che non.
Diversamente, il "vantaggio" esclusivo di chi realizza l'illecito esclude la responsabilità dell'Ente.
Per quanto attiene, invece, al requisito della territorialità, la condotta criminosa è rilevante indistintamente dal fatto che essa sia posta in essere sul territorio italiano o all'estero.
La responsabilità amministrativa degli Enti non esclude, ma anzi si somma a quella della persona fisica che ha realizzato l'illecito.

Le sanzioni amministrative irrogabili agli Enti nel caso in cui ne sia accertata la responsabilità sono:

a. Sanzione Pecuniaria

Si applica per qualsiasi illecito amministrativo e può variare nella sua somma finale da un minimo di € 25.822,84 a un massimo di € 1.549.370,70. Nell'ipotesi in cui l'Ente sia responsabile per una pluralità di illeciti commessi con un'unica azione od omissione o comunque commessi nello svolgimento di una medesima attività e prima che per uno di essi sia stata pronunciata sentenza anche non definitiva, si applica la sanzione più grave aumentata sino al triplo;

b. Sanzioni Interdittive

Si applicano per alcune tipologie di illeciti contemplate dal Decreto e per le ipotesi di maggior gravità. Possono essere irrogate anche in via cautelare e si traducono in:

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

c. Confisca del prezzo o del profitto del reato
È sempre disposta con la sentenza di condanna, ad eccezione di quella parte del prezzo o del profitto del reato che può restituirsi al danneggiato;

d. Pubblicazione della sentenza
Può essere disposta quando all'Ente viene applicata una sanzione interdittiva.

3. GLI ILLECITI AMMINISTRATIVI - REATI PRESUPPOSTO

I reati attualmente rilevanti ai sensi del Decreto ed il cui compimento l'Azienda si prefigge di prevenire con l'ausilio del Modello Organizzativo, sono:

- 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. 24);
- Delitti informatici e trattamento illecito di dati (art. 24-bis);
- Delitti di criminalità organizzata (art. 24-ter);
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione (Art. 25);
- Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis);
- Delitti contro l'Industria e il commercio (art. 25-bis 1);
- Reati societari (art. 25-ter);
- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater);
- Pratiche di mutilazione degli organi genitali femminili (art. 25-quater.1);
- Delitti contro la personalità individuale (art. 25-quinquies);
- Abusi di mercato (art. 25-sexies);
- Altre fattispecie in materia di abusi di mercato (Art. 187-quinquies TUF);
- Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies);
- Ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25- octies);
- Delitti in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies.1);
- Delitti in materia di Violazione del diritto d'autore (art. 25-novies);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 25-decies);
- Reati ambientali (art. 25-undecies);
- Impiego di cittadini di Paesi terzi il cui permesso di soggiorno è irregolare (art. 25- duodecies);
- Razzismo e xenofobia (Art. 25-terdecies);
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25-quaterdecies);

- Reati di c.d. criminalità organizzata transnazionale (art. 10 L. 146/2006);
- Reati Tributari (art. 25- quinquiesdecies);
- Contrabbando (art. 25-sexiesdecies);
- Delitti contro il patrimonio culturale (25-septiesdecies);
- Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (25-duodevicies)

4. DESTINATARI DEL MODELLO

Il Modello Organizzativo è indirizzato a tutto il personale (anche quello in stage o in prova) di **MB Consulting Srl** e, in particolare, a quanti svolgano le attività identificate come "a rischio".
Le prescrizioni del presente Modello Organizzativo devono pertanto essere rispettate sia dal Legale rappresentante, e da ogni altro soggetto in posizione apicale, sia da tutti i lavoratori subordinati (personale dirigente, impiegatizio, operaio, ecc.) che operano in nome e per conto della società, cui le disposizioni contenute nel Modello Organizzativo e nel Codice Etico, che si ritiene parte integrante del modello stesso, sono divulgate attraverso specifiche attività di formazione ed informazione.
Sono tenuti altresì al rispetto delle prescrizioni del Modello Organizzativo anche i dipendenti di ogni ordine e grado delle imprese esterne che lavorano presso la MB Consulting Srl, i fornitori, i collaboratori esterni intesi sia come persone fisiche sia come società ed enti, consulenti e partner commerciali.

5. STRUTTURA DEL MODELLO ORGANIZZATIVO

Il presente Modello Organizzativo si compone di una serie articolata di analisi e documentazione di supporto redatte in relazione alle tipologie di reati la cui commissione è astrattamente ipotizzabile nella società, in ragione delle attività svolte. Come già rimarcato al punto 4 deve intendersi come parte del Modello anche il Codice Etico, approvato dal Legale Rappresentante.
Non viene utilizzata la tradizionale suddivisione tra Parte Generale e Parte Speciale, in quanto il Modello Organizzativo viene inteso come il sistema di organizzazione dell'azienda che, oltre a normare l'organizzazione dell'attività aziendale (tramite il Sistema per la Gestione della Qualità, il Sistema di Gestione della Salute e della Sicurezza sul luogo di lavoro, procedure, deleghe ecc.) mira a impedire o contrastare la commissione dei reati da parte degli amministratori o dei dipendenti, sanzionati dal decreto. Il Modello Organizzativo, pertanto, si articola in diverse componenti tra cui, a titolo meramente esemplificativo e non esaustivo: organigramma, procure, deleghe, istruzioni o procedure operative, software, programmi di formazione, report, check list, audit ecc. Alcune componenti sono invece caratteristiche e tipiche delle norme previste nel D.Lgs. 231/2001 quali ad esempio, Organismo di Vigilanza, identificazione e valutazione delle aree sensibili, regolamento disciplinare sanzionatorio, "sistema wistleblowing".)
Alle fattispecie di reato previste ad oggi dal D.Lgs. 231/2001 e dalle sue successive modificazioni ed integrazioni è probabile che nel tempo ne vengano aggiunte altre. Per questa ragione il Legale Rappresentante di **MB Consulting Srl** avrà il potere di adottare apposite delibere per l'integrazione del Modello con l'inserimento di ulteriori procedure nell'ambito del Modello relative alle tipologie di reati che, per effetto di diversi interventi normativi, vengano inserite o comunque collegate nell'ambito di applicazione del D.Lgs. 231/2001.

5.1 Criteri Generali

Secondo l'art. 6 del D.Lgs. 231/2001, anche alla luce delle Linee guida predisposte da Confindustria, il Modello Organizzativo deve mirare a 4 fondamentali finalità:

I) <u>Individuazione e mappatura dei rischi</u>

L'art. 6, comma 2, lett. (a) del D.Lgs. 231/2001 richiede anzitutto che il Modello provveda alla cosiddetta mappatura dei rischi. È necessaria in altri termini, l'analisi della complessiva attività della società e l'individuazione in essa delle fasi operative o decisionali che comportano una possibilità di commissione di atti illeciti ricompresi nel campo di applicazione del D.Lgs. 231/2001. La mappatura dei rischi non è da ritenersi mai definitiva e immodificabile, ma, al contrario, è da ritenersi dinamica e sottoponibile a revisione in ragione dei mutamenti strutturali o di attività della società.

II) <u>Articolazione di un sistema di controllo</u>

Ai sensi dell'art. 6, comma 2 lett. (b) del D.Lgs. 231/2001, una volta compiuta l'attività di analisi di cui sopra e dopo aver selezionato le aree di rischio nell'ambito della complessiva attività della società, è necessario prevedere specifici protocolli (procedure) diretti a programmare la formazione e l'attuazione delle decisioni dell'ente nelle aree di attività a rischio.
Come la mappatura dei rischi anche le procedure ed i rimedi adottati non saranno mai da ritenersi definitivi ma potranno essere oggetto di continua rivalutazione della loro efficacia ed eventualmente immediatamente migliorato qualora si evidenzino carenze o necessità di integrazioni.

III) <u>Designazione dell'Organismo di Vigilanza</u>

Ai sensi dell'art. 6, comma 1 lett. b), la terza finalità è l'individuazione dell'OdV che provveda:

- al controllo costante del rispetto delle prescrizioni del Modello, nonché delle specifiche disposizioni delle misure e delle procedure predisposte in attuazione dello stesso, da parte dei dirigenti e dei dipendenti della società;
- all'attività di valutazione costante e continuativa dell'adeguatezza della mappatura dei rischi e delle procedure descritte ai punti I) e II);
- alla proposta al Legale Rappresentante di tutte le modifiche necessarie per garantire l'efficacia del Modello.

**L'organo in parola (OdV) è collegiale, del tutto autonomo e indipendente.*

IV) <u>Tutela Whistleblowing</u>

Ai sensi dell'art. 6, comma 2 bis, la quarta finalità è la tutela dell'integrità dell'ente, attraverso l'attivazione di canali di segnalazione interna che consentano di presentare segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del D. Lgs 231/2001 e fondate su elementi di fatto precisi e concordanti, o di violazioni del Modello adottato in azienda, di cui si è venuti a conoscenza in ragione delle funzioni svolte nell'ambiente lavorativo.
Tali canali devono essere idonei e garantire la riservatezza, anche con modalità informatiche, dell'identità del segnalante nelle attività di presa in carico e gestione della segnalazione.
Deve anche essere rispettato il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione fatta.
Nel sistema disciplinare del Modello, adottato ai sensi del comma 2, lettera e), devono essere previste delle 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.

5.2 Codice Etico, Protocollo e Procedure

Il Codice Etico contiene le regole di natura etica da osservarsi da parte di tutti i destinatari ivi specificati nell'ambito dell'esercizio delle attività aziendali.
I Protocolli e le Procedure raggruppano tutte le norme interne in grado di pervenire o comunque fortemente ridurre il rischio di commissione di reati: non sono previste procedure specifiche per quelle tipologie di reati, che, in base all'attività di **MB Consulting Srl** non possono nemmeno in astratto essere commessi.
Il Codice Etico e tutti i protocolli (procedure) sono parte integrante del Modello Organizzativo.

6. PRINCIPI DI ADOZIONE

MB Consulting Srl, anche al fine di ribadire le condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, ha adottato il presente Modello Organizzativo, con il chiaro obiettivo di:

- adeguarsi alla normativa sulla responsabilità amministrativa degli Enti, ancorché il Decreto non ne abbia imposto l'obbligatorietà;
- verificare e valorizzare i presidi già in essere, atti a scongiurare condotte illecite rilevanti ai sensi del Decreto;
- informare tutto il personale della portata della normativa e delle severe sanzioni che possono ricadere sulla stessa nell'ipotesi di perpetrazione dei Reati;
- informare tutto il personale dell'esigenza di un puntuale rispetto delle disposizioni contenute nel Modello Organizzativo stesso, la cui violazione è punita con severe sanzioni disciplinari;
- informare i collaboratori esterni, i consulenti ed i partner della portata della normativa nonché dei principi etici e delle norme comportamentali adottate dalla Società ed imporre agli stessi il rispetto dei valori etici cui si ispira l'Azienda;
- informare i collaboratori esterni, i consulenti ed i partner delle gravose sanzioni amministrative applicabili alle società nel caso di commissione degli illeciti di cui al Decreto;
- compiere ogni sforzo possibile per prevenire gli illeciti nello svolgimento delle attività sociali, mediante un'azione di monitoraggio continuo sulle aree a rischio, attraverso una sistematica attività di formazione del personale sulla corretta modalità di svolgimento dei propri compiti e mediante un tempestivo intervento per prevenire e contrastare la commissione degli illeciti.
- in osservanza e applicazione della disciplina ex D. Lgs. 24/2023, adottare un sistema *whistleblowing*, ossia attivare idonei "canali di segnalazione interna" volti a garantire la tutela e la riservatezza delle segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del D. Lgs 231/2001 o del Modello stesso e fondate su elementi di fatto precisi e concordanti, o di violazioni del Modello adottato in azienda, di cui si è venuti a conoscenza in ragione delle funzioni svolte nel contesto lavorativo.

6.1 Implementazione del Modello Organizzativo

Il Modello Organizzativo è stato predisposto, come già ribadito precedentemente, tenendo presenti, oltre alle prescrizioni del D.Lgs. 231/01, le Linee guida elaborate in materia da Confindustria, nonché ogni altra disposizione applicabile alla Società.
Si descrivono qui di seguito, brevemente, le fasi in cui si è sviluppato il lavoro di costruzione del presente Modello Organizzativo.
La prima fase ha riguardato l'esame della documentazione aziendale disponibile presso le Direzioni rispettivamente competenti (procedure e regole interne di comportamento, organigrammi,

elementi relativi alle sanzioni disciplinari previste dai C.C.N.L. applicabili, etc.) al fine della comprensione del contesto operativo interno ed esterno di riferimento per **MB Consulting Srl**.
Sulla base dell'analisi della documentazione raccolta e tramite interviste ai Responsabili di Direzione e di Funzione, si è proceduto all'individuazione delle principali attività svolte.
Sono state, quindi, identificate le aree ritenute a rischio di commissione di reati e i processi a queste strumentali: con dette espressioni s'intendono, rispettivamente, le attività il cui svolgimento può dare direttamente adito alla commissione di una delle fattispecie di reato (aree a rischio) e i processi nella cui esecuzione, in linea di principio, potrebbero configurarsi le condizioni, le occasioni o i mezzi per la commissione dei medesimi illeciti (processi strumentali).
Sulla base della mappatura effettuata e dei meccanismi di controllo in essere, è stata eseguita un'analisi intesa a valutare il sistema dei controlli esistente, ossia l'attitudine a prevenire o individuare comportamenti illeciti quali quelli sanzionati dal D.Lgs. 231/2001. Sono state, quindi, definite le esigenze di allineamento dei meccanismi di controllo in essere rispetto a ciascuna delle aree a rischio reato e/o strumentali identificate.
L'elaborazione del Modello Organizzativo, oltre alla stesura del presente documento ed alla predisposizione del Codice Etico, ha contemplato un riesame del sistema dei poteri, verificando che esso rispetti i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli, attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.
A conclusione delle attività, sono state identificate le procedure, con riferimento alle aree individuate a rischio di reato. Dette procedure contengono la disciplina ritenuta maggiormente idonea a governare il profilo di rischio ravvisato: si tratta, pertanto, di un insieme di regole di comportamento, nonché di modalità operative cui le varie funzioni aziendali devono adeguarsi, con riferimento all'espletamento delle attività a rischio.
In particolare, le procedure identificano:

1. la segregazione funzionale delle attività operative e di controllo;
2. la documentabilità delle operazioni a rischio e dei controlli posti in essere per impedire la commissione dei Reati;
3. la ripartizione ed attribuzione dei poteri autorizzativi e decisionali, delle responsabilità di ciascuna struttura, basate su principi di trasparenza, chiarezza e verificabilità delle operazioni.

6.2 Profili di Rischio

La costruzione del presente Modello Organizzativo ha preso l'avvio da una puntuale individuazione delle attività poste in essere da **MB Consulting Srl** e dalla conseguente identificazione dei processi societari sensibili alla commissione dei reati.
MB Consulting Srl è uno studio di consulenza alle imprese che opera nell'ambito di **tre dipartimenti:**

1. Dipartimento "Formazione"

L'attività svolta riguarda il sostegno professionale per favorire la crescita professionale e l'ottimizzazione delle risorse messe a disposizione per finanziare la formazione continua delle imprese con i **Fondi Interprofessionali e/o Regionali-Nazionali oppure in modalità diretta a pagamento con corsi a Catalogo o progettati ad hoc.**
Le principali macro-attività possono riguardare:

- Analisi e Profilazione dei fabbisogni aziendali
- Individuazione delle fonti di finanziamento
- Progettazione e Monitoraggio di pacchetti formativi
- Coordinamento e Tutoraggio
- Organizzazione e Gestione di piani strutturati

- Predisposizione delle pratiche burocratiche per la presentazione, rendicontazione e certificazione di Piani

2. Dipartimento "Incentivi"

L'attività svolta riguarda il supporto professionale per sostenere gli investimenti delle imprese con servizi di analisi, gestione e rendicontazione di progetto nel rispetto degli incentivi più funzionali e strategici scelti ed applicati. Il servizio riguarda l'area dei principali bandi nazionali e di Regione Lombardia ma soprattutto **l'ambito Impresa 4.0 e 5.0** con il focus sui **crediti di imposta per i piani formativi 4.0 e 5.0, per gli investimenti in beni strumentali 4.0, per i progetti di Ricerca e Sviluppo e Innovazione 4.0 (R&S&I) e per i progetti legati alla Transizione 5.0.**

Il Dipartimento INCENTIVI opera in ambito di «finanza agevolata» che è uno degli strumenti finanziari a disposizione delle imprese per sostenere investimenti e sviluppare l'attività.

Tra i servizi offerti rientrano in questo dipartimento: Bandi Vari, Beni strumentali, Formazione 4.0 e 5.0, Mix 4.0, Transizione 5.0.

Le principali macro-attività possono riguardare:

- Personalizzazione del servizio in base alle caratteristiche dell'impresa e al panorama legislativo al fine di definire "progetti ad hoc"
- Individuazione degli incentivi
- Analisi dei requisiti, studio e verifica di fattibilità
- Progettazione e definizione del progetto ad hoc d'investimento/di spesa
- Predisposizione della pratica
- Organizzazione, gestione e rendicontazione del progetto ad hoc

3. Dipartimento "Consulenza"

L'attività svolta riguarda la consulenza e il sostegno professionale per sostenere le imprese e/o i professionisti nell'ambito della **certificazione** dei crediti d'imposta, nell'elaborazione di **perizie,** nel servizio di **audit 4.0** e nell'affiancamento all'ottenimento di requisiti di legge.

Tra i servizi offerti rientrano in questo dipartimento: Audit R&S&I 4.0, Certificazione crediti 4.0 e Perizie beni 4.0.

Le principali macro-attività possono riguardare:

- Servizio di Audit ex ante (in via precauzionale) e/o ex post (in risposta all'Agenzia delle Entrate), con attività di analisi e verifica dell'impostazione progettuale e della documentazione del progetto di R&S&I 4.0 con l'obiettivo di verificare rispettivamente la sussistenza e/o la corrispondenza dei requisiti di legge ed accertarne la relativa correttezza e completezza in merito all'aspetto tecnico progettuale ed economico.
- Attività consulenziale di certificazione dei crediti 4.0 tramite di revisori legali dei conti aderenti alla rete, con coordinamento e supporto al revisore da parte del team MBc.
- Attività consulenziale tecnico peritale delle spese sostenute per tramite di periti aderenti alla rete, con coordinamento e supporto al perito da parte del team MBc.

Si segnala che in alcuni casi il suddetto Dipartimento Consulenza ha alcuni punti di incontro e coinvolgimento reciproco con il Dipartimento Incentivi e Dipartimento Formazione, al fine di fornire all'Impresa interessata un servizio completo di "Global service".

Oltre ai suddetti dipartimenti, MB Consulting Srl in qualità di Impresa di riferimento del Contratto di Rete "RETICA", svolge alcune attività consulenziali e operative, nel ruolo di Project Manager, rispetto ad alcuni servizi erogati dalla Rete.

Lo svolgimento delle attività di cui sopra implica uno stretto rapporto con soggetti privati e pubblici di seguito elencati:

Soggetti privati:

- **AZIENDE** (tra cui società di servizi e aziende prevalentemente manifatturiere in ambito lombardo, ma non solo). Le aziende sono i **CLIENTI** dello studio che si avvalgono dei servizi di MB Consulting Srl al fine di ottenere contributi, finanziamenti agevolati e/o crediti d'imposta a copertura dei costi sostenuti per la realizzazione di piani formativi o investimenti aziendali.
- **STUDI PROFESSIONALI** (in prevalenza enti formativi, consulenti, revisori). Gli studi professionali e/o le società di consulenza sono i PARTNER dello studio con cui la MB Consulting Srl crea delle sinergie e delle collaborazioni al fine di erogare un servizio completo "chiavi in mano" sia in ambito formativo che agevolativo.

Lo studio si interfaccia nello svolgimento delle sue attività/servizi erogati alle aziende clienti con i seguenti enti pubblici:

- **REGIONE LOMBARDIA** (in prevalenza Direzione Generale Istruzione, Formazione e Cultura.) La Regione Lombardia, attraverso le diverse Direzioni Generali, emana dei bandi/Avvisi pubblici al fine di sostenere le aziende nella realizzazione di progetti di investimento, sia in ambito formativo che in ambito trasversale (ricerca e sviluppo, innovazione, trasformazione digitale, internazionalizzazione, sviluppo ed efficientamento produttivo, ecc.)

MB Consulting Srl si interfaccia con gli uffici regionali per poter conoscere e gestire i diversi strumenti agevolativi da proporre alle aziende. Segue tutto l'iter burocratico per la presentazione della pratica, monitora lo stato in fieri della pratica fino all'erogazione dell'agevolazione.

MB Consulting Srl si interfaccia nello svolgimento delle sue attività/servizi erogati alle aziende clienti con i seguenti soggetti privati a partecipazione pubblica:

- **FONDI INTERPROFESSIONALI** (in prevalenza Fondimpresa, Fondirigenti, Fonarcom E Fonservizi). I Fondi Interprofessionali, ognuno nel rispetto delle proprie Linee Guida, emanano dei bandi/Avvisi pubblici al fine di sostenere le aziende aderenti nella realizzazione Piani Formativi per i propri dipendenti.

MB Consulting Srl si interfaccia con i Fondi per poter conoscere e gestire i diversi strumenti agevolativi da proporre alle aziende. Segue l'iter burocratico per la presentazione della pratica, monitora lo stato in fieri della pratica fino all'erogazione dell'agevolazione.

MB Consulting Srl si interfaccia inoltre con i seguenti soggetti datoriali/sindacali:

- **RAPPRESENTANZE DATORIALI** (in prevalenza Assolombarda, Confindustria Brescia, Confindustria Monza e Brianza, Confindustria Bergamo Unione Degli Industriali)
- **RAPPRESENTANZE SINDACALI** (in prevalenza CIGL, CIS, UIL, Federmanager, Manager Italia)

Le rappresentanze datoriali e sindacali, in riferimento ai Fondi Interprofessionali, hanno costituito delle commissioni finalizzate a valutare i progetti formativi aziendali con lo scopo di condividere i Piani prima che siano presentati ai rispettivi fondi.

MB Consulting Srl si interfaccia con le diverse commissioni, costituite in base alle rappresentanze e al territorio, per presentare e condividere i piani formativi che le aziende clienti intendono presentare ai fondi a cui sono aderenti. Segue l'iter burocratico per la presentazione della pratica alla commissione fino alla firma di condivisione.

Di recente, MB Consulting Srl è anche proprietaria della PIATTAFORMA DIGITALE INNOVATIVA, denominata «MY MATRIX»: piattaforma ideata, progettata e sviluppata internamente, regolarmente

registrata alla SIAE - Registro pubblico speciale per i programmi per elaboratore. La registrazione è stata effettuata in data 12/11/2021 con n. progressivo: D000016560, n. registrazione: D000015618.

MYM come PIATTAFORMA DEL SAPERE che consente di codificare il sapere, di mappare le opportunità, strutturare i servizi, ricercare gli incentivi per fornire alle aziende e ai professionisti risultati concreti e proporre le soluzioni più adatte alle diverse esigenze in modo semplice, rapido ed efficiente.

7. MAPPATURA DEI RISCHI - PROCEDURE E PROTOCOLLI PER ELIMINARE O RIDURRE IL RISCHIO DI COMMISSIONE DEI REATI

In ragione della specifica operatività dell'Azienda, si sono quindi ritenuti rilevanti o potenziali i rischi di commissione dei reati come dettagliati di seguito:

1. **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.**

Aree sensibili	**Operazioni a rischio commissione reato**	**Livello di rischio**
Direzione Generale	**MB Consulting Srl** presenta piani complessi in ATS con altri enti a valere su bandi/Avvisi pubblici e se ammesso in graduatoria riceve agevolazioni per realizzare piani formativi a benefici di aziende aderenti; quindi, potrebbe incorrere nel reato di cui al punto	2
Legale rappresentante		2
Amministrazione, gestione risorse umane, dipartimenti interessati		2

Legenda:1=rischio basso – 2=rischio medio – 3= rischio alto

Procedure e protocolli per eliminare o ridurre il rischio di commissione dei reati

Al fine di eliminare o comunque ridurre il rischio di commissione dei reati presupposto, la società ha elaborato ed adottato i seguenti protocolli e procedure:

Divieto di adesione ad un bando/avviso per finanziamento pubblico e/o predisposizione della relativa documentazione in autonomia da parte di un solo operatore: il soggetto che intrattiene rapporti con soggetti pubblici non può da solo e liberamente decidere l'adesione ad un bando rispetto al quale ha curato la fase istruttoria ovvero predisporne la documentazione senza la condivisione con la Direzione.

Autorizzazione formalizzata: l'adesione ad un bando o finanziamento pubblico, avverrà solo sulla base di apposita delega e/o autorizzazione formalizzate.

Documentazione: tutta la documentazione relativa alla progettualità per la richiesta e l'ottenimento di agevolazioni o contributi, formerà oggetto di attività di controllo - Audit interni ed attività dell'Organismo di Vigilanza. (PIANO CONTROLLI ANNUALI).

Riferimento: Procedura Sistema Gestione Qualità e Codice Etico Aziendale.

2. **Art. 24-bis Delitti informatici e trattamento illecito di dati**

L'azienda accede a sistemi informatici di pubblica utilità per quanto concerne le procedure di partecipazione a Bandi/avvisi e in relazione alla normale attività aziendale (Agenzia entrate per

modello F24, comunicazione di assunzione personale dipendente ecc.). In considerazione della crescente pervasività e vulnerabilità dei sistemi informatici e della progressiva informatizzazione della P.A. l'azienda ritiene, in via cautelativa, di considerare come potenzialmente applicabile tale fattispecie di reato. Sono state previste apposite procedure di prevenzione di tali reati; l'accesso ai sistemi informatici risulta comunque già regolato da password personali, autenticazione dell'utente autorizzato, il tutto gestito dal responsabile aziendale. L'azienda in materia di cybersecurity ha implementato ulteriormente i sistemi di accesso e sicurezza ai dati e informazioni aziendali. L'azienda utilizza server iperconvergenti Syneto HYPERSeries HSA-2111 per la gestione della virtualizzazione e del Disaster Recovery, garantendo backup giornalieri e settimanali delle macchine virtuali critiche. Inoltre, in materia di cybersecurity sono stati implementati ulteriormente i sistemi di accesso e sicurezza ai dati e informazioni aziendali

Aree sensibili	**Operazioni a rischio commissione reato**	**Livello di rischio**
Direzione Generale	Utilizzo di reti informatiche e Pc; criterio di assegnazione e gestione delle password di accesso al sistema e modalità di trattamento dei dati all'interno del sistema. **MB Consulting Srl** gestisce sia i dati aziendali che i dati dei dipendenti delle aziende clienti	2
Legale rappresentante /Responsabile commerciale		2
Amministrazione e gestione risorse umane		2
Ufficio IT		3
Logistica ed ufficio acquisti		2
Qualità e sicurezza		2
Service		2
Produzione/Assistenza		2

Legenda:1=rischio basso – 2=rischio medio – 3= rischio alto

Procedure e protocolli per eliminare o ridurre il rischio di commissione dei reati

Come precedentemente indicato, al fine di eliminare o comunque ridurre il rischio di commissione dei reati presupposto indicati, la società ha elaborato ed adottato la procedura denominata **"REGOLAMENTO UTILIZZO PC, INTERNET E POSTA ELETTRONICA"** che viene di seguito riportato integralmente, nonché la corretta applicazione delle disposizioni previste dal D.Lgs. 196/03 - Codice Privacy.

Regolamento Aziendale Utilizzo Pc, Internet e Posta Elettronica "Le linee guida del Garante per posta elettronica e internet"

MB Consulting Srl ha adottato una serie di misure di sicurezza interne, al fine di proteggere le proprie informazioni e dati aziendali, per evitare possibili Data Breach. In ambito web le comunicazioni e lo scambio di informazioni sono protetti grazie all'utilizzo di protocolli di sicurezza crittografati TLS/SSL che garantiscono privacy e integrità dei dati.

Si segnala che, a fronte dell'utilizzo dello smart working da parte dei propri dipendenti e collaboratori, la società **MB Consulting Srl** ha potenziato il proprio sistema di sicurezza "cyber security", volto ad impedire l'accesso non consentito e la diffusione illecita dei dati e, a tal fine, ha assunto ulteriori misure di accesso e protezione dei dati aziendali.

L'accesso "da remoto" al sistema VPN contenente tutti i dati aziendali, consentito tramite apposite credenziali, è protetto con un'ulteriore misura di accesso, consistente in un codice identificativo, generato in automatico ed inviato sul telefono mobile del dipendente, ogni volta che questo, lavorando in modalità smart working, vorrà accedere al sistema VPN da remoto. A tal fine è stata implementata una VPN utilizzando *OpenVPN GUI* per potenziare la sicurezza e migliorare l'efficienza dell'accesso remoto alle risorse aziendali. Questa soluzione consente ai dipendenti, in particolare a coloro che lavorano in modalità smart working, di connettersi alla rete aziendale in modo sicuro da qualsiasi luogo, garantendo operatività e protezione dei dati sensibili. Il sistema include anche un'autenticazione a due fattori (2FA), che richiede un codice di verifica dinamico generato da Google Authenticator, incrementando così il livello di sicurezza. Per accedere, ogni dipendente autorizzato deve inserire le proprie credenziali personali insieme al codice 2FA; una volta verificati, OpenVPN stabilisce una connessione sicura e crittografata.
Il presente Regolamento disciplina i termini e le modalità di utilizzo dei sistemi informatici messi a disposizione dal titolare del trattamento dei dati, MB Consulting Srl, ai propri dipendenti e collaboratori, nonché i termini e le modalità di accesso e utilizzo della rete Internet e della posta elettronica tramite i suddetti sistemi.
L'utilizzo delle tecnologie informatiche e l'accesso alla rete Internet espongono il datore di lavoro e gli utenti (dipendenti, collaboratori e assimilabili) a rischi di natura patrimoniale e/o penale, oltre ad incidere concretamente sui profili organizzativi e di sicurezza dell'azienda.
Il Regolamento interno sull'utilizzo dei sistemi informatici detta le condizioni per il corretto utilizzo degli strumenti informatici da parte dei lavoratori della società nel rispetto dei principi di diligenza e correttezza nel rapporto di lavoro, consapevoli degli utilizzi consentiti, delle legittime forme di controllo previste, e delle eventuali relative sanzioni disciplinari.
Le prescrizioni di seguito previste si aggiungono e integrano le istruzioni e procedure previste dal D.Lgs. n. 196/2003 - Codice Privacy.

1. Ambito di applicazione del Regolamento

1.a Il presente Regolamento si applica a tutti i dipendenti e collaboratori a qualsiasi titolo del Titolare, **MB Consulting Srl** (dipendenti, lavoratori c.d. "interinali", collaboratori a progetto, stagisti, apprendisti ecc.), - di seguito denominati "utenti" – i quali siano autorizzati, tramite l'assegnazione di specifiche credenziali di autenticazione, all'accesso alla rete e all'utilizzo di sistemi informatici forniti dal Titolare, **MB Consulting Srl** - di seguito denominato "datore di lavoro".
1.b Il datore di lavoro **MB Consulting Srl** è Titolare del Trattamento ai sensi del D.Lgs. n. 196/2003.

2. Utilizzo del Personal Computer

2.a Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è pertanto vietato in quanto potrebbe, tra l'altro, cagionare disservizi, costi di manutenzione e dar luogo a minacce alla sicurezza del sistema informatico della società. Sono fatte salve le azioni consentite dal presente Regolamento.
2.b L'utente è tenuto a custodire con cura il Personal Computer, evitando ogni possibile forma di danneggiamento, e ricorrendo esclusivamente al Responsabile IT ed Amministrativo che provvederanno, ciascuno per la propria competenza, a provvedere alla riparazione oppure a contattare la società di servizi che si occupa della manutenzione dell'hardware aziendale ove ravvisasse anomalie nel funzionamento.
2.c Il Personal Computer affidato all'utente permette l'accesso alla rete informatica aziendale solo attraverso specifiche credenziali di autenticazione, conferite dal titolare del trattamento dei dati

personali, con l'indicazione delle modalità di conservazione e utilizzo contenute nella relativa lettera di incarico.

2.d Le Società incaricate dell'assistenza hardware e software, unitamente al Responsabile IT, sono gli unici autorizzati a compiere interventi nel sistema informatico aziendale al fine di verificare e garantire la sicurezza e la salvaguardia del sistema stesso, nonché per motivi tecnici e/o manutentivi (come aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware ecc.). Tali interventi potranno anche comportare l'accesso ai dati trattati da ciascun utente nell'esercizio della propria attività professionale in relazione e conformemente alla lettera d'incarico di cui alla normativa Privacy, nonché l'accesso e il trattamento di dati riferibili all'utente stesso contenuti negli strumenti informatici da parte dell'utente e/o desumibili dall'utilizzo degli stessi, ivi compresi gli archivi di posta elettronica e la visualizzazione dei siti internet acceduti dall'utente. La stessa facoltà, ai fini della sicurezza del sistema e/o al fine di garantire la normale operatività dell'Azienda, potrà essere esercitata, ove necessario, anche in caso di assenza prolungata od impedimento dell'utente.

2.e È vietato installare dispositivi di memorizzazione (pen drive, hard disk esterni e simili) o altre periferiche (masterizzatori, cellulari e simili) anche diversi da quelli forniti insieme al PC, al fine di importare nella macchina fornita contenuti inerenti all'attività lavorativa. In caso di necessità l'utente dovrà rivolgersi al Responsabile IT.

2.f Al fine di agevolare e rendere più rapida ed efficiente la comunicazione all'interno dell'azienda o con soggetti esterni, comunque per ragioni inerenti alla prestazione professionale, è consentito all'utente utilizzare software di comunicazione istantanea (chat) come, a titolo esemplificativo, Teams, messenger e skype. L'utente avrà cura di inserire, accettare e conservare tra i propri contatti solo soggetti appartenenti alla struttura organizzativa aziendale, collaboratori, consulenti, clienti e fornitori.

2.g Il Personal Computer deve essere spento al termine di ogni turno di lavoro, prima di lasciare l'ufficio. Nel caso in cui l'utente durante l'orario di lavoro si allontani dalla postazione affidata in modo tale da non poter esercitare su di essa un controllo diretto, è tenuto a disconnettere il PC dalla rete aziendale, reintroducendo le credenziali di autenticazione al momento della ripresa dell'utilizzo del PC. Si sottolinea che lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

3. Navigazione in Internet

3.a Il PC assegnato al singolo utente e abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi consentita la navigazione in Internet per motivi e finalità legati all'attività lavorativa ed all'espletamento delle mansioni assegnate.

È in ogni caso rimandato alla correttezza e diligenza dell'utente di utilizzare la navigazione in Internet in modo congruamente inerente all'attività lavorativa.

3.b È consentito all'utente l'accesso a siti di webmail per l'utilizzo di posta elettronica privata. L'utente è tenuto a ricorrere con moderazione e senza abuso a tale facoltà concessa dal datore di lavoro, e comunque in modo che non sia compromessa, limitata, condizionata e in alcun modo diminuita la prestazione professionale. Qualora si inviassero o ricevessero allegati pesanti l'utente utilizzerà per l'invio di essi formati compressi tramite software fornito dall'azienda, richiedendo ove possibile l'utilizzo di formati compressi anche al mittente di posta in entrata. Nel caso di mail provenienti da mittenti sconosciuti contenenti messaggi insoliti l'utente deve provvedere all'eliminazione senza aprirli. Nel caso di mail provenienti da mittenti conosciuti contenenti file allegati con estensioni e/o messaggi insoliti, l'utente deve provvedere all'eliminazione dei messaggi senza aprirli.

3.c Transazioni finanziarie online, operazioni in remoto di home banking, acquisti online e simili sono effettuabili solo ed esclusivamente per finalità lavorativa dal personale incaricato che presta attività lavorativa presso la sede, tramite account e procedure autorizzate dal datore di lavoro.
3.d Sono consentite la registrazione e la partecipazione a forum, community, blog e simili purché di contenuto inerente all'attività lavorativa e funzionali all'attività svolta nell'azienda.
3.e Sono vietati l'upload ed il download di software gratuiti (freeware) e shareware, di documenti, contenuti, file di qualsiasi estensione dai siti accessibili per finalità lavorative

4. Utilizzo della posta elettronica aziendale

4.a Agli utenti è messo a disposizione un account di posta elettronica. La casella di posta elettronica assegnata all'utente è uno strumento di lavoro e di uso esclusivamente aziendale. Qualora ritenuto rispondente alle necessità aziendali, il datore di lavoro autorizza la creazione di account di posta elettronica individuali a uso esclusivo dei singoli utenti. Resta inteso che in tal caso l'account di posta elettronica conferito all'utente è individuale ma non "privato" e pertanto destinato ad un uso legato esclusivamente all'attività lavorativa e a finalità professionali. Gli utenti possono servirsi di strumenti di comunicazione (es. Teams e Sistemi di web conferencing – Go To Meeting).
4.b È vietato utilizzare l'account di posta elettronica di servizio per motivi e finalità non inerenti all'attività lavorativa, per comunicazioni private, per scambio di file ecc.
4.c È consentito l'invio in allegato e la ricezione di file per finalità legate ed inerenti all'attività professionale.
In tal caso, qualora gli allegati siano pesanti, l'utente utilizzerà per l'invio di essi formati compressi tramite software fornito dall'azienda o piattaforme di trasferimento file, richiedendo ove possibile l'utilizzo di formati compressi anche al mittente di posta in entrata nell'account aziendale.
4.d Nel caso di mail provenienti da mittenti sconosciuti contenenti messaggi insoliti l'utente deve provvedere all'eliminazione dei messaggi senza aprirli.
4.e Nel caso di mail provenienti da mittenti conosciuti contenenti file allegati con estensioni insolite, l'utente consulterà il Responsabile IT, che provvederà ad autorizzare l'apertura del messaggio e del file o ne ordinerà la cancellazione senza aprirli.
4.f La casella elettronica deve essere mantenuta in ordine, cancellando documenti inutili e allegati ingombranti, qualora non più necessari per l'espletamento dell'attività lavorativa.
4.g Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica di servizio, i messaggi in uscita devono contenere un avvertimento standardizzato, fornito dall'azienda, nel quale sia dichiarata la natura non privata dei messaggi stessi, precisando che, pertanto, il personale debitamente incaricato dal Titolare del trattamento, rispettando le procedure di cui al punto 6 del presente Regolamento, potrà accedere al contenuto della corrispondenza in entrata e in uscita dall'account di posta elettronica aziendale.
4.h Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto dei principi di necessità e proporzionalità, in caso di assenze non programmate superiori a due giorni, il titolare/amministratore di sistema, potrà accedere alla casella di posta elettronica per l'esclusiva finalità di garantire la normale operatività dell'azienda e/o per motivi tecnici e manutentivi.

5. Protezione antivirus

5.a Il sistema informatico aziendale è protetto da software antivirus regolarmente aggiornato. L'utente è tenuto comunque a comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale tramite virus informatici e/o software aggressivi.
5.b Qualora il software antivirus rilevi la presenza di virus con l'avviso che il software non è stato in grado di ripulire/eliminare il virus, l'utente è tenuto a sospendere ogni elaborazione in corso senza

spegnere il PC, e segnalare prontamente l'accaduto al Responsabile IT che provvederà per quanto di competenza anche con l'ausilio di consulente esterno.
5.c Ogni dispositivo magnetico di provenienza esterna installato sul PC, dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovrà essere utilizzato.

6. Accesso ai dati
6.a Le Società incaricate dell'assistenza hardware e software, unitamente al Responsabile IT per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi, e comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa degli utenti, hanno facoltà di accedere, nel rispetto della normativa sulla privacy, agli strumenti informatici aziendali e ai documenti ivi contenuti, compresi i file di log della navigazione svolta e gli archivi di posta elettronica. Si sottolinea comunque che l'accesso a tali dati è residuale rispetto alle misure preventiva di sicurezza del sistema (tecniche e gestionali) adottate, non continuativo, e legato alle finalità di cui sopra.
6.b Il sistema informatico aziendale è programmato e configurato in modo tale da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico la cui conservazione non sia necessaria.
6.c I file di log vengono conservati per un periodo non superiore a giorni 60, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Azienda.
6.d Un eventuale prolungamento dei tempi di conservazione avrà luogo, in via di eccezione, solo in relazione a: esigenze tecniche o di sicurezza straordinarie; indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria; obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

7. Sistemi di controllo graduati
7.a In caso di anomalie nell'utilizzo degli strumenti informatici che abbiano cagionato o cagionino un evento dannoso e/o una situazione di pericolo per la sicurezza del sistema informatico aziendale che i preventivi accorgimenti tecnico-gestionali non abbiano impedito, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali, da parte degli utenti, nell'utilizzo degli strumenti informatici.
7.b Ove possibile e sufficiente alla verifica dell'anomalia e alla eliminazione del danno e/o della situazione di pericolo, sarà effettuato un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa, e pertanto anonimo. Ove venga riscontrata tale anomalia, il datore di lavoro provvederà a diffondere uno o più avvisi generalizzati diretti alla struttura lavorativa nel suo complesso con l'invito rivolto agli utenti di attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite per l'utilizzo dei sistemi oggetto del Regolamento.
7.c Potranno essere compiuti controlli su base individuale solo ed esclusivamente nel caso di successive ulteriori anomalie tali da far persistere la situazione di danno o di pericolo che ha legittimato il controllo anonimo di cui al punto b).
7.d Tanto i controlli anonimi di cui al punto b), quanto i controlli individuali di cui al punto c), saranno comunque esercitati in base ai principi di pertinenza e non eccedenza rispetto al danno da rimuovere e/o alla situazione di pericolo da evitare.
7.e Non saranno comunque effettuati controlli sistematici, prolungati, costanti o indiscriminati.

8. Sanzioni
8.a È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei

confronti del personale dipendente con provvedimenti disciplinari e risarcitori, adottati nel rispetto della L. 300/1970, previsti dal CCNL di riferimento vigente, fatte salve azioni civili e penali nei confronti dei dipendenti e di tutti gli utenti soggetti al presente Regolamento.

9. Approvazione e revisione

9.a Il presente Regolamento è proposto dal datore di lavoro alla consultazione e approvazione degli utenti, che accettano e si impegnano alla corretta osservanza delle disposizioni in esso contenute.

3. Art. 24-ter Delitti di criminalità organizzata

Aree sensibili	**Operazioni a rischio commissione reato**	**Livello di rischio**
Direzione Aziendale	Gestione di rapporti commerciali, di intermediazione o distribuzione con associazioni delle quali si presume il vincolo associativo e la finalità criminale	3
Legale rappresentante/Responsabile commerciale		3
Amministrazione e gestione risorse umane		2
Logistica ed ufficio acquisti		2
Qualità e sicurezza		2

Legenda:1=rischio basso – 2=rischio medio – 3= rischio alto

L'Azienda ha rilevato un rischio puramente ipotetico ed astratto di commissione di tali reati, comunque delimitato ai rapporti con eventuali partners non consolidati o allo svolgimento di attività non costituenti l'oggetto sociale principale.
Con riferimento alle associazioni di tipo mafioso ("l'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e delle condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o il controllo di attività economiche, concessioni, autorizzazioni, etc.." art. 416-bis c.p.), può verificarsi l'ipotesi di un rapporto con fornitori /partner che, per la presenza storica di criminalità organizzata sul territorio in cui operano, potrebbero intrattenere rapporti illeciti con associazioni di tipo mafioso: in ottica preventiva, per i fornitori/partner occasionali sono previste verifiche di onorabilità (ad esempio richiesta del Certificato della Camera di Commercio con Dicitura Antimafia e/o relativa autocertificazione).

Procedure e protocolli per eliminare o ridurre il rischio di commissione dei reati

Con riferimento all'associazione per delinquere ("quando tre o più persone si associano allo scopo di commettere più delitti" art. 416 c.p.), l'Azienda potrebbe ottenere un interesse o vantaggio dall'associazione di più persone interne / collaboratori esterni nell'ambito di:

- **Partecipazione a gare, avvisi, bandi o appalti pubblici**

In tale caso si fa riferimento alla procedura di seguito indicata denominata "Partecipazione a bandi e avvisi" e al Codice Etico Aziendale.

Partecipazione a bandi e avvisi

Scopo

La presente procedura ha lo scopo di definire le modalità adottate e le responsabilità coinvolte per la gestione delle attività di partecipazione a bandi e avvisi indetti dalla Pubblica Amministrazione per l'erogazione di servizi formativi. Scopo della stessa è di regolamentare e di monitorare la corretta gestione nella partecipazione a tali bandi, così da evitare la commissione di reati. In particolare, viene descritta la gestione di tutta l'attività commerciale dalla fase di gara fino all'ottenimento del contratto.

Definizioni

Pubblici ufficiali: si intendono i soggetti incaricati di pubblica funzione appartenenti alla Pubblica Amministrazione

Incaricato di pubblico servizio: incaricato di un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni d'ordine e della prestazione di opera meramente materiale.

L'elemento discriminante per indicare se un soggetto rivesta o meno la qualità di "incaricato di un pubblico servizio" è rappresentato, non dalla natura giuridica assunta o detenuta dall'ente, ma dalle funzioni affidate al soggetto le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale.

Gare/Appalto pubblico: appalto per la fornitura di beni o di servizi indetto dalla Pubblica Amministrazione. Funzioni aziendali interessate: Direzione Aziendale, Responsabile commerciale, Direzione Tecnica ed Amministrativa sono le funzioni coinvolte nella selezione della gara alla quale partecipare, nella successiva elaborazione dell'offerta e trasmissione alla Pubblica Amministrazione della partecipazione alla gara d'appalto.

Organismo di vigilanza e controllo: l'OdV che assolve, sulla base delle indicazioni contenute nel D.Lgs. 231/2001, il compito di vigilare sulla effettività ed adeguatezza del Modello di organizzazione, gestione e controllo adottato dalla Società per prevenire i reati indicato nel suddetto decreto.

Modalità Operative

Si veda apposita procedura del Sistema di gestione della qualità.

4. Art. 25 Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione

Viene effettuata una dettagliata e precisa analisi delle attività a rischio del reato in oggetto, fornendo delle specifiche procedure al fine della non attuazione dello stesso.

Aree sensibili	Operazioni a rischio commissione reato	Livello di rischio
Direzione Generale	Gestione dei rapporti con le pubbliche amministrazioni, gli enti pubblici e gli organismi di controllo. **MB Consulting Srl** gestisce le pratiche di richiesta agevolazioni per le aziende clienti	3
Legale Rappresentante /Responsabile commerciale		3
Amministrazione e gestione risorse umane		3
Ufficio IT		2
Logistica ed ufficio acquisti		2
Qualità e sicurezza		2
Service		2
Assistenza		2

Legenda:1=rischio basso – 2=rischio medio – 3= rischio alto

Procedure e protocolli per eliminare o ridurre il rischio di commissione dei reati

Al fine di eliminare o comunque ridurre il rischio di commissione dei reati presupposto di cui all'art. 25 del D.Lgs. 231/2001, l'azienda ha elaborato e adottato i seguenti controlli e procedure

a. Divieto di stipula dei contratti in autonomia: il soggetto che intrattiene i rapporti con la pubblica amministrazione non può da solo e liberamente stipulare i contratti che ha negoziato. La negoziazione e la stipula dei contratti avvengono solo sulla base di una delega, autorizzazione o procura a tal fine formalizzata, con l'indicazione di vincoli e responsabilità.
b. Divieto di accesso a risorse finanziarie in autonomia: il soggetto che intrattiene rapporti con soggetti pubblici non può da solo e liberamente accedere a risorse finanziarie e/o autorizzare disposizioni di pagamento. L'effettuazione delle spese avviene solo su in base ad una delega, autorizzazione o procura a tal fine formalizzate con l'indicazione di valore, vincoli e responsabilità. Le spese possono essere effettuate solo in base a documenti giustificativi con motivazione, attestazione di inerenza e congruità, con approvazione di adeguato livello gerarchico.
c. Obbligo di collaborazione: il soggetto che intrattiene rapporti con la Pubblica Amministrazione è obbligato alla massima correttezza, collaborazione e trasparenza nei rapporti con tali soggetti. Tutte le azioni, le operazioni e, in genere, i comportamenti posti in essere nello svolgimento dell'attività sensibile, devono essere improntati ai principi di correttezza, integrità, legittimità e chiarezza. Qualsiasi informazione o comunicazione destinata ai soggetti pubblici deve essere accurata, veritiera, corretta, completa, chiara, puntuale e sempre rigorosamente conforme a quanto previsto dalle disposizioni applicabili.

Riferimento: Procedura "Partecipazione a gare ed appalti" e "Gestione Amministrativa e Finanza Dispositiva, di seguito riportata.

PROCEDURA GESTIONE AMMINISTRATIVA E FINANZA DISPOSITIVA

1. SCOPO

Il presente protocollo regola, in stretta relazione con le modalità operative e le prassi aziendali già ampiamente adottate in **MB Consulting Srl** e nel rispetto delle norme legislative dei principi contabili e del modello, le fasi estimative del processo di predisposizione di dati economici, patrimoniali e finanziari per la successiva comunicazione all'esterno, ivi compresa la redazione dei documenti economici consolidati.

Le procedure, le prassi e gli strumenti informatici esistenti garantiscono il controllo e la tempestività dei processi contabili, in particolare attraverso:

- idonea documentazione atta ad individuare l'unità organizzativa che ha generato l'evento amministrativo
- adeguata documentazione conservata agli atti

Il presente protocollo riguarda le fasi comprendenti la comunicazione dei dati per la redazione dei documenti economici e l'approvvigionamento delle risorse finanziarie necessarie al funzionamento dell'attività (acquisti di beni e di servizi, oneri finanziari, fiscali e previdenziali, stipendi e salari).

2. AMBITO DI APPLICAZIONE

Il presente protocollo si riferisce a **MB Consulting Srl.**

3. INDIRIZZI GENERALI

Le attività di predisposizione da parte degli organi amministrativi interni alla Società di dati economici, patrimoniali e finanziari per la successiva comunicazione ai professionisti esterni ai fini della redazione del bilancio aziendale, devono essere ispirate a principi di competenza, trasparenza e veridicità e devono rispettare le autorizzazioni richieste dalle procedure in atto e garantire la tracciabilità delle operazioni.

4. FUNZIONI AZIENDALI INTERESSATE

Responsabile Amministrativo e Direzione Aziendale.

5. MODALITÀ OPERATIVE

La gestione amministrativo finanziaria, viene svolta all'interno dell'azienda dalla Funzione Amministrativa.
Vi è un supporto consulenziale da parte di professionisti esterni ai quali la Funzione Amministrativa si rivolge per chiarimenti ed interpretazioni normative e per situazioni particolarmente complesse.
Le operazioni contabili sono eseguite nel rispetto dei dettati normativi ed elaborate con apposito software gestionale per la produzione di tutta la documentazione inerente all'attività (Ddt, fatture, ricevute bancarie, ecc.) con archiviazione cartacea e/o digitale della documentazione stessa nel rispetto delle disposizioni legislative.
Le disposizioni di pagamento dei dipendenti, dei fornitori e dei professionisti sono eseguite materialmente dalla Funzione Amministrativa su specifica disposizione ed autorizzazione della Direzione Generale. Il controllo e la verifica da parte della Direzione Aziendale sono eseguiti preventivamente, per verificare la disponibilità finanziaria per effettuare i pagamenti; è responsabilità della Funzione Amministrativa in seguito alle disposizioni ricevute effettuare correttamente le operazioni di pagamento.
Per quanto concerne gli incassi viene effettuata da parte della Direzione Aziendale una costante verifica sull'andamento e vengono date specifiche indicazioni procedurali alla Funzione Amministrativa per l'eventuale recupero di importi di pagamenti scaduti e non ancora riscossi.
Per la predisposizione del bilancio, con il supporto dei consulenti esterni, ne viene predisposta una bozza e consegnata al Legale Rappresentante che provvedere ad analizzarla. A conclusione dell'analisi vengono predisposti i documenti finanziari, eventualmente modificati, che possono così essere approvati dal Legale Rappresentante. Dell'esito della riunione ne va data informazione all'Organismo di Vigilanza.

5. Art. 25-bis Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento

L'Azienda non utilizza né gestisce flussi finanziari in contanti al di sopra dei limiti di legge, né emette o è in grado di alterare carte di credito. L'utilizzo di valori bollati è limitato. Pur non ravvisando alcun concreto interesse nella contraffazione di strumenti o segni di riconoscimento, data la natura dell'attività aziendale, si è voluto monitorare l'attività che riguarda gli acquisti al fine di evitare o ridurre il rischio di acquisto di beni contraffatti.

Aree sensibili	Operazioni a rischio commissione reato	Livello di rischio
Direzione Generale		2

Legale rappresentante /Responsabile commerciale	Modalità di impiego di marchi, brevetti e segni distintivi: gestione degli acquisti di prodotti	2
Amministrazione e gestione risorse umane		2
Logistica e acquisti		2

Legenda:1=rischio basso – 2=rischio medio – 3= rischio alto

Procedure e protocolli per eliminare o ridurre il rischio di commissione dei reati

Al fine di eliminare o comunque ridurre il rischio di commissione dei reati presupposto di cui all'art. 25 bis del D.Lgs. 231/2001, l'azienda ha elaborato e adottato i seguenti controlli e procedure:

a. Prescrizioni comportamentali: divieto, da parte degli apicali e dei sottoposti nell'ambito delle proprie attività lavorative e/o mediante utilizzo di risorse della società, di contraffazione e alterazione, sotto qualsiasi forma, di marchi o segni distintivi, di prodotti industriali, ovvero di brevetti, disegni o modelli e divieto di utilizzo di tali marchi, segni distintivi, brevetti, disegni o modelli industriali contraffatti o alterati.
b. Qualificazione ed accreditamento dei fornitori: preventiva verifica dei requisiti di onorabilità specifica dei fornitori utilizzati ai fini dell'approvvigionamento di beni e servizi per la società, facendosi rilasciare dagli stessi una dichiarazione ai sensi degli artt. 473 e 474 c.p., nonché alla mancata sottoposizione a procedimenti giudiziari relativi a violazioni delle predette disposizioni. La società, inoltre, effettua gli approvvigionamenti da fornitori accreditati.
c. Contratti di approvvigionamento: tutti i contratti di approvvigionamento di beni o servizi, contengono clausole di dichiarazione e garanzia del fornitore in ordine all'assenza di forme di contraffazione e alterazione di marchi o segni distintivi, nazionali o esteri, di prodotti industriali, ovvero di brevetti, disegni o modelli, nonché disposizioni di autotutela della società con riferimento alle ipotesi di inadempimento del fornitore rispetto a tali dichiarazioni e garanzie.

Riferimento Protocollo: procedura Sistema Qualità "PG702 GESTIONE FORNITORI ED APPROVVIGIONAMENTI"e Codice Etico.

6. Art. 25-bis-1 Delitti contro l'industria ed il commercio

Con riguardo ai delitti contro l'industria ed il commercio di cui all'art. 25-bis1 del D.Lgs. 231/2001, l'analisi dei rischi svolta dall'azienda ha portato alle conclusioni di seguito indicate:

Aree sensibili	Operazioni a rischio commissione reato	Livello di rischio
Direzione Generale	Gestione dei rapporti con la concorrenza; modalità di acquisizione di informazioni su prodotti dei concorrenti, rapporti con quest'ultimi e modalità di definizione del servizio rispetto a quello dei concorrenti	2
Legale rappresentante /Responsabile commerciale		2
Amministrazione e gestione risorse umane		2

Legenda:1=rischio basso – 2=rischio medio – 3= rischio alto

Procedure e protocolli per eliminare o ridurre il rischio di commissione dei reati

Al fine di eliminare o comunque ridurre il rischio di commissione dei reati presupposto di cui all'art. 25-bis 1 del D.Lgs. 231/2001, la società ha elaborato ed adottato i seguenti controlli e procedure:

a. Prescrizioni comportamentali: divieto, da parte degli apicali e dei sottoposti nell'ambito delle proprie attività lavorative e/o mediante utilizzo di risorse della società, di vendere o mettere in circolazione opere dell'ingegno o dei prodotti industriali con nomi, marchi o segni distintivi, nazionali od esteri, atti ad indurre in inganno il compratore sull'origine, la provenienza o qualità dell'opera o del prodotto; divieto di mettere in circolazione sotto qualsiasi forma oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso; divieto di porre in essere comportamenti di qualunque natura volti ad impedire o turbare il libero esercizio e normale svolgimento dell'industria e del commercio ovvero atti di concorrenza con violenza o minaccia nell'ambito dell'offerta sul mercato di beni o servizi da parte della società.

Riferimento Protocollo: procedura Sistema Qualità "PG701 GESTIONE DEI PROCESSI COMMERCIALI e Codice Etico

7. Art. 25-ter Reati societari

Con riguardo ai reati societari di cui all'art. 25-ter del D.Lgs. 231/2001, l'analisi dei rischi svolta dall'azienda ha portato alle conclusioni di seguito indicate:

Aree sensibili	Operazioni a rischio commissione reato	Livello di rischio
Direzione Generale	Modalità di formazione e redazione del bilancio: definizione delle informazioni da inserire nel bilancio e decisioni in ordine alle valutazioni delle poste di bilancio Modalità di gestione dei rapporti con il consulente esterno per la comunicazione dei dati ai fini della consulenza fiscale, finanziaria e per la redazione del bilancio	2
Legale rappresentante /Responsabile commerciale		2
Amministrazione e gestione risorse umane		2

Legenda:1=rischio basso – 2=rischio medio – 3= rischio alto

Procedure e protocolli per eliminare o ridurre il rischio di commissione dei reati

Al fine di eliminare o comunque ridurre il rischio di commissione dei reati presupposto di cui all'art. 25-ter del D.Lgs. 231/2001, l'azienda ha elaborato e adottato i seguenti controlli e procedure:

a. Redazione del bilancio: le funzioni preposte alla gestione dei dati amministrativo-contabili effettuano un controllo preventivo sulla correttezza, completezza e veridicità delle informazioni da fornire al consulente esterno ai fini della predisposizione del bilancio aziendale. La funzione preposta alla redazione del bilancio e degli altri documenti contabili societari, predispongono adeguate procedure amministrative, nonché ogni altra documentazione di carattere finanziario. Adotta anche un Sistema informatico: il sistema informatico utilizzato per la trasmissione dei dati ed informazioni garantisce la singola registrazione dei passaggi relativi all'elaborazione di tutti i flussi contabili e l'identificazione

dei soggetti che inseriscono i dati a sistema (mediante credenziali di autenticazione Id utente e password).

b. Gestione dei documenti contabili e di bilancio: le procedure amministrative e contabile predisposte dalle figure preposte alle registrazioni contabili e predisposizione dei dati di bilancio prevedono regole formalizzate che identifichino ruoli e responsabilità relativamente alla tenuta, conservazione ed aggiornamento delle operazioni contabili
c. Attività di preparazione, svolgimento e verbalizzazione dell'assemblea dei soci.
d. La società è dotata di un Bilancio d'esercizio Certificato a cura di Revisore contabile.

Riferimento Protocollo: procedura Sistema gestione qualità e Codice Etico

8. Art. 25-quater Delitti con finalità di terrorismo o di eversione dell'ordine democratico

L'Azienda non dispone nella pratica né delle risorse né delle opportunità per la commissione dei reati in oggetto. L'azienda pertanto valuta come non attinente al proprio contesto di riferimento la fattispecie di reato in oggetto.

9. Art. 25-quater1 Pratiche di mutilazione degli organi genitali femminili

L'Azienda non dispone intrinsecamente né delle risorse né delle opportunità per la commissione dei reati in oggetto. L'Azienda pertanto valuta come non attinente al proprio contesto di riferimento la fattispecie di reato in oggetto.

10. Art. 25-quinquies Delitti contro la personalità individuale

L'Azienda non ha stabilimenti all'estero, pertanto non impiega manodopera al di fuori della legislazione nazionale; applica e garantisce i principi dettati dai contratti collettivi nazionali di riferimento; non opera in settori tali per cui sia possibile configurare reati a sfondo sessuale.
In ogni caso, è stato previsto nel Codice Etico uno specifico impegno a far rispettare ai propri fornitori la normativa vigente in materia di lavoro che si traduce nella richiesta e verifica che i propri partner commerciali rispettino gli obblighi di legge in tema di a) tutela del lavoro minorile e delle donne; b) condizioni igienico sanitarie e di sicurezza; c) diritti sindacali e di associazione.
Non si ritiene, inoltre, che l'utilizzo della rete aziendale per navigare su siti internet illegali possa essere un'ipotesi di reato adottabile nell'interesse o vantaggio della società, in quanto configurabile solo come comportamento disdicevole del singolo individuo. Per tale motivo se ne esclude l'applicabilità in capo al D. Lgs. 231/2001, sebbene l'azienda vieti tale comportamento all'interno del Codice Etico e implementi un filtro di protezione sulla navigazione dei siti internet **(REGOLAMENTO UTILIZZO PC, INTERNET E POSTA ELETTRONICA**).

11. Art. 25-sexies Abusi di mercato e Altre fattispecie in materia di abusi di mercato (reati aggiunti dalla L. 62/2005 e L. 238/2021)

I reati previsti dagli artt. 184,185 e 187- quinquies T.U.F. non sono attinenti alla posizione della società.

12. Art. 25-septies Omicidio colposo o lesioni colpose gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Sono state ritenuti "processi sensibili", in relazione a tali reati, quelli relativi all'adozione ed efficace attuazione di tutti gli adempimenti in materia di sicurezza del lavoro, resi maggiormente stringenti a seguito dell'entrata in vigore del D. Lgs. 81/2008 ed in particolare: l'approvazione del Sistema di

gestione Salute e Sicurezza sul lavoro, che contempla l'intero sistema aziendale sulla sicurezza contenente tra l'altro il Documento di Valutazione dei Rischi; l'effettuazione di attività di formazione ed informazione del personale; la nomina delle figure obbligatorie (Medico Competente, RSPP, Preposti alla sede di lavoro, RLS, Addetti servizio Primo Soccorso, Squadra Antincendio, ecc.).

Con riguardo ai reati di cui all'art. 25-septies, per i protocolli operativi e di controllo si fa riferimento al Sistema di Gestione della Salute e Sicurezza sul luogo di Lavoro aziendale – ed alla documentazione redatta in conformità al D. Lgs. 81/08 (TU Sicurezza) e s.m.i.

13. Art. 25-octies Ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, art. 25 octies 1 Delitti in materia di strumenti di pagamento diversi dai contanti e art. 25-octies 1 comma 2 Altre fattispecie in materia di strumenti di pagamento diversi dai contanti

I reati previsti dal presente articolo sono valutati pertinenti in quanto potrebbero verificarsi casi in cui venga, anche inconsapevolmente, acquistato materiale proveniente originariamente da furto o venga messo in circolazione denaro ricevuto in pagamento ma di provenienza illecita. Pur non escludendone l'applicabilità e ritenendo il compimento del reato marginale, vengono stabilite le procedure ed i protocolli operativi di seguito indicati.

Aree sensibili	**Operazioni a rischio commissione reato**	**Livello di rischio**
Direzione Generale	Modalità di approvvigionamento delle materie prime: criteri adottati per la scelta dei fornitori e verifica circa la rispondenza a tali criteri, rapporti con i fornitori	2
Legale rappresentante /Responsabile commerciale		2
Amministrazione e gestione risorse umane		2
Logistica ed acquisti		2

Legenda:1=rischio basso – 2=rischio medio – 3= rischio alto

Procedure e protocolli per eliminare o ridurre il rischio di commissione dei reati

a. Prescrizioni comportamentali: divieto da parte degli apicali e dei sottoposti, nell'ambito delle rispettive competenze e mediante l'utilizzo delle risorse della società, di contrattare con soggetti che abbiano subito condanne per i reati di cui agli artt. 648, 648bis e 648ter c.p. può essere inserita, in calce alla conferma d'ordine, la seguente dicitura: IN LINEA CON I VALORI PERSEGUITI E DICHIARATI DA MB Consulting Srl, IL FORNITORE SI IMPEGNA AD ADERIRE ESPRESSAMENTE AI PRINCIPI ED ALLE REGOLE COMPORTAMENTALI DEL NOSTRO CODICE ETICO E DEL MODELLO ORGANIZZATIVO DI GESTIONE E CONTROLLO, CHE POSSONO ESSERE RICHIESTI ALLA DIREZIONE AZIENDALE.
b. Conoscenza della controparte: obbligo di preventiva verifica dei requisiti di onorabilità specifica dei fornitori utilizzati ai fini dell'approvvigionamento di beni e servizi per la società, ottenendo dichiarazioni dagli stessi in merito alla mancata applicazione di sanzioni per violazioni degli artt. 648, 648bis e 648ter nonché alla mancata sottoposizione a procedimenti giudiziari relativi a violazioni delle predette disposizioni.
c. Lista dei fornitori: la società effettua i propri approvvigionamenti di beni e servizi avvalendosi delle funzioni aziendali preposte a tali finalità e selezionando i fornitori ed inserendoli

nell'"Elenco fornitori qualificati" L'inserimento/eliminazione dei fornitori dalla lista e basato su criteri oggettivi. L'individuazione, all'interno della lista, del fornitore è motivata e documentata.

Riferimento protocolli: procedura Sistema Gestione Qualità aziendale "PG702 GESTIONE FORNITORI ED APPROVVIGIONAMENTI" e Codice Etico

14. Art. 25-novies Delitti in materia di violazione dei diritti di autore

È previsto nel Codice Etico l'impegno affinché non vengano acquisiti e/o installati software applicativi non autorizzati o senza licenza. Inoltre, il singolo non ha diritti amministrativi per poter essere accreditato a scaricare / installare programmi: tale attività può essere svolta solamente dal Responsabile Informatico aziendale.

Riferimento protocolli: REGOLAMENTO UTILIZZO PC, INTERNET E POSTA ELETTRONICA e Codice Etico

15. Art. 25-decies Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Nei rapporti con l'Autorità giudiziaria, i membri dell'organizzazione aziendale sono tenuti a prestare una fattiva collaborazione ed a rendere dichiarazioni veritiere, trasparenti ed esaustivamente rappresentative dei fatti. Nel Codice Etico e nella sezione Principi Generali sono previsti i comportamenti da tenere in tali situazioni.

Riferimento protocolli: Codice Etico e prassi aziendale.

16. Art. 25-undecies Reati ambientali

Nella fattispecie si tratta di reati che hanno una reale possibilità di commissione, anche in maniera colposa, indipendente dalla volontà del singolo membro dell'organizzazione aziendale del D.Lgs. 231/01.

Aree sensibili	Operazioni a rischio commissione reato	Livello di rischio
Direzione Generale	Gestione della tematica ambientale: modalità delle richieste delle autorizzazioni, modalità di esercizio delle attività in rapporto ai contenuti delle autorizzazioni, gestione degli scarichi, dei rifiuti, delle sostanze inquinanti e dei livelli di emissione in atmosfera	2
Legale rappresentante /Responsabile commerciale		2
Amministrazione e gestione risorse umane		2
Ufficio IT		2
Logistica ed ufficio acquisti		2
Qualità e sicurezza		2
Service		2
Produzione/Assistenza		2

Legenda:1=rischio basso – 2=rischio medio – 3= rischio alto

Procedure e protocolli per eliminare o ridurre il rischio di commissione dei reati

a. Gestione degli adempimenti normativi interni in materia di tutela ambientale: l'azienda mediante la funzione amministrativa monitora ed effettua la gestione di tutti gli obblighi previsti dalla vigente legislazione ed in quanto applicabili all'azienda (ad esempio gestione rifiuti) e si avvale della collaborazione di consulenti esterni per specifiche situazioni e necessità (smaltimento rifiuti pericolosi ecc.) provvedendo alla produzione ed archiviazione della necessaria documentazione.

Riferimento protocolli: Codice Etico

17. Art. 25-duodecies Impiego di cittadini di paesi terzi il cui permesso di soggiorno è irregolare

Stante la politica aziendale, ribadita anche nel Codice Etico, ed i sistemi di controllo delle assunzioni da parte degli organi preposti, definiti da apposita procedura nell'ambito di apposita procedura contenuta nel Sistema di Gestione per la Qualità Aziendale non si ravvede la possibilità che venga commessa tale tipologia di reato. È stata comunque predisposta apposita procedura di seguito riportata, denominata "GESTIONE LAVORATORI EXTRACOMUNITARI"

Riferimento protocolli: Codice Etico – Gestione Lavoratori extracomunitari e procedura Sistema Gestione Qualità "PG601 Gestione Risorse Umane".

GESTIONE LAVORATORI EXTRACOMUNITARI

Scopo: La presente procedura attua quanto previsto dall'art. 2 del Dlgs 16 Luglio 2012, n.109 e s.m.i. (in attuazione alla direttiva 2009/52/CE), introducendo norme minime relative a sanzioni e a provvedimenti nei confronti del DL che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare.

Premessa

Nonostante il cosiddetto reato di "caporalato" previsto dall'art. 603 del Codice Penale non sia direttamente ed interamente richiamato dal D.Lgs. 231/2001, ad eccezione del comma 3 richiamato dall'art. 22 comma 12-bis, D.Lgs. 109 del 16.07.2012 e s.m.i., l'azienda non utilizza intermediari per il reclutamento di lavoratori (sino ad ora non sono state utilizzate le Agenzie di somministrazione (di lavoro interinale) autorizzate dal Ministero del Lavoro).
Qualora in futuro ci sarà la necessità di reclutare i lavoratori tramite dette Agenzie, il Responsabile Amministrativo avrà cura di richiedere il Durc.

Presentazione domanda di nulla osta all'assunzione di lavoratore straniero:

Per instaurare un rapporto di lavoro subordinato (a tempo indeterminato, determinato o stagionale) con un cittadino extracomunitario residente all'estero, il DL deve presentare una specifica richiesta nominativa di nulla osta, cioè di autorizzazione, all'atto di assunzione, presso la Prefettura – Ufficio territoriale del governo (Sportello unico competente) per il luogo in cui l'attività lavorativa dovrà effettuarsi, compilata su un apposito modulo:
-solo a partire dalla data stabilita dal "decreto flussi" che fissa le quote di ingresso per motivi di lavoro subordinato, cioè il numero di lavoratori stranieri autorizzati ad entrare in Italia;
-solo per via telematica, tramite personal computer dotato di connessione ad Internet e di un indirizzo di posta elettronica valido e funzionante.

NB: È importante sapere che il nulla osta al lavoro subordinato ha validità pari a 6 mesi dalla data del rilascio, durante i quali il lavoratore deve fare ingresso in Italia, presentarsi allo Sportello e stipulare il contratto.

Richiesta e rilascio del visto in ingresso

Il DL invia il nulla osta al lavoratore straniero, che richiede all'ambasciata o al consolato italiani il rilascio del visto di ingresso per motivi di lavoro subordinato, presentando il passaporto, il nulla osta ed altri documenti eventualmente richiesti.
NB: Il visto deve essere richiesto entro i 6 mesi di validità del nulla osta. Se vi sono i requisiti previsti, entro 30 giorni dalla presentazione della domanda al cittadino straniero viene rilasciato il visto di ingresso per motivi di lavoro subordinato non stagionale che consente di entrare regolarmente in Italia.
Il lavoratore straniero che si intende assumere deve trovarsi nel Paese di provenienza.
Se il lavoratore straniero soggiorna irregolarmente in Italia, l'assunzione è possibile solo seguendo la normale procedura: il lavoratore deve comunque rientrare nel suo Paese per ottenere il rilascio del necessario visto d'ingresso.

Ingresso in Italia

Quindi, il lavoratore straniero entro 8 giorni lavorativi dall'ingresso deve richiedere il rilascio del permesso di soggiorno per lavoro subordinato: la domanda, compilata su apposito modulo e con allegati i documenti richiesti, deve essere presentata ad uno degli uffici postali abilitati, che rilascia la ricevuta.
Se non viene richiesto entro 8 giorni lavorativi, il permesso di soggiorno viene rifiutato ed il cittadino straniero viene espulso, a meno che il ritardo non sia provocato da documentate cause di forza maggiore (ad esempio, malattia o incidente).

Obblighi di comunicazione per assunzione

Il DL deve:

- comunicare l'instaurazione del rapporto di lavoro al Centro per l'impiego, competente per la sede di lavoro, il giorno precedente all'inizio dell'attività, inviando per via telematica lo specifico modello ''Unificato – Lav''. Questa comunicazione vale anche per l'INAIL e per l'INPS;
- se concede al lavoratore l'uso di un'abitazione a qualunque titolo (ospitalità, affitto, comodato), presentare la specifica comunicazione di ''cessione di fabbricato'' entro 48 ore all'autorità di pubblica sicurezza: alla Questura o al Commissariato di polizia (mod. Cessione di fabbricato), o al Sindaco nei comuni in cui non è presente un presidio della Polizia di Stato (mod. Comunicazione al Sindaco di ospitalità o di cessione di immobili).

Per la compilazione e l'invio della domanda si deve seguire correttamente la specifica procedura illustrata sul sito web del Ministero dell'Interno (www.interno.it).
NB: Le operazioni di compilazione (che deve essere predisposta nel periodo precedente il giorno dell'invio) e di invio delle domande possono essere materialmente effettuate anche da una persona diversa dal datore di lavoro e non necessariamente tramite il PC aziendale; per l'effettuazione di tutte le operazioni il datore di lavoro, comunque, può rivolgersi anche ad associazioni di categoria o a patronati accreditati per questo compito. Le domande si possono inviare solo dal PC su cui è stato compilato il modulo.

Poiché le quote di ingresso per motivi di lavoro subordinato sono ampiamente inferiori alle domande e viene stabilita una graduatoria in base all'ordine di presentazione, per vedere accolta la domanda è assolutamente necessario effettuare l'invio della domanda nei primi minuti successivi all'avvio della ''lotteria delle quote'', nel giorno stabilito dal decreto flussi.
Nella domanda il datore di lavoro si impegna a garantire al lavoratore straniero il trattamento retributivo ed assicurativo previsto dalle leggi vigenti e dai contratti collettivi nazionali di lavoro applicabili, ad assicurare al lavoratore una idonea sistemazione alloggiativi, un alloggio che rientri nei parametri previsti dalle norme provinciali per gli alloggi di edilizia residenziale pubblica e ad effettuare entro i termini di legge le comunicazioni obbligatorie relative al rapporto di lavoro.

Rilascio di nulla osta all'assunzione
Il nulla osta all'assunzione viene rilasciato dallo Sportello Unico Immigrazione (SUI). Lo Sportello Unico:

- acquisisce il parere del Questore circa la sussistenza, nei confronti del lavoratore straniero, dei motivi ostativi al rilascio del nulla osta;
- acquisisce il parere della Direzione Provinciale del Lavoro circa la sussistenza o meno dei requisiti minimi contrattuali e della capienza reddituale del datore di lavoro.

NB: In caso di parere negativo da parte di almeno uno degli Uffici, lo Sportello rigetta l'istanza. In caso di parere favorevole:

- convoca il datore di lavoro per la consegna del nulla osta e per la firma del contratto (che successivamente viene sottoscritto anche dal lavoratore straniero dopo l'ingresso in Italia);
- trasmette per via telematica la documentazione agli uffici consolari.

NB: È importante sapere che il nulla osta al lavoro subordinato ha validità pari a 6 mesi dalla data del rilascio, durante i quali il lavoratore deve fare ingresso in Italia, presentarsi allo Sportello e stipulare il contratto.

Richiesta rinnovo permesso di soggiorno prima della scadenza
Il permesso per motivi di lavoro subordinato ha una durata pari a quella prevista dal contratto di soggiorno e, comunque, non superiore a 2 anni, se il contratto è a tempo indeterminato, e ad 1 anno, nel caso di un lavoro a tempo determinato.
Prima della scadenza del permesso di soggiorno, pertanto, il lavoratore straniero deve presentare ad uno degli uffici postali abilitati la domanda di rinnovo, compilata su apposito modulo ed allegando i documenti richiesti.
NB: È necessario presentare la domanda di rinnovo prima della scadenza del permesso e, comunque, assolutamente prima che passino 60 giorni dalla scadenza del vecchio permesso. Se trascorrono più di 60 giorni, il rinnovo del permesso di soggiorno può essere rifiutato ed il cittadino straniero può essere espulso. L'ufficio postale rilascia la ricevuta che, in attesa del rilascio del nuovo permesso di soggiorno, garantisce al lavoratore straniero sostanzialmente gli stessi diritti di un permesso ancora valido: in particolare rimane regolarmente in vita il rapporto di lavoro.
Quindi, purché il lavoratore abbia presentato la domanda di rinnovo entro i termini stabiliti e sia in possesso della ricevuta postale, la scadenza del permesso di soggiorno non provoca la cessazione o la sospensione del rapporto di lavoro.

Assunzione di un lavoratore straniero già soggiornante in Italia
Il DL può assumere anche lavoratori stranieri già soggiornanti in Italia, purché siano in possesso di un valido documento di soggiorno che abilita a prestare lavoro.
Può essere legalmente assunto, pertanto, il cittadino straniero munito di:

- permesso di soggiorno europeo per soggiornanti di lungo periodo (è il titolare di soggiorno di durata illimitata che ha sostituito la vecchia ''carta di soggiorno '').
- permesso di soggiorno che abiliti al lavoro, e quindi di un permesso per lavoro subordinato o autonomo, per attesa occupazione, per famiglia, per ''assistenza minore'', per asilo politico, per protezione sociale, per motivi umanitari.
- ricevuta postale rilasciata dietro presentazione della domanda di rinnovo di un permesso di soggiorno che abilita al lavoro (quindi di uno dei premessi sopra indicati);
- ricevuta postale rilasciata dietro presentazione della domanda di rilascio del primo permesso di soggiorno, ma solo per motivi di lavoro subordinato o di attesa occupazione e non, pertanto, per altri motivi.

Può essere assunto anche il cittadino straniero titolare di un permesso di soggiorno per motivi di studio, ma solo per rapporti di lavoro subordinato per un tempo non superiore a 20 ore settimanali, cumulabili per 52 settimane in modo da non superare, comunque, il limite di 1.040 ore in un anno.
La procedura di assunzione di un lavoratore straniero già regolarmente soggiornante, nei casi legalmente previsti, prevede:

- la preventiva stipulazione del contratto di soggiorno sullo specifico modello per l'assunzione di stranieri già soggiornanti in Italia: le parti del rapporto devono solo conservare una copia di contratto, che non deve essere inviato o consegnato a nessun ente.
- altri obblighi già esaminati a proposito dell'assunzione di lavoratore al primo ingresso in Italia, quali quello di comunicare l'assunzione al Centro per l'impiego, competente per la sede di lavoro, il giorno precedente all'inizio dell'attività, inviando per via telematica lo specifico modello ''Unificato – Lav'' e l'obbligo di comunicare all'autorità di pubblica sicurezza (presidio della Polizia di Stato o Sindaco) l'ospitalità o la cessione di un'abitazione a qualunque titolo.

Archiviazione della documentazione
Tutta la documentazione oggetto della presente procedura (atti, verbali, contratti, missive ed altri documenti), in formato sia elettronico che cartaceo, deve essere archiviata e facilmente rintracciabile.
A tal fine, la Funzione Amministrativa assicura la tracciabilità delle fonti/elementi informativi e cura l'archiviazione di tutta la relativa documentazione prodotta/ricevuta con riferimento alle attività propedeutiche e conseguenti alla presentazione della domanda di nulla osta all'assunzione di lavoratore straniero residente all'estero.

18. Art. 25- terdecies Razzismo e xenofobia

Non si ravvisano rischi di violazione di tali reati.

19. Art.10 L.146/2006 Reati di criminalità organizzata transnazionale

Non si ravvisano rischi di violazione di tali reati in particolare nel favoreggiamento dell'immigrazione clandestina.

20. Art. 25- quaterdecies Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati

Non si ravvisano rischi di violazione di tali reati.

21. Art. 25 quinquiesdecies Reati Tributari

[Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, Dichiarazione fraudolenta mediante altri artifici, Emissione di fatture o altri documenti per operazioni inesistenti, Occultamento o distruzione di documenti contabili, Sottrazione fraudolenta al pagamento di imposte, Dichiarazione infedele, Omessa dichiarazione, Indebita compensazione]

Nella fattispecie si tratta di reati che hanno una reale possibilità di commissione, sia da parte della Direzione Generale e dei soggetti apicali, sia da parte dei dipendenti e subordinati dell'area Amministrativa e contabile.

Con riguardo ai reati fiscali descritti all'art. 25 quinquiesdecies, si è ipotizzato che la commissione di tale reato si possa verificare nelle aree e nelle operazioni indicate nella tabella seguente:

Aree sensibili	**Operazioni a rischio commissione reato**	**Livello di rischio**
Direzione Generale	**MB Consulting Srl** svolge le seguenti attività/operazioni: emissione/ricezione di fatture verso/da clienti e fornitori; tenuta registro contabile; redazione e deposito bilancio; dichiarazione dei redditi; calcolo e versamento delle dovute imposte. Pertanto, potrebbe incorrere nei reati di cui al punto	2
Legale rappresentante		2
Amministrazione e Contabilità		1

Legenda:1=rischio basso – 2=rischio medio – 3= rischio alto

Procedure e protocolli per eliminare o ridurre il rischio di commissione dei reati

Al fine di eliminare o comunque ridurre il rischio di commissione dei reati presupposto, la società ha elaborato e adottato i seguenti protocolli e procedure:

- Autorizzazione formalizzata: Il pagamento di ciascuna fattura avviene previa autorizzazione da parte della Direzione;
- Tutte le fatture emesse transitano attraverso il sistema elettronico SDI;
- Non viene utilizzato il sistemo elettronico SDI solo ed esclusivamente per le note di debito esenti di Iva verso i soggetti che rilasciano apposita dichiarazione di esenzione iva;

- Ogni documento contabile è tracciato e gestito attraverso un sistema gestionale contabile, a cui ha accesso, per il dovuto controllo, anche il dott. Commercialista incaricato dall'azienda;
- Redazione del bilancio: le funzioni preposte alla gestione dei dati amministrativo-contabili effettuano un controllo preventivo sulla correttezza, completezza e veridicità delle informazioni da fornire al dott. Commercialista incaricato dall'azienda ai fini della predisposizione del bilancio aziendale. La funzione preposta alla redazione del bilancio e degli altri documenti contabili societari, predispongono adeguate procedure amministrative, nonché ogni altra documentazione di carattere finanziario;
- Il Bilancio sociale viene correttamente e annualmente depositato presso il Registro delle Imprese di Brescia;
- Il Bilancio così depositato è oggetto anche di controllo e certificazione del Revisore contabile esterno;
- Gestione dei documenti contabili e di bilancio: le procedure amministrative e contabili predisposte dalle figure preposte alle registrazioni contabili e predisposizione dei dati di bilancio prevedono regole formalizzate e strumenti elaborati ad hoc che identifichino ruoli e responsabilità relativamente alla tenuta, conservazione ed aggiornamento delle operazioni contabili;
- Documentazione: tutta la suddetta documentazione sarà oggetto di attività di controllo - Audit interni ed attività dell'Organismo di Vigilanza. (PIANO CONTROLLI ANNUALI).

22. Art. 25 quinquiesdecies 1 bis Reati fiscali transfrontalieri

Il comma 1 bis prevede che tutte le fattispecie di reati fiscali di cui all'art. 25 quinquiesdecies possono essere commessi anche in territorio transfrontaliero.

Nella fattispecie si tratta di reati che, considerati i rapporti con alcuni Clienti e fornitori con residenza fiscale non in Italia, hanno così una reale possibilità di commissione, sia da parte della Direzione Generale e dei soggetti apicali, sia da parte dei dipendenti e subordinati dell'area Amministrativa e contabile.

Con riguardo ai reati fiscali descritti all'art. 25 quinquiesdecies comma 1 bis, si è ipotizzato che la commissione di tale reato si possa verificare nelle aree e nelle operazioni indicate nella tabella seguente:

Aree sensibili	**Operazioni a rischio commissione reato**	**Livello di rischio**
Direzione Generale	**MB Consulting Srl** svolge le seguenti attività/operazioni: emissione/ricezione di fatture verso/da clienti e fornitori; tenuta registro contabile; redazione e deposito bilancio; dichiarazione dei redditi; calcolo e versamento delle dovute imposte. Pertanto, potrebbe incorrere nei reati di cui al punto	2
Legale rappresentante		2
Amministrazione e Contabilità		1

Legenda:1=rischio basso – 2=rischio medio – 3= rischio alto

Procedure e protocolli per eliminare o ridurre il rischio di commissione dei reati

Al fine di eliminare o comunque ridurre il rischio di commissione dei reati presupposto, la società ha elaborato e adottato gli stessi protocolli e procedure previste, di cui al punto che precede, al fine di eliminare o ridurre il rischio di commissione dei reati fiscali fuori dai confini nazionali.

23. Art. 25-sexiesdecies Contrabbando

Non si ravvisano rischi di violazione di tali reati.

24. Art. 25-septiesdecies Delitti contro il patrimonio culturale

Non si ravvisano rischi di violazione di tali reati.

25. Art. 25-duodevicies Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici

Non si ravvisano rischi di violazione di tali reati.
La Società sulla base dell'analisi sopra riportata si è comunque determinata a rafforzare il sistema di controllo interno con specifico riferimento a detti reati istruendo se necessario, dove non presenti, ulteriori protocolli/procedure atte all'eliminazione e/o riduzione della possibilità di incorrere in violazioni di legge.

8. COMPOSIZIONE DEL MODELLO ORGANIZZATIVO

Sulla base delle analisi di rischi di cui al punto precedente il presente Modello Organizzativo è così costituito:

- Codice Etico
- Regolamento dell'Organismo di Vigilanza (versione aggiornata del 04.12.2023)
- Regolamento disciplinare (versione aggiornata del 04.12.2023)
- Criteri Generali, illustrativi del contesto normativo di riferimento, degli obiettivi, delle linee di struttura e delle modalità di implementazione dello stesso
- Procedure e Protocolli implementati e riferimento a procedure e protocolli nell'ambito dei sistemi di gestione Qualità – Salute&Sicurezza
- "Sistema Whistleblowing"

Allegati:

- Organigramma Aziendale aggiornato.

9. ORGANISMO DI VIGILANZA

L'OdV viene nominato dal Legale Rappresentante.
Il dettaglio dei requisiti, compiti, poteri e regole dell'OdV della società è riportato all'interno del Regolamento dell'OdV.
Le funzioni istituzionali dell'OdV a termini dell'art. 6, 1° comma, lettera b), del D.Lgs. 231/01 sono le seguenti:

- vigilare sul funzionamento e sull'osservanza del Modello Organizzativo;
- segnalare le esigenze di revisione e/o aggiornamento del Modello Organizzativo.
- gestire in totale riservatezza, nella persona del suo Presidente, le segnalazioni di violazioni dei reati presupposto ex D.Lgs 231/2001 o del Modello adottato in azienda, fatte da chiunque ne abbia rilevato la commissione nell'esercizio delle sue funzioni nel contesto lavorativo. Le segnalazioni vengono fatte attraverso il "canale interno di segnalazione" attivato *ad hoc*

dall'azienda nel rispetto e in applicazione dell'art. 6, comma 2bis del D.Lgs. 231/2001, sulla piattaforma digitale personalizzata **whistlesblow.it** all'indirizzo **whistlesblow.it/c/mb-consulting-srl/1**.

Tutti i dipendenti, dirigenti e tutti coloro che, a qualsiasi titolo (ad es. collaboratori con altri rapporti contrattuali/stagisti etc), collaborano con azienda e/o cooperano al perseguimento degli obiettivi aziendali, possono avanzare - mediante il canale di segnalazione interno attivato tramite la **piattaforma digitale whistlesblow.it** all'indirizzo **whistlesblow.it/c/mb-consulting-srl/1**- **una segnalazione all'OdV** rispetto alla violazione o "fondato e concreto" sospetto di violazione, appreso nell'esercizio delle proprie funzioni nel contesto lavorativo, di:

- norme comportamentali prescritte dal Codice Etico, dal Modello Organizzativo, dai principi di comportamento e modalità esecutive disciplinate dai protocolli e dalle procedure aziendali rilevanti ai fini del D.Lgs. 231/2001 (Violazione del Modello adottato);
- reati presupposto ex D.Lgs. 231/2001.

L'Organismo è inserito in posizione di staff al Legale Rappresentante. La ricorrenza e la permanenza dei requisiti per ciascun componente dell'OdV vengono accertate dal Legale Rappresentante in sede di nomina e saranno verificate dal medesimo organo periodicamente, per la durata del mandato in cui il componente dell'OdV rimarrà in carica.
L'OdV riporta direttamente al Legale Rappresentante della società cui riferisce in merito all'attuazione del Modello Organizzativo ed all'emersione di eventuali criticità. Il reporting sarà su base continuativa e periodica. Si prevedono 4 riunioni trimestrali dell'OdV e una relazione OdV annuale finale in merito al controllo sulla corretta osservanza del Modello adottato ed eventuali correttivi, aggiornamenti necessari.
In particolare, la relazione periodica dovrà indicare l'attività svolta nel periodo, sia in termini di controlli effettuati e degli esiti ottenuti, che in ordine alle eventuali necessità di revisione e/o aggiornamento del Modello Organizzativo.
Oltre a quanto sopra previsto, i Responsabili di Direzione/Funzione, nell'ambito dello svolgimento delle attività di propria competenza, sono tenuti a fornire all'OdV, ogni qualvolta l'evento si verifichi e tempestivamente, le informazioni richieste dai relativi protocolli/procedure rilevanti ai fini del Modello Organizzativo.
Peraltro, in aggiunta al flusso di informazioni di cui sopra, qualora comunque non si verifichino situazioni in cui sia necessario un tempestivo coinvolgimento dell'OdV, mediante flussi informativi i Responsabili di Direzione/Funzione forniranno appositi report contenenti anche l'assicurazione sulla completezza delle informazioni comunicate.

9.1. Piano dei flussi delle comunicazioni/report verso l'OdV previsti nel Modello

Il destinatario delle comunicazioni e segnalazioni in tabella è sempre l'OdV di MB Consulting Srl.				
Frequenza	Entro	Competenza	Ambito	Contenuti
TEMPESTIVAMENTE	3 giorni lavorativi	Responsabile del conferimento di incarico	Consulenze e prestazioni professionali	Comunica eventuali criticità rilevate nella gestione del rapporto con il consulente/ professionista
		Resp.di funzione competenti	Rapporti con la P.A.	In caso di ispezioni della P.A.: trasmissione della copia del verbale di accesso rilasciato; trasmissione dei successivi verbali / comunicazioni
				report sulle richieste di informazioni da parte delle autorità di vigilanza
		Resp. Amministrazione	Personale	report sull'assunzione di personale che abbia avuto esperienze pregresse nell'ambito della P.A. o abbia relazioni di parentela o affinità con dipendenti/collaboratori o soggetti che ricoprono cariche nell'ambito della P.A.
				In caso di ispezioni: trasmissione della copia del verbale di accesso
		Resp. Sistemi Informatici	Utilizzo rete aziendale / internet	report su eventuali gravi anomalie riscontrate nella gestione dei Sistemi Informatici
		Datore di lavoro	Salute e Sicurezza	Comunica eventuali infortuni verificatisi in azienda e relativi verbali di ispezione rilasciati dagli enti competenti

Il destinatario delle comunicazioni e segnalazioni in tabella è sempre l'OdV di MB Consulting Srl				
Frequenza	Entro	Competenza	Ambito	Contenuti
	30 giugno, 31 dicembre	Resp. Amministrazione	Patrimonio e operazioni sul capitale	report sui flussi finanziari non standard ed operazioni straordinarie di capitale
			Movimentazione dei flussi finanziari	comunicazione eventuali rapporti con banche estere / movimenti di denaro contante
			Rapporti con la P.A., gare e bandi	report sulla partecipazione a progetti finanziati con denaro pubblico, gare e bandi per appalti pubblici
				report periodico sugli adempimenti fiscali
			Consulenze ed incarichi professionali	report periodico su consulenze esterne (fuori dall'ordinario)
			Omaggi e spese di rappresentanza	report periodico sulle spese di rappresentanza, omaggi e sponsorizzazioni
			Procedimenti arbitrali e giudiziali	report sui contenziosi e/o transazioni in corso
		Resp. Amministrazione	Personale	report su rimborsi spese a soggetti apicali
				report su formazione in temi di interesse (sicurezza sul lavoro, d.lgs. 231, ambiente, etc.)

SEMESTRALE				report su situazioni di Cassa Integrazione, Mobilità, Contratti di Solidarietà, ecc.
				report su provvedimenti disciplinari attuati (sia verbali che scritti)
		Resp. di Funzione competente	Rapporti con la P.A.	riepilogo periodico degli incontri con componenti della P.A. dei vari responsabili di funzione (es. ARPA in campo ambientale, ASL in campo S&S)
		Datore di lavoro	SISTEMA DI GEST. DELLA SICUREZZA SUL LAVORO	Introduzione di nuovi DPI a fronte di una revisione della variazione dei rischi
				Relazione sull'andamento infortunistico ed eventuali segnalazioni dei preposti e relativi sanzioni disciplinari applicate
				Scadenziario degli adempimenti di legge
			AMBIENTE	Esito analisi ambientali di laboratorio (emissioni, scarichi, etc.)
				Scadenziario degli adempimenti di legge
				Relazione smaltimento rifiuti
		Direzione Generale Datore di lavoro Resp. Amministrazione	Sviluppo tecnologico	Acquisti nuovi impianti / modifiche impianti esistenti
			Infrastrutture	Interventi rilevanti su immobili
			Risorse umane	Avanzamento del piano formativo in corso
ANNUALE	31 dicembre	Resp. Amministrazione	Assemblee e rapporti con terzi	scambio di informazioni e riunioni periodiche tra OdV e organi preposti alla redazione del bilancio
		Datore di lavoro	SISTEMA DI GEST. DELLA SICUREZZA SUL LAVORO	report statistiche sugli infortuni / incidenti
				Verbale di riunione periodica ex art. 18 D. Lgs. 81/2008
				Relazione sanitaria annuale del medico competente
			SISTEMA DI GESTIONE INTEGRATO	Riesame della Direzione del sistema di gestione Qualità-Salute&Sicurezza

Tutte le informazioni, generali e specifiche, sono fornite in forma scritta ed indirizzate al all'OdV.
Ogni informazione e report previsto nel Modello Organizzativo è conservata dall'OdV in un apposito archivio informatico e/o cartaceo in conformità alle disposizioni contenute nel Decreto Legislativo n. 196/2003.
A carico dei componenti dell'OdV vi è l'obbligo assoluto e inderogabile di mantenere il segreto sulle attività svolte e sulle informazioni societarie di cui vengono a conoscenza nell'esercizio del loro mandato.
Al fine di garantire all'OdV una piena autonomia nell'espletamento delle proprie funzioni, senza limitazioni che possano conseguire da insufficienti risorse finanziarie, è assegnato a tale organismo un budget annuo di **€ 10.000,00** definito dal Legale Rappresentante, fatta salva la possibilità di richiederne integrazioni se necessarie.

10. SISTEMA WHISTLEBLOWING

La normativa di riferimento è il D. Lgs 24/2023

10.1. Ambito di applicazione

La tutela sulla riservatezza del soggetto segnalante (oltre che della segnalazione e soggetti coinvolti), attuata attraverso la disciplina strutturata per garantire la protezione degli «informatori/segnalanti o whistleblowers» è introdotta dalla **normativa D.Lgs 24/2023** e, nel caso in cui sia stato adottato in azienda un Modello 231, **si applica alle segnalazioni di violazioni (di comportamenti, atti od omissioni), che devono essere «fondate su elementi di fatto precisi e concordanti», e che ledono l'interesse pubblico o l'integrità dell'ente privato e che consistono in condotte illecite rilevanti ai sensi del D.lgs. 231/2001 o violazioni del Modello adottato,** di cui si è venuto a conoscenza nel contesto lavorativo.
Nel contempo, al fine di evitare false segnalazioni o allarmismi non giustificati, **il soggetto segnalante deve limitarsi a segnalare le sole violazioni che siano «fondate su elementi di fatto precisi e concordanti»,** tralasciando invece le questioni/lamentele personali così come anche le semplici "voci di corridoio". Si ricorda che l'azienda può assumere delle azioni disciplinari, qualora le segnalazioni risultino manifestatamente false o infondate, o fatte esclusivamente per un interesse personale e non ai fini di tutelare l'interesse pubblico e dell'azienda.
Sono da intendere ***"whistleblowers"***, ossia come soggetti meritevoli di riservatezza e protezione, **tutti quei soggetti che sono collegati in senso ampio all'organizzazione aziendale** nella quale si è verificata la violazione e che, a fronte della segnalazione fatta, potrebbero temere atti pregiudizievoli/comportamenti ritorsivi.
Sono considerati **Whistleblower**:

- Lavoratori subordinati
- Lavoratori autonomi che svolgono la propria attività lavorativa all'azienda;
- Liberi professionisti e consulenti che prestano la propria attività all'azienda;
- Tirocinanti che prestano la propria attività all'azienda;
- Azionisti (persone fisiche);
- Persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso l'azienda

**(La tutela si applica anche durante il periodo di prova e anteriormente o successivamente alla costituzione del rapporto di lavoro o altro rapporto giuridico)*.

In aggiunta, **la tutela si applica anche a:**

- (se presente) Facilitatore, persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;
- Persone del medesimo contesto lavorativo del segnalante, denunciante o di chi effettua una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- Colleghi di lavoro del segnalante, denunciante o di chi effettua una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
- Enti di proprietà - in via esclusiva o in compartecipazione maggioritaria di terzi - del segnalante, denunciante o di chi effettua una divulgazione pubblica;
- Enti presso i quali il segnalante, denunciante o chi effettua una divulgazione pubblica lavorano (art. 3, co. 5, lett. d));

- Enti che operano nel medesimo contesto lavorativo del segnalante, denunciante o di chi effettua una divulgazione pubblica.

Le segnalazioni possano essere effettuate attraverso **tre diversi canali di segnalazione:** interna, esterna (all'ANAC), tramite divulgazione pubblica.
Le 3 tipologie di segnalazione **devono però necessariamente essere utilizzate in modo progressivo e sussidiario**, nel senso che il segnalante può effettuare:

- una segnalazione esterna solo se non ha potuto effettuare una segnalazione interna o se questa non ha avuto un seguito;
- una divulgazione pubblica solo dopo aver effettuato una segnalazione interna e/o esterna senza seguito.

**Chi fa una segnalazione deve essere consapevole che possono essere rilevati a suo carico profili di responsabilità civile, amministrativa e penale (ad es. per diffamazione), qualora non ci sia la fondatezza della segnalazione fatta o questa sia mendace.*

Divieto di atti ritorsivi
La normativa, a tutela di chi segnala, introduce anche il divieto di porre in essere atti ritorsivi a danno del soggetto segnalante. Per atti ritorsivi si intende qualsiasi atto comportamento/omissione/atto discriminatorio o minaccia di un danno ingiusto a discapito del segnalante.
Eventuali ritorsioni possono essere segnalate esternamente all'ANAC.

10.2. Impegni aziendali

In osservanza della disciplina ex D. Lgs. 24/2023, in riferimento a quanto previsto all'art. 6 comma 2-bis, **MB Consulting srl si attiva a:**

- tutelare il soggetto segnalante (il whistleblower), predisponendo all'interno del Modello l'adozione di un appropriato e riservato "canale di segnalazione interno" (in via telematica per segnalazioni in forma scritta e anonima);
- strutturare e assumere apposite procedure di presa in carico e gestione delle segnalazioni al fine di minimizzare, se non escludere, il rischio di possibili ritorsioni e/o condotte pregiudizievoli a sfavore di chi fa la segnalazione;
- individuare e incaricare l'OdV, nella figura del suo Presidente, come responsabile della presa in carico e gestione delle segnalazioni;
- qualora a fronte di istruttoria, la segnalazione risulti fondata, intervenire attivamente e tempestivamente con azioni correttive/sanzionatorie e ogni altro intervento necessario, al fine di porre fine alla violazione in corso o scongiurarne la futura possibile commissione.

10.3. Interventi aziendali

In applicazione della disciplina ex D. Lgs. 24/2023, in riferimento a quanto previsto all'art. 6 comma 2-bis, al fine di tutelare il soggetto segnalante, **MB Consulting srl:**

- ha adottato un sistema whistleblowing, ossia **ha attivato** per tutti coloro che ne abbiano interesse il cosiddetto **"canale di segnalazione interno"** tramite la **nuova piattaforma digitale whistlesblow.it**, **garantendone la sicurezza e la riservatezza del segnalante e delle segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del D. Lgs 231/2001 o del Modello stesso** e fondate su elementi di fatto precisi e concordanti, di cui si è venuti a conoscenza in ragione delle funzioni svolte nel contesto lavorativo.

Qualora ***il wistleblower*** (soggetto segnalante), nell'esercizio delle proprie funzioni nel contesto lavorativo, sia venuto a conoscenza di una violazione, "fondata e circostanziata", o abbia il fondato

sospetto che possa esser commessa una violazione del Modello o commissione dei reati presupposto così come previsti dal Modello stesso, **può fare, in totale sicurezza e riservatezza, una segnalazione** attraverso l'accesso alla piattaforma digitale personalizzata **whistlesblow.it**, accedendo al seguente link**: whistlesblow.it/c/mb-consulting-srl/1**.

**La piattaforma è a norma del 679/2016 GDPR e conforme al Trattamento dei dati.*

La piattaforma è di chiara comprensione e facile fruizione e guida il soggetto segnalante nella descrizione della propria segnalazione.

Accedendo al link sopra indicato, la segnalazione potrà esser fatta esclusivamente in forma scritta e potrà essere avanzata anche in forma anonima.

A prescindere dall'anonimato o meno della segnalazione, una volta inviata tramite piattaforma, il sistema genererà automaticamente un codice con il quale il soggetto segnalante, facendo accesso nuovamente al link sopra indicato, potrà monitorare lo stato avanzamento della medesima e, eventualmente, comunicare con il Responsabile delle Segnalazioni.

La segnalazione inviata mediante il canale interno disponibile verrà presa in carico nel più breve tempo possibile e gestita in sicurezza nel massimo della riservatezza sulla identità del segnalante e sull'entità della segnalazione stessa, al fine di minimizzare, se non escludere, il rischio di possibili ritorsioni e/o condotte pregiudizievoli a sfavore di chi fa la segnalazione.

MB Consulting Srl:

- **ha strutturato e assunto apposite procedure di presa in carico e gestione delle segnalazioni** al fine di minimizzare, se non escludere, il rischio di possibili ritorsioni e/o condotte pregiudizievoli a sfavore di chi fa la segnalazione (vedasi di seguito).
- **ha nominato come Responsabile e gestore delle segnalazioni l'OdV,** soggetto terzo e indipendente, nella persona del suo Presidente, il quale attraverso la piattaforma **whistlesblow.it** prenderà in carico e gestirà le segnalazioni avanzate. L'accesso al canale di segnalazione interno avverrà con credenziali esclusivamente a lui note.

Di seguito la procedura e le relative tempistiche previste per la gestione delle segnalazioni mediante il canale interno sopracitato.

1. **AVVISO DI RICEVIMENTO**
   Tramite piattaforma verrà dato riscontro, ove possibile, **entro 7 gg dal momento del ricevimento della segnalazione.**
2. **VALUTAZIONE SULLA PROCEDIBILITA' E AMMISSIBILITA' DELLA SEGNALAZIONE**
   - Attività istruttoria in merito alla segnalazione ricevuta: verificare la fondatezza della segnalazione, tra cui ad es. se il soggetto segnalante ha connessione/rapporto con azienda, se la segnalazione rientra nell'ambito della normativa ex D.Lgs. 24/2023. Verrà svolta istruttoria e accertamento tramite verifiche dirette o per tramite di funzioni interne/esterne/tecnici/audizioni. Verranno mantenute le interlocuzioni con il soggetto segnalante richiedendo a quest'ultimo, ove necessario, alcune integrazioni.
3. **ESITO, al termine dell'istruttoria, entro 3 mesi dalla ricezione della segnalazione.**
   **Se istruttoria è molto complicata, verrà comunque comunicato entro 3 mesi al soggetto segnalante la complessità e, pertanto, la riserva di dare riscontro in seguito.*
   a) **SE è NON FONDATA** → verrà comunicata l'improcedibilità motivata e si archivierà;
   b) **SE FONDATA MA NON RIENTRANTE NELLA DISCIPLINA WHISTLEBLOWING** → non si farà, in ogni caso, decadere la segnalazione, ma si procederà su altre funzioni aziendali (es. in caso fosse rilevato "mobbing" → pur non rientrando nella disciplina e tutela whistleblowing, si segnalerà comunque il caso alla funzione HR);
   c) **SE FONDATA** → trasmissione alle funzioni interne competenti. L'azienda si impegna ad intervenire attivamente e tempestivamente con azioni correttive/sanzionatorie e ogni altro intervento necessario, al fine di porre fine alla violazione in corso o scongiurarne la futura possibile commissione.

Si precisa che le segnalazioni inviate per mezzo della piattaforma **whistlesblow.it** saranno archiviate nella stessa per un periodo di 5 anni. Il momento di conservazione della segnalazione decorre dal data di chiusura della stessa o, in automatico, decorsi 90 giorni di inattività da parte del Responsabile delle segnalazioni e del segnalante.

**Al gestore non competono le valutazioni successive e correlate nel merito, conseguenti all'istruttoria. Sarà poi l'Azienda nella figura della Direzione che interverrà con attività di intervento o meno.*

11. SISTEMA SANZIONATORIO-DISCIPLINARE

I comportamenti realizzati in violazione del Modello Organizzativo, comprensivo di tutti i suoi allegati, che ne costituiscono parte integrante, nonché di tutti i protocolli/procedure volti a disciplinare in maggior dettaglio l'operatività nell'ambito delle aree a rischio reato e dei processi strumentali, da parte del personale di **MB Consulting Srl** sono sanzionati a termini dell'art. 6, 2° comma, lettera e), e dell'art. 7, 4° comma, lett. b) del D.Lgs. 231/01. La società reagirà tempestivamente alla violazione delle regole di condotta anche se il comportamento non integri gli estremi del Reato, ovvero non ne determini la responsabilità diretta. Le sanzioni irrogabili sono quelle previste dall'art. 7 della L. 20.05.1970, n. 300 (Statuto dei lavoratori) e dal Contratto Collettivo Nazionale applicato in azienda.
L'inosservanza degli obblighi e delle norme contenute nel presente Modello Organizzativo, nei suoi allegati e nelle procedure relative agli adempimenti previsti dai D.lgs. n. 231/2001, D.Lgs, n. 196/2003 e dal D.Lgs. n. 81/08 e s.m.i. da parte del personale dipendente comporta **i seguenti provvedimenti disciplinari,** che saranno presi dalla Società in relazione all'entità delle mancanze e alle circostanze che le accompagnano:

1. **richiamo verbale;**
2. **ammonizione scritta;**
3. **multa non superiore a tre ore di retribuzione oraria** calcolata sul minimo tabellare;
4. **sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni;**
5. **licenziamento per mancanze con preavviso e senza preavviso.**

La violazione da parte del dipendente degli obblighi previsti nei codici, modelli, allegati ivi richiamati e/o successivamente emanati dalla Società / datore di lavoro costituiscono comportamento rilevante dal punto di vista disciplinare e potrà comportare l'applicazione di provvedimenti disciplinari in relazione alla gravità del comportamento e/o alla eventuale recidiva nonché al grado della colpa, anche in relazione alla natura delle responsabilità affidate al dipendente stesso.
Si segnala che i suddetti provvedimenti disciplinari possono essere assunti dall'Azienda anche in ipotesi di segnalazioni (tutelate dalla disciplina *whistleblowing*) false, manifestatamente infondate, dipese da un comportamento scorretto in mala fede del segnalante, o comunque riguardanti semplici lamentele personali. L'accertamento delle suddette infrazioni, eventualmente anche su segnalazione dell'Organismo di Vigilanza, la gestione dei procedimenti disciplinari e l'irrogazione delle sanzioni stesse restano di competenza delle Funzioni aziendali a ciò preposte e delegate. Ogni violazione da parte dei dipendenti delle imprese esterne, dei consulenti o dei fornitori delle regole contenute nel Codice Etico e nel Modello Organizzativo agli stessi applicabili o di commissione di reati nello svolgimento della loro attività può generare la risoluzione del contratto. A questo fine può essere prevista apposita clausola contrattuale da inserire all'interno di ogni ordine di appalto/acquisto da sottoscrivere dall'appaltante all'atto dell'accettazione del lavoro/fornitura. Qualora la violazione coinvolga e comprometta anche l'immagine di **MB Consulting Srl** nei confronti del pubblico esterno e della clientela, l'Azienda si riserva di effettuare anche un'azione di rivalsa sui danni di immagine.

12. DIFFUSIONE DEL MODELLO ORGANIZZATIVO

Ai fini dell'efficace attuazione del Modello Organizzativo è obiettivo generale dell'Azienda garantire verso tutti i destinatari del Modello Organizzativo medesimo una corretta conoscenza e divulgazione delle regole di condotta ivi contenute. Tutto il personale, nonché i soggetti apicali, i consulenti, i partner ed i collaboratori esterni sono tenuti ad avere piena conoscenza sia degli obiettivi di correttezza e trasparenza che si intendono perseguire con il Modello Organizzativo, sia delle modalità attraverso le quali l'Azienda intende perseguirli. Obiettivo di carattere particolare è poi rappresentato dalla necessità di garantire l'effettiva conoscenza delle prescrizioni del Modello Organizzativo e le ragioni sottese ad un'efficace attuazione nei confronti di risorse le cui attività sono state riscontrate a rischio. Tali determinazioni sono indirizzate verso le attuali risorse della società nonché verso quelle ancora da inserire. L'idoneità allo scopo dei corsi di cui al successivo paragrafo 9.2 sarà oggetto di valutazione da parte dell'Organismo di Vigilanza.

12.1. La comunicazione iniziale

L'adozione del presente Modello Organizzativo è stata comunicata a tutto il personale in forza al momento dell'adozione stessa. In particolare, la comunicazione è stata disposta attraverso:

- Presa visione del Modello Organizzativo, disponibile presso la Funzione Amministrativa;
- Per il personale neoassunto dopo la prima divulgazione del Modello, esso viene condiviso durante il programma di formazione iniziale con la quale assicurare allo stesso le conoscenze considerate di primaria rilevanza.

12.2. La formazione

Per **MB Consulting Srl** l'attività di formazione del personale ha un ruolo preminente tra le attività societarie. L'azienda pertanto effettuerà un'intensa attività di promozione della propria cultura aziendale tra il personale, con un particolare accento sulla necessità di applicare i principi etici adottati e le regole interne, costruite nel più ampio rispetto della trasparente e corretta gestione delle società. In particolare, l'Azienda prevede l'erogazione di corsi destinati ai Responsabili di funzione, con i quali illustrare, nel contesto normativo sempre aggiornato, il Modello Organizzativo aggiornato, il ruolo dell'OdV e le modalità di gestione del Modello. Con specifico riferimento agli adempimenti in materia di salute e sicurezza dell'ambiente di lavoro, le funzioni preposte si occupano di predisporre i necessari corsi di aggiornamento e di addestramento previsti dalla legge, nonché corsi di formazione per specifici ruoli in materia di sicurezza, dandone pronta comunicazione all'Organismo di Vigilanza.

12.3. La formazione in materia WHISTLEBLOWING

Rispetto alla disciplina whistleblowing e la relativa tutela così come introdotta dalla stessa, l'azienda si assume l'impegno di informare e formare tutto il personale (e ulteriori altri soggetti interessati) attraverso informazioni di facile comprensione. Al personale verranno mostrate le funzionalità della piattaforma digitale **whistlesblow.it** per il suo corretto e facile utilizzo. Verranno spiegate tutte le procedure assunte con il presente Modello in relazione alla disciplina di riferimento. Inoltre, ai fini della trasparenza e pubblicità verso terzi, verranno indicati anche sul sito aziendale i riferimenti del canale di segnalazione interno adottato da MB Consulting Srl, specificando la possibilità di effettuare segnalazioni scritte, anche in forma anonima, attraverso il link alla piattaforma **whistlesblow.it/c/mb-consulting-srl/1** .

12.4. La comunicazione di aggiornamento

L'aggiornamento del presente Modello Organizzativo è comunicato a tutto il personale dipendente, anche se in stage. In particolare, la comunicazione viene disposta attraverso:

- Diffusione del Modello Organizzativo aggiornato attraverso invio mail. Il Modello rimane sempre disponibile presso la Funzione Amministrativa;
- Per il personale neoassunto dopo la prima divulgazione del Modello, esso verrà condiviso durante il programma di formazione iniziale con la quale assicurare allo stesso le conoscenze considerate di primaria rilevanza.

13. AGGIORNAMENTO DEL MODELLO ORGANIZZATIVO

Il D.Lgs. 231/01 prevede espressamente la necessità di aggiornare il Modello Organizzativo, al fine di renderlo costantemente ritagliato sulle specifiche esigenze dell'Ente e della sua concreta operatività. Gli interventi di adeguamento e/o aggiornamento del Modello Organizzativo saranno realizzati essenzialmente in occasione di:

- Innovazioni normative;
- Esiti negativi di verifiche / Audit sull'efficacia del medesimo;
- Violazioni del Modello Organizzativo;
- Modifiche della struttura organizzativa della società;
- Introduzione di nuovi Reati presupposto;
- Aggiornamenti/implementazioni necessarie introdotte da nuova e successiva normativa applicabile al D. Lgs. 231/01.
- Altri aggiornamenti/implementazioni di procedure.

L'aggiornamento del Modello Organizzativo e, quindi, la sua integrazione e/o modifica, spetta all'Amministratore Unico ed è oggetto di analisi e monitoraggio da parte dell'OdV.

14. RIFERIMENTI NORMATIVI AGGIORNATI

Il presente Modello tiene conto dei seguenti aggiornamenti normativi:
– D.Lgs. 24/2023: protezione dei segnalanti (whistleblowing)
– D.Lgs. 19/2023: recepimento Direttiva UE 2017/1371 (Direttiva PIF)
– L. 15/2022: riforma Cartabia e introduzione art. 129-bis c.p.
– D.L. 123/2023 convertito in L. 159/2023: rafforzamento disciplina reati informatici (art. 24-bis)
– D.Lgs. 184/2021: reati doganali (art. 25-sexiesdecies)

15. PARTE SPECIALE – Reati Informatici e Sicurezza Digitale (Art. 24-bis)

A seguito delle modifiche introdotte dalla L. 159/2023, risultano rafforzate le misure sanzionatorie per reati informatici quali accesso abusivo a sistemi informatici, danneggiamento di sistemi, frodi informatiche e phishing, anche se commessi in danno di soggetti privati.

In relazione all'utilizzo della piattaforma digitale MyMatrix, MBcRETICA ha adottato misure organizzative e protocolli interni per garantire:
– la protezione dei dati trattati;
– l'autenticazione sicura degli utenti;
– il controllo degli accessi ai dati sensibili;
– la prevenzione di intrusioni o uso illecito dei sistemi;
– il rispetto delle policy di sicurezza informatica aziendale.

L'OdV vigila sul rispetto delle procedure e sull'aggiornamento delle misure di sicurezza informatica anche alla luce del continuo evolversi delle minacce digitali.