# - CODICE ETICO E DI COMPORTAMENTO -

# 2023

Il Codice Etico e di Comportamento (di seguito anche "Codice") è uno degli strumenti della responsabilità sociale delle imprese per la diffusione ed attuazione di buone pratiche di comportamento. A maggior ragione, More Than Access S.r.l. Società Benefit (di seguito anche "MTA") vi si sente impegnata in quanto Società Benefit.

È uno strumento di autoregolamentazione: ciò significa che le organizzazioni che lo adottano, lo fanno volontariamente perché riconoscono che dotarsi di regole esplicitamente formulate, volontarie, dimostrando la possibilità di operare delle scelte in coerenza con i propri valori e non perché imposte dalle normative.

Il Codice Etico e di Comportamento di MTA nasce da questa convinzione: essere responsabili significa fondare la relazione tra le persone, sull'obiettivo del bene comune, che non si raggiunge sommando le utilità di ciascuno, ma costruendo in modo condiviso un sistema valoriale a cui ogni persona aderisce in modo spontaneo, avendo partecipato alla sua definizione.

Il Codice vuole essere un punto di riferimento e una guida per chi lavora in MTA e per chi ha interesse a perseguirne la Mission. Esso esprime impegni che ogni collaboratrice e collaboratore di MTA – ognuno secondo il proprio ruolo, le proprie responsabilità e la propria naturale attitudine - si assume nel condurre ogni attività aziendale, al di là di quanto prescritto dalla legge, verso tutti i portatori di interesse dell'impresa.

Non è un caso che il percorso per la sua definizione sia stato avviato sin dalla costituzione di MTA, per far fronte a nuove sfide e responsabilità in modo etico e trasparente nel rispetto delle attese delle nostre persone, delle richieste dei nostri clienti, dei cambiamenti istituzionali.

## Differenti utilità del Codice Etico

Il Codice serve innanzitutto a definire l'ammissibilità o inammissibilità dei comportamenti, ma ha anche altre finalità:

a. proporre modalità di comportamento che aiutino a orientare la propria condotta in quelle aree dell'agire quotidiano in cui possono manifestarsi potenziali conflitti tra morali individuali, logiche d'impresa e culture diverse,
b. accrescere la coesione interna e la coerenza del sistema: il Codice ha come scopo il miglioramento delle relazioni interne e la formazione di un'immagine esterna unitaria e chiara attraverso la formazione di un sentire e di un vissuto comune tra tutte le persone dell'azienda,
c. c. favorire la costruzione di un clima di fiducia entro l'azienda e verso i suoi "pubblici" di riferimento, sostenendo la reputazione di MTA agli occhi dei suoi stakeholder.

MTA non ha costruito il suo Codice come parte integrante del modello di organizzazione, gestione e controllo previsto dal D. Lgs. 231/01, che l'azienda potrà adottare in un prossimo futuro, ma a garanzia e quale strumento del rispetto dei comportamenti "giusti", in coerenza con i valori aziendali, per questo i suoi intendimenti sono più

profondi di un'eventuale conformità ad un dettato legislativo e si collegano integralmente alle sue diverse e connesse finalità.
Un'ultima notazione riguarda la natura proattiva del Codice: esso non è uno strumento rivolto a sanzionare, ma ad indirizzare, definendo linee guida per il comportamento nelle diverse attività svolte.
Perché ciò si possa realizzare, è molto importante che l'aspetto più apprezzato sia la sua ispirazione complessiva e l'attiva partecipazione alla sua elaborazione, ancor più delle singole indicazioni.

## Destinatari del Codice

I destinatari del Codice sono tutti coloro che a vario titolo e con differenti responsabilità costituiscono l'organizzazione e/o ne realizzano direttamente e indirettamente gli scopi.

## I portatori di interesse o *stakeholder* di MTA

Sono tutti i soggetti con cui MTA entra in relazione nello svolgimento delle sue attività e che, a vario titolo, concorrono al raggiungimento della Mission di MTA:

Collaboratori: sono coloro che, al di là della qualificazione giuridica del rapporto, intrattengono con MTA una relazione di lavoro finalizzata al raggiungimento degli scopi dell'impresa. Rientrano in questa categoria oltre ai dipendenti, anche i collaboratori a progetto, gli stagisti e i consulenti;

Clienti: sono le organizzazioni che, nei diversi mercati di riferimento dell'attività di MTA fruiscono dei servizi dell'azienda;

Soci: sono i proprietari dell'azienda, coloro che detengono una quota di MTA;

Fornitori: sono tutti quei soggetti (persone fisiche e/o giuridiche) che, a vario titolo, scambiano con MTA beni, servizi, prestazioni e risorse necessari alla realizzazione della sua attività caratteristica;

Territorio: comprende il contesto fisico (ambiente) e sociale (comunità) in cui MTA è chiamata ad operare, tanto a livello locale che nazionale o internazionale;

Istituzioni: sono i soggetti pubblici con cui MTA si relaziona, al di là del rapporto consulenziale che l'azienda intrattiene con essi.

## La Mission di MTA

Siamo una società benefit che produce valore facendolo emergere nelle molte imprese che lo valorizzano solo in parte. Lo facciamo formando le persone che in queste imprese operano. Affianchiamo imprese profit ed enti del Terzo settore aiutandoli a generare la felicità delle persone. Contribuiamo a realizzare un'economia circolare attenta alla sostenibilità socio-ambientale. Sappiamo di poterci riuscire promuovendo comunità sulla base di valori condivisi.

## I Valori di MTA

Sono i principi di riferimento che fanno da sfondo all'attività quotidiana di MTA, nei quali ci riconosciamo e sui quali formuliamo linee di condotta per raggiungere i nostri obiettivi strategici:

### *Sostenibilità*

La sostenibilità socio-ambientale ed economica è un valore imprescindibile nell'operatività di MTA che si impegna anche a divulgarne la pratica presso clienti fornitori partner. L'estensione dell'economia circolare ne è una concreta modalità.

### *Economia della condivisione*

La partecipazione al valore generato dall'impresa, così come da qualsiasi altra organizzazione o istituzione da parte di tutti coloro che vi contribuiscono, costituisce per MTA il principale *driver* di tutte le proprie attività. Ciò affinché questo sia un modello delle relazioni economiche di riferimento per la comunità territoriale ed il settore di riferimento.

### *Essere Benefit*

MTA è una Società Benefit e ha scelto di generare, nell'ambito delle sue attività, taluni benefici comuni da riversare sulla comunità. Il principale essa ritiene essere quello di aiutare tutte le imprese a esplicitare tutto il valore che generano e di renderne partecipi tutti coloro che vi contribuiscono. Ritiene di dover adempiere a questo impegno con tutti i mezzi in suo possesso per estendere questa modalità di fare economia quanto più ampiamente possibile e contribuire a renderla quella prevalente.

### *Collaborazione, Partecipazione e Partnership*

La fiducia quale base di ogni rapporto professionale e di *business* imposta i rapporti di MTA con clienti, fornitori, collaboratori, dipendenti, oltre che fra Soci. Una fiducia che porti a concreta collaborazione e ovunque ci siano le condizioni, a *partnership* con beneficio non solo fa le parti, ma per la comunità. Sono valori che sviluppano un forte senso di appartenenza all'azienda.

### *Onestà, Coerenza e Trasparenza*

Chiarezza delle regole, coerenza dell'azione professionale con queste, trasparenza nell'applicarle sono le linee guida dell'agire di MTA e del suo comunicarsi all'esterno. Riconoscendo limiti del nostro operare e coltivando le potenzialità del miglioramento.

### *Competenze e Qualità*

Il possesso delle competenze necessarie allo svolgimento delle attività va di pari passo con uno standard qualitativo elevato in MTA. È questa la norma a valere per tutti coloro che operano nella nostra società e lo standard che vogliamo far raggiungere a coloro che si rivolgono a noi. Finalizziamo tutto questo alla produzione di risultati che diano a clienti e *partner* valore riconosciuto e duraturo.

### *Innovazione*

L'innovazione è parte della nostra genetica: uscire dal consueto in un mondo in perenne cambiamento è l'elemento fondante della nostra attività. Concepiamo l'innovazione nell'approccio al *business*, all'organizzazione, al sistema di rapporti sociali sottesi a tutta l'attività economica. La concepiamo anche nelle tecnologie che per far questo è utile impiegare.

### *Conciliazione vita-lavoro e Attenzione alle persone*

La conciliazione tra vita privata e vita lavorativa, per tutti (donne e uomini), è parte essenziale del rispetto necessario per tutte le persone. Vogliamo portare attenzione ai bisogni delle persone per poterci accorgere di eventuali loro difficoltà ed apprestare quanto in potere dell'azienda per aiutarle.

### *Riconoscimento del merito*

Riconoscere le potenzialità ed il merito di ognuno, valorizzandone gli elementi caratteristici è un valore particolarmente importante per MTA.

## Le Norme di comportamento

Sono le indicazioni emergenti dalle responsabilità che, alla luce dei principi sui quali fondiamo la nostra attività, ci assumiamo nei confronti dei nostri portatori di interesse.

## Responsabilità verso i Collaboratori

### *Valorizzazione delle persone.*

MTA garantisce una dimensione di lavoro in cui ciascuno possa collaborare, esprimendo la propria attitudine professionale.

A tal fine, si impegna a:

a. investire nello sviluppo delle competenze, capitalizzando dalle diversità presenti in azienda, valorizzando le potenzialità e l'impegno di tutti,
b. predisporre programmi di aggiornamento e formazione atti a valorizzare le professionalità specifiche e a conservare e sviluppare la competitività dei collaboratori all'interno dell'azienda e sul mercato del lavoro esterno.

### *Motivazione delle persone*

MTA interpreta l'impresa come il luogo della responsabilità.

Essa si impegna a creare le condizioni perché la Direzione possa mantenere alta la condivisione con i collaboratori, rilevandone le aspettative, facendosene ove possibile carico e proponendo le soluzioni organizzative più opportune.

In particolare, MTA si impegna a:

a. comunicare e condividere con chiarezza percorsi professionali e relative valutazioni, obiettivi di miglioramento per ciascun profilo professionale,
b. rendere omogenei i processi di valutazione dei percorsi di aziendali, così come i meccanismi di incentivazione (economici e non).

### *Equità*

MTA si impegna a promuovere e favorire il riconoscimento del merito sviluppando strumenti di ascolto e dialogo con le persone, strumenti che consentano di tradurre le loro necessità professionali e personali in soluzioni organizzative efficaci, nel rispetto delle esigenze di sostenibilità economica dell'azienda.

### *Coinvolgimento dei collaboratori*

MTA promuove il coinvolgimento delle persone. A tal fine, si impegna a:

- definire con chiarezza i ruoli,
- organizzare incontri periodici per la condivisione degli obiettivi aziendali,
- sviluppare un clima lavorativo positivo, in cui ciascuno possa esprimere le proprie preoccupazioni in buona fede e con correttezza,
- far sì che MTA sia un ambiente capace di attrarre persone motivate e di talento, offrendo loro una occasione di apprendimento basata sull'esperienza attiva e diretta,
- incoraggiare una cultura dello scambio e della condivisione entro l'azienda ed entro i team di lavoro.

### *Rispetto*

MTA tutela l'integrità fisica e morale delle sue persone:

a. garantendo una dimensione di lavoro libero da pressioni e condizionamenti (interni ed esterni) impropri,
b. individuando modalità per prestare attenzione alle necessità delle persone che lavorano in MTA, soprattutto nelle situazioni di difficoltà che possono impedire il normale svolgimento dell'attività lavorativa.

L'azienda fissa, inoltre, le procedure relative ai comportamenti che devono essere tenuti dai collaboratori al fine di minimizzare i rischi di incidenti e, in generale, per salvaguardare la salubrità dell'ambiente di lavoro.

### *Gestione e condivisione della conoscenza*

Ogni collaboratore, al fine di legittimare l'identità professionale di MTA, è chiamato a diffondere informazioni e conoscenza entro l'impresa, senza mai manipolarle o usarle per incrementare il proprio potere personale a danno di coloro che gli sono a fianco oppure a danno dell'impresa stessa.

### *Conflitto di interesse*

Ogni collaboratore deve evitare situazioni in cui possano manifestarsi conflitti di interesse con MTA e deve astenersi dall'avvantaggiarsi personalmente di possibili opportunità di business connesse allo svolgimento delle proprie funzioni.

### *Diligenza nell'utilizzo delle risorse aziendali*

Ogni collaboratore è chiamato ad un uso diligente delle risorse aziendali, al fine di prevenire danni o riduzione dell'efficienza aziendale.

## Responsabilità verso i Soci

### *Creazione di valore*

MTA si impegna alla creazione di valore a medio-lungo termine per i suoi soci attraverso una gestione sostenibile delle proprie attività ed un utilizzo efficiente delle proprie risorse che ne preservi e remuneri equamente l'investimento nel tempo.

### *Reputazione*

MTA tutela il marchio e la reputazione dell'azienda, astenendosi dal compiere azioni che potrebbero screditarne l'immagine. Agisce, inoltre, con integrità in tutte le relazioni istituzionali.

### *Dovere di rendere conto*

MTA assume il dovere di dare conto ai soci della coerenza tra obiettivi annunciati e risultati conseguiti, anche a fronte dell'impegno ad una gestione sostenibile del proprio business.

## Responsabilità verso il sistema delle Società Benefit

### *Interdipendenza*

MTA è consapevole della novità e dell'importanza del cambio di paradigma che l'introduzione delle Società benefit ha apportato al ruolo dell'impresa nell'economia e nella società. Un nuovo paradigma che impegna tutte le Società Benefit a coinvolgersi attivamente nella sua diffusione e nella sua attuazione.

Tale attuazione passa necessariamente da un legame di reciproca interdipendenza fra Società Benefit.

MTA, pur nell'autonomia delle scelte che le sono pertinenti, impronta le proprie relazioni con le altre S.B. alla massima interdipendenza.

### *Apertura alla collaborazione*

MTA, ritenendo che uno dei caratteri dell'interdipendenza, sia l'apertura di ciascuna S.B. alla collaborazione con le altre S.B., è impegnata a collaborare con le altre Società Benefit su tutti i versanti in cui tale collaborazione possa essere funzionale all'affermazione di tale nostro nuovo paradigma economico.

### *Gli ambiti auspicabili della collaborazione*

MTA si impegna a collaborare con le altre S. B. in particolare, ma senza escluderne altri possibili, nei seguenti ambiti di attività:

a. nell'identificare aree di conduzione collaborativa delle attività di business sul mercato
b. nel creare le possibilità di agevolare le attività economiche fra S.B. nella conduzione del business fra S.B.
c. nella ricerca di opportunità di individuazione di benefici comuni che, scelti congiuntamente da più S.B. moltiplichino gli impatti positivi sui destinatari
d. nella creazione di condizioni organizzative e associative affinché le S.B. possano ritrovarsi in un'unica Comunità per meglio tutelare, divulgare, attuare a favore dell'intera società il modello di conduzione dell'attività economica che le caratterizza.

## Responsabilità verso i Clienti

### *Onestà nella relazione*

MTA impronta la relazione con il cliente ad una logica di partnership di medio- lungo termine. Si impegna, tuttavia, ad evitare situazioni di "dipendenza" reciproca che possano frenare la crescita vicendevole.

In tutte le diverse fasi di un intervento consulenziale MTA opererà con la massima onestà intellettuale, eventualmente comunicando, ove se ne ravvisasse la necessità, la propria decisione di uscire dalla relazione col cliente per il bene di quest'ultimo e di MTA.

### *Trasparenza nella relazione*

MTA fornisce solo quei servizi professionali che è nelle sue capacità e competenze rendere, senza mai operare al di sotto di quanto si è impegnata a fare.

### *Equità, efficacia ed efficienza nella relazione*

In ogni momento della relazione consulenziale, MTA garantisce un uso efficace ed efficiente delle risorse del cliente, richiedendo un'equa remunerazione per i servizi resi, pianificando e -successivamente - rendicontando al cliente su costi e risorse effettivamente impegnate sul progetto.

### *Qualità dell'offerta*

MTA si impegna a far evolvere organizzazione, professionalità e cultura avendo come punto di riferimento la qualità dell'offerta consulenziale ed il servizio al cliente.

### *Attenzione ai bisogni del cliente*

MTA, in conformità agli standard di qualità di cui si è dotata, adotta strumenti per il monitoraggio e la valutazione continua della *customer satisfaction*.

Si impegna, inoltre, a tradurre con tempestività le necessità individuali del cliente in adeguate risposte:

a. capitalizzando dalle esperienze pregresse, ma cercando sempre soluzioni *tailor made*, che tengano conto della realtà che si ha di fronte,
b. favorendo la condivisione di eventuali criticità su un progetto in ogni fase del rapporto consulenziale.

### *Comunicazione e informazione "da" e "verso" il cliente*

MTA si impegna a rendere sempre esplicite al cliente le caratteristiche dei prodotti e dei servizi offerti, i loro limiti e potenzialità.

L'azienda gestisce e tutela la riservatezza delle informazioni e dei dati dei clienti di cui entra in possesso. Ogni collaboratore dell'azienda, in particolare, non utilizzerà informazioni confidenziali per scopi personali e agirà con oculatezza quando lavorerà con un competitor del cliente.

### *Indipendenza*

MTA agisce con correttezza ed integrità, proteggendo la fiducia dei suoi clienti e facendo in modo che la propria indipendenza non venga compromessa o venga, in qualche modo, percepita come tale.

In nessun caso, sottoporrà il cliente a pressioni indebite per ottenere l'affidamento di un incarico professionale.

### *Sostenibilità*

Avendo scelto la sostenibilità come orientamento strategico, MTA si impegna, ove ve ne fossero le condizioni, a proporre ai propri clienti soluzioni organizzative che vadano nella direzione di coniugare la massimizzazione del profitto con una migliore gestione degli impatti sociali ed ambientali della propria attività.

## Responsabilità verso i Fornitori

### *Rapporto coi fornitori*

MTA opera perché si creino, specialmente coi fornitori di servizi di consulenza partner su taluni progetti, rapporti di cooperazione finalizzati allo scambio di informazioni e competenze reciproche per la creazione di valore comune e condiviso verso il cliente.

### *Correttezza nella relazione*

MTA improntа la relazione coi fornitori alla correttezza e alla disponibilità e si impegna a rispettare i tempi e le modalità di pagamento convenute. Al verificarsi di eventi imprevisti che portassero a modificare le condizioni contrattuali iniziali, MTA non sfrutterà il proprio margine di discrezionalità per imporre condizioni inique ai fornitori.

### *Criteri di selezione dei fornitori*

Nella fase di approvvigionamento di beni e servizi, MTA ricerca sempre qualità ed economicità dell'offerta, riconoscendo pari opportunità ai fornitori, attraverso l'utilizzo di criteri di valutazione e qualificazione oggettivi e imparziali.

### *Regali e benefici*

MTA evita ogni forma di pagamento illecito a fornitori o loro rappresentanti e non elargisce benefici e/o regali intesi ad ottenere speciali condizioni di favore. Parimenti, respinge benefici e/o regali dei fornitori intesi a ottenere condizioni di favore.

## Responsabilità verso il Territorio

### *Ambiente*

MTA considera la tutela e la salvaguardia dell'ambiente come una delle sue più grandi responsabilità sul fronte della sostenibilità.

A tal fine, si impegna:

a. a promuovere una attività di sensibilizzazione e a mettere in atto una serie di iniziative finalizzate a ridurre l'impatto ambientale diretto delle proprie attività,
b. a sensibilizzare le organizzazioni sue clienti, perché sviluppino azioni e strumenti volti ad una significativa riduzione dell'impatto ambientale delle loro attività.

### *Attenzione alla Comunità*

MTA vuole diventare un soggetto riconosciuto della comunità in cui opera, un punto di riferimento per le nuove generazioni, un interlocutore autorevole del mondo accademico e della ricerca locale e nazionale.

A tal fine, si impegna a potenziare la propria presenza nei contesti istituzionali e a sviluppare partnership innovative con attori chiave del contesto socio-economico locale, nazionale ed internazionale, che innalzino la competitività e la sostenibilità del territorio.

### *Cittadinanza responsabile*

MTA si impegna ad agire come "cittadino" responsabile, ascoltando i bisogni del territorio in cui è chiamata via via ad operare e mettendo a disposizione della propria comunità competenze ed esperienze maturate nel tempo.

Lo sviluppo locale dovrà essere promosso attraverso la selezione di iniziative attente alle reali esigenze delle comunità e del territorio, in coerenza con l'obiettivo della creazione di valore sostenibile.

## Responsabilità verso le Istituzioni

Gli amministratori, i soci e i collaboratori di MTA agiscono verso le istituzioni con integrità e lealtà. Nel rispetto delle leggi e delle norme, codificate o meno, di una convivenza civile improntata alla collaborazione per il bene comune.

# Allegato 1 al CODICE ETICO E DI COMPORTAMENTO

# - POLICY ANTICORRUZIONE –

## Premessa

More Than Access S.r.l. Società Benefit (di seguito anche "MTA" o "l'Azienda") intende promuovere e consolidare al proprio interno una cultura improntata all'etica e all'integrità finalizzata ad assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione ed immagine, delle aspettative dei propri *stakeholder* (dipendenti, clienti, fornitori, Stato e istituzioni, collettività, ecc.), nella convinzione che l'assoluto rispetto di questi valori rappresenti una premessa indispensabile ai fini del raggiungimento degli obiettivi aziendali di eccellenza.

MTA è consapevole dell'importanza di dotarsi di un sistema di controllo interno idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri amministratori, dipendenti, ecc. e pertanto le Linee guida Anticorruzione hanno l'obiettivo di fornire un quadro sistematico di riferimento delle norme e delle procedure in materia di anticorruzione, di definire ruoli e responsabilità, nonché dettare presidi di prevenzione e di controllo in relazione alla gestione dei rapporti con le Pubbliche Amministrazioni e con gli Enti Privati, al fine di prevenire, nell'esecuzione dell'attività di impresa, la commissione di atti corruttivi che possono danneggiare gravemente l'immagine dell'Azienda, nonché comportare la responsabilità civile e penale dei collaboratori coinvolti.

La presente Policy è redatta nel rispetto dei principi indicati dal Codice Etico adottato da MTA, delle leggi, dei regolamenti e degli standard internazionali previsti in materia di anticorruzione.

## Definizioni

- *"Corruzione"*: per corruzione si intende l'offerta o la consegna, la sollecitazione o la ricezione, in modo diretto o indiretto, di un indebito vantaggio in denaro o di altra natura, a o da un'altra persona, cosicché quest'ultima, violando i propri doveri:
  - agisca o si astenga dall'agire o perché ha agito o si è astenuta dall'agire; o
  - abusi della propria influenza reale o presunta o perché ha abusato della propria influenza reale o presunta;

  allo scopo di ottenere o di conservare un affare o qualsiasi altro vantaggio inappropriato o improprio nell'ambito delle attività esercitate.
- *"Destinatari"*: Organi societari (Amministratori e Sindaci), Dipendenti, fornitori, consulenti, procuratori, outsourcer e altri soggetti con cui l'Azienda entri in contatto nello svolgimento di relazioni d'affari.
- *"Direzione"*: l'Amministratore Unico, i Soci, il Managing Director ed il *Senior Management* dell'Azienda, in funzione del senso della frase di riferimento.
- *"Evento"*: un evento di lavoro, un evento sociale o una commistione tra questi due tipi di eventi cui partecipi (tra gli altri) un Destinatario. Le tre categorie di evento sono qui di seguito definite: gli eventi di lavoro sono finalizzati alla creazione di una rete di conoscenze, alla trattazione di tematiche professionali e lavorative ed in essi sono trattati argomenti inerenti il business aziendale ad esempio si tratta di dimostrazioni, conferenze, presentazioni, seminari, attività promozionali, interventi, fiere dedicate a operatori professionali e/o attività di vendita di prodotti e servizi e possono includere la somministrazione

di cibi e bevande; gli eventi sociali sono finalizzati alla creazione di relazioni e sono incentrati su tematiche relative alla socializzazione quali ritrovi o eventi sportivi organizzati a livello aziendale, eventi culturali, ricreativi, o inerenti qualsivoglia altro tipo di relazione interpersonale, possono includere somministrazione di cibi e bevande e non possono durare oltre le 24 ore; gli eventi commisti sono indirizzati contemporaneamente sia alla creazione di reti di conoscenze e alla trattazione di argomenti professionali e lavorativi che alla costruzione di relazioni, possono includere la somministrazione di cibi e bevande.

- *"Partner"*: soggetti con cui l'Azienda entra in contatto nello svolgimento di relazioni d'affari e, più precisamente, dealer che si avvalgono, per la vendita dei prodotti e/o servizi offerti, di un network costituto da una pluralità di soggetti aventi o meno una propria autonomia giuridica. In quanto tale, il Partner è un Destinatario.
- *"Personale"*: tutte le persone fisiche che intrattengono con l'Azienda un rapporto di lavoro, inclusi i lavoratori dipendenti, interinali, i collaboratori, gli "stagisti" ed i liberi professionisti che abbiano ricevuto un incarico da parte dell'Azienda.
- *"Pubblica Amministrazione"* o *"P.A."*: per Amministrazione Pubblica si deve intendere:
  - lo Stato (o Amministrazione Statale);
  - o gli Enti Pubblici; si specifica che l'Ente Pubblico è individuato come tale dalla legge oppure è un Ente sottoposto ad un sistema di controlli pubblici, all'ingerenza dello Stato o di altra Amministrazione per ciò che concerne la nomina e la revoca dei suoi amministratori, nonché l'Amministrazione dell'Ente stesso. È caratterizzato dalla partecipazione dello Stato, o di altra Amministrazione Pubblica, alle spese di gestione; oppure dal potere di direttiva che lo Stato vanta nei confronti dei suoi organi; o dal finanziamento pubblico istituzionale; o dalla costituzione ad iniziativa pubblica. A titolo puramente esemplificativo e non esaustivo sono da considerarsi Pubbliche Amministrazioni in senso lato le seguenti Società: Ferrovie dello Stato, Autostrade SpA, AEM Milano, ecc.
  - Pubblico Ufficiale: colui che esercita "una pubblica funzione legislativa, giudiziaria o amministrativa". Agli effetti della legge penale "è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi" (art. 357 c.p.);
  - Incaricato di Pubblico Servizio: colui che "a qualunque titolo presta un pubblico servizio. Per pubblico servizio deve intendersi 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 di ordine e della prestazione di opera meramente materiale" (art. 358 c.p.). Si rappresenta che "a qualunque titolo" deve intendersi nel senso che un soggetto esercita una pubblica funzione, anche senza una formale o regolare investitura (incaricato di un pubblico servizio "di fatto"). Non rileva, infatti, il rapporto tra la P.A. e il soggetto che esplica il servizio.
- *"Regalo"*: Qualsiasi tipo di dono, prodotto, erogazione liberale o beneficio (inclusa qualsiasi cosa che abbia un valore nominale) che è dato o ricevuto. Non sono compresi in tale definizione le Spese di rappresentanza o gli Eventi. Si considerano Regali di modico valore i doni, prodotti, gratuità o benefici di importo non superiore a € 50,00.
- *"Senior Management"*: i soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Azienda o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale.
- *"Sistema Disciplinare"*: l'insieme delle misure sanzionatorie applicabili in caso di violazione delle regole procedimentali e comportamentali previste dal Modello.
- *"Spese di rappresentanza"*: l'insieme delle cortesie adottate nell'ambito della usuale gestione delle attività lavorative in cui possono rientrare cibi e bevande.

- ***"Utilità"***: qualsiasi cosa abbia valore, ogni sorta di beneficio incluso, ma non limitato, a denaro, prestiti, obbligazioni, diritti contrattuali o interessi, beni immobili, beni personali, o altri interessi nascenti da una relazione di lavoro, regali, svaghi, pranzi, spese di rappresentanza, contributi o donazioni, viaggi e relative spese, sconti al di sotto del valore di mercato, rimborsi, ribassi, trattamenti privilegiati nella fornitura, o accesso privilegiato a opportunità di business, beni, servizi che non abbiano una ragionevole giustificazione commerciale, o costituiscano un incentivo improprio. Nella definizione "Utilità" è compresa, inoltre, l'offerta di un impiego.

## Policy

MTA ha una posizione di assoluta intransigenza nei confronti di qualsiasi forma di corruzione, anche nei confronti di personale di imprese private. Questa posizione contribuisce al rispetto degli impegni cui l'Azienda si è volontariamente vincolata anche attraverso la formalizzazione del proprio Codice Etico e di Comportamento. Tutto il Personale è tenuto, nello svolgimento delle attività di lavoro, ad assumere una posizione di ferma opposizione rispetto ad ogni forma di abuso d'ufficio e corruzione.
MTA e i Destinatari si impegnano al fine di assicurare che tutte le leggi e i regolamenti che mirano a contrastare la corruzione, in ogni giurisdizione in cui si opera, siano rispettati nella loro totalità.

## Applicazione

Tutti i Destinatari sono tenuti a operare conformemente alla presente policy qualora agiscano in nome o per conto dell'Azienda.

## Regole e principi di condotta

Di seguito sono definiti gli standard di comportamento che devono essere osservati dall'Azienda e dal Personale, al fine di assicurare un approccio "tolleranza zero" nei confronti di comportamenti corruttivi riguardanti esponenti della Pubblica Amministrazione e personale di imprese private.

### *1. Divieto di corruzione in ogni sua forma e raccomandazioni generali*

Qualsiasi atto illecito e di corruzione è vietato. I Destinatari non devono:

- direttamente o indirettamente offrire denaro od altra Utilità ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori o a sottoposti alla direzione o vigilanza dei predetti soggetti, di Società clienti o fornitrici, o di altro ente, al fine di ottenere un interesse o vantaggio di qualsiasi tipo, tra cui ottenere o mantenere vantaggi in termini di business/affari per o per conto di MTA;
- direttamente o indirettamente richiedere o accettare denaro o altra Utilità da parte di clienti, fornitori, o di altro soggetto o ricercare un vantaggio di qualsiasi tipo in cambio.

È inoltre vietato qualsiasi comportamento consistente, a titolo esemplificativo e non esaustivo, in:

- offrire, suggerire, autorizzare l'offerta o il pagamento di denaro o altra Utilità al fine di indurre o remunerare un abuso d'ufficio di una funzione o attività, pubblica o privata;
- pagare o approvare il pagamento di denaro o altra Utilità al fine di indurre o remunerare un abuso d'ufficio di una funzione o attività, pubblica o privata;
- accettare o sollecitare pagamento di denaro o altra Utilità al fine di indurre o remunerare abuso d'ufficio di una funzione o attività, pubblica o privata;

- utilizzare fondi di cui si sappia o si sospetti essere di provenienza di un reato;
- assistere o partecipare al compimento di qualsiasi attività costituente reato;
- stabilire, definire consapevolmente o mantenere processi o procedure o schemi con l'intento di effettuare pagamenti illeciti;
- intraprendere qualsiasi attività con consumatori, clienti, fornitori, partner commerciali e altre terze parti che possa costituire reato.

A titolo esemplificativo, le seguenti attività possono configurare Corruzione:

- la dazione di denaro o altra Utilità al fine di ottenere una opportunità di lavoro;
- la corresponsione di denaro o altra Utilità a un dipendente di una persona giuridica al fine di ottenere informazioni confidenziali;
- l'accettazione di regali sproporzionati da un fornitore di servizi.

È vietato eludere le suddette prescrizioni ricorrendo a forme diverse di aiuti e contribuzioni che, nella forma di, ad esempio, sponsorizzazioni, incarichi, consulenze, pubblicità, perseguano le stesse finalità sopra vietate.
Ciascun Destinatario che accetti richieste, sollecitazioni o autorizzi qualcuno ad accettare o sollecitare, direttamente o indirettamente qualsiasi vantaggio economico o altra Utilità da chiunque (cd. corruzione passiva) è esposto alle stesse sanzioni di colui che offra, prometta, dia, paghi, autorizzi qualcuno a dare o pagare, direttamente o indirettamente, un vantaggio economico o altra Utilità a un Pubblico Ufficiale o a un soggetto privato (cd. corruzione attiva).

Atti illeciti e corruzione possono esporre a responsabilità penale personale e a responsabilità in capo all'Azienda ai sensi del D. Lgs. 231/2001.
Se un dipendente si trova di fronte al bivio tra essere coinvolto in una attività che comporti la commissione di un atto illecito e concludere, attraverso lo sfruttamento di tale attività, un affare nell'interesse o a vantaggio dell'Azienda, questi deve scegliere di rinunciare all'affare.

## *2. Spese di rappresentanza*

Le Spese di Rappresentanza devono avere un obiettivo commerciale appropriato, devono comportare una attinenza con qualche forma di attività lavorativa e debbono essere gestite dalle Funzioni aziendali nei limiti della presente Policy.

## *3. Regali, Intrattenimenti commerciali ed Eventi, Pranzi di lavoro*

I Destinatari (o chiunque per loro conto) non devono:

- dare o ricevere alcun Regalo;
- offrire o accettare di partecipare a intrattenimenti commerciali, eventi o altre forme di ospitalità che potrebbero:
  - costituire motivo di influenza o di incentivo improprio (tenuto conto anche del loro costo), tra cui ad esempio, l'aspettativa di ricevere un vantaggio di business o di ottenere un ringraziamento per un vantaggio già ottenuto ovvero potrebbero essere percepite come tali;
  - consistere in regali e/o partecipazioni ad eventi commerciali per amici o parenti dei Destinatari;
  - violare leggi e regolamenti o procedure dell'Azienda.

Quando si offrono o si ricevono Regali di non modico valore o si organizza/si accetta di partecipare a intrattenimenti di lavoro ed eventi devono essere rispettati anche i seguenti principi:

- la causale sottesa al Regalo, all'intrattenimento di lavoro o all'evento deve essere strettamente correlata al *business* (ad esempio: lo sviluppo della relazione commerciale o la promozione dei prodotti e dei servizi di MTA);
- questi devono essere modesti e ragionevoli in valore, appropriati in tutte le circostanze e tali da non compromettere l'integrità e la reputazione dell'Azienda. In ogni caso, i regali non devono essere percepiti come effettuati al fine di esercitare pressione o comunque un'impropria influenza. In tale contesto, assumono rilevanza, ad esempio, la tempistica del Regalo, il fatto che sia stato effettuato in maniera trasparente ed il destinatario prescelto.
- questi devono essere coerenti con il contesto dell'occasione di business e in accordo con le pratiche abituali aziendali.
- questi devono essere trasparenti e discussi apertamente. In altre parole, se comunicati alle società di informazione, non devono causare imbarazzo per il destinatario né per l'Azienda;
- questi devono essere organizzati temporalmente in modo appropriato. In altre parole, non devono coincidere con la partecipazione ad un'offerta commerciale, con il processo di acquisizione di un potenziale business, o con qualsiasi momento decisionale relativo a nuovi business/transazioni;
- questi devono essere coerenti con tutti i requisiti di questo documento e per gli stessi tutte le autorizzazioni devono essere state ottenute (vedi sotto).

Per evitare qualsiasi dubbio, il dare/ricevere Regali di non modico valore e in ogni caso l'organizzazione/ partecipazione a intrattenimenti commerciali ed eventi sono vietati sia se fatti direttamente (in prima persona) che indirettamente (attraverso parti terze), salvo espressa autorizzazione della Direzione.
La Direzione, ricevuta la richiesta, può decidere di non darvi seguito, qualora essa non risponda alla policy aziendale, ovvero di esprimere il proprio parere favorevole (eventualmente con alcune riserve o commenti). Pranzi offerti a/da clienti, consulenti o fornitori effettivi e potenziali che siano di valore ragionevole, occasionali e comunque offerti in connessione e in occasione di incontri lavorativi sono ammessi.
Per nessun motivo Regali ed Eventi devono essere offerti ad esponenti della Pubblica Amministrazione, soggetti referenti di Società concessionarie, amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori o a sottoposti alla direzione o vigilanza dei soggetti citati.

## *4. Utilizzo di Terze Parti*

I Destinatari devono prestare attenzione quando si seleziona e/o si opera con soggetti terzi (agenzie, Società di intermediazione, ecc.). MTA, infatti, può essere ritenuta responsabile per atti illeciti e corruzione commessi da tali terzi soggetti.

L'impiego di soggetti terzi deve essere valutato attentamente per controllare che sia coerente con i seguenti principi:

- la natura della transazione e delle attività oggetto del rapporto con i soggetti terzi, in ragione delle pratiche locali deve essere coerente e conforme alle leggi o regolamenti applicabili;
- le condizioni di impiego dei suddetti soggetti terzi (in modo particolare l'assegnazione e le modalità di compenso) sono chiaramente definite e sancite in accordi scritti;
- la proposta remunerazione deve essere coerente con i servizi che sono resi, sia in assoluto che in relazione al valore del business in oggetto.

MTA proibisce a qualsiasi Destinatario o soggetto terzo di dare, promettere di dare, offrire denaro o altra Utilità ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori o a sottoposti alla direzione o vigilanza dei soggetti citati nell'interesse o a vantaggio della medesima Azienda.

Nessun Destinatario deve dare o promettere denaro o altra Utilità ad un soggetto terzo, sapendo che parte o tutto del valore verrà trasferito ad uno dei soggetti sopra citati in violazione di questa procedura.

### *5. Erogazioni Liberali e Sponsorizzazioni*

Erogazioni Liberali e Sponsorizzazioni ad associazioni e altre organizzazioni non profit sono permesse, ma strettamente monitorate dalla Direzione.
Dal momento che le Erogazioni Liberali e le Sponsorizzazioni possono configurarsi come atti prodromici alla corruzione se concesse impropriamente e senza il rispetto dei limiti previsti dalle procedure, queste sono concesse solo se:

- non effettuate allo scopo di ottenere un vantaggio indebito o di influenzare una decisione;
- l'Azienda non riceva e non vi sia alcun sospetto che riceva alcuna contropartita impropria in cambio;
- effettuate in maniera trasparente;
- effettuate ad un'organizzazione che goda di una buona reputazione (ossia, sia registrata presso le autorità del Paese in cui opera, nota alle autorità fiscali).

In ogni caso, qualsiasi donazione effettuata in favore di un'organizzazione senza scopo di lucro dovrà essere sottoposta all'autorizzazione preventiva da parte della Direzione.

### *6. Finanziamenti ai partiti politici*

MTA mantiene una posizione politica neutrale e rifiuta qualsiasi finanziamento diretto o indiretto ai partiti politici, anche nel caso tale azione sia autorizzata dalla giurisdizione locale. MTA e il Personale non sono autorizzati a effettuare donazioni politiche.

## Ruoli e Responsabilità

I Soci, la Direzione e il Personale di MTA devono assicurare di aver letto e di osservare la presente Policy Anticorruzione. La prevenzione, l'individuazione e l'informazione relativa a comportamenti illeciti e a forme di corruzione sono responsabilità di tutti coloro che, Dipendenti o altri Destinatari, operino per conto dell'Azienda.
La Direzione, e in particolare il Managing Director, ha la responsabilità di identificare, monitorare e controllare i rischi di concussione e corruzione, anche con il supporto di consulenti legali. Il Managing Director è responsabile di garantire l'effettiva attuazione della presente Policy approvata dall'Amministratore Unico. Il Managing Director lavora per raggiungere l'obiettivo di garantire che tutti i Destinatari si astengano dall'attuare comportamenti che possono configurare illeciti o corruzione e siano tutti ben consapevoli dei requisiti normativi applicabili, promuovendo una forte cultura anticorruzione in tutta l'organizzazione.
Tutti i Destinatari devono evitare qualsiasi attività che potrebbe suggerire o condurre a violare la presente Policy.
I Destinatari, non appena possibile, devono segnalare alla Direzione i casi in cui ritengano o sospettino si sia verificata o si verificherà in futuro una violazione del presente codice comportamentale.
MTA o qualunque altro Destinatario non deve mettere in atto forme di ritorsione nei confronti di chiunque abbia rifiutato di commettere comportamenti o atti in violazione del presente codice comportamentale.
I Destinatari possono ottenere chiarimenti in relazione a dubbi circa l'applicabilità della presente procedura o la valutazione dei comportamenti che possono configurare illeciti o corruzione rivolgendosi alla Direzione.
I Destinatari devono comunicare alla Direzione se ritengono di aver proposto un accordo corruttivo, gli è stato chiesto di farlo, sospettano che potrebbe accadere in futuro.
I Destinatari che rifiutano di accettare o proporre un accordo corruttivo, o quelli che sollevano interrogativi o riferiscono un fatto illecito di un altro dipendente, non dovranno temere eventuali ripercussioni.

MTA è tenuta ad assicurare che nessuno subisca trattamenti lesivi come conseguenza del rifiuto di prendere parte ad un accordo corruttivo o dell'avere riferito in buona fede un fondato sospetto relativo ad una effettiva, potenziale o futura corruzione.
I Soci, la Direzione e il Personale devono essere consapevoli dell'impegno assunto da MTA nei confronti della lotta ai comportamenti illeciti e alla corruzione. Tutti i Destinatari dovranno quindi agire nel rispetto delle leggi, dei regolamenti, del Codice Etico e di Comportamento, nonché della presente Policy Anticorruzione.

## Informazione e consapevolezza

MTA dovrà:

- garantire la conoscenza da parte del Personale della presente Policy attraverso un'opportuna attività di comunicazione e formazione;
- prevedere un'attività di formazione obbligatoria nei confronti di tutti i dipendenti e i collaboratori in ordine ai principi di cui al presente codice comportamentale.

MTA, nei rapporti con i soggetti terzi, laddove possibile, inserirà nei contratti apposite clausole che informano sulle politiche e le procedure adottate, nonché sulle conseguenze che comportamenti contrari a tali documenti possono avere con riguardo ai rapporti contrattuali stessi.

## Segnalazioni

Si faccia riferimento alla specifica "Procedura Whistleblowing" redatta nel rispetto della Direttiva UE 2019/1937 e del D.Lgs. n. 24/2023.

## Le sanzioni

L'inosservanza dei principi contenuti nella presente Policy può comportare l'applicazione delle misure sanzionatorie contenute nel Sistema Disciplinare aziendale e/o previste dalle prassi aziendali, nell'osservanza della rigida applicazione del Contratto di lavoro.

# Allegato 2 al CODICE ETICO E DI COMPORTAMENTO

## - *FAIR COMPETITION POLICY* -

## L'impegno di MTA

La presente *Fair Competition Policy* ("Policy") stabilisce che More Than Access S.r.l. Società Benefit (di seguito anche "MTA" o "l'Azienda") si aspetta una concorrenza leale e aperta da parte dei propri dipendenti e collaboratori che conducono qualsiasi attività per conto di MTA, per mezzo di pratiche commerciali oneste e trasparenti che rispettino la disciplina comunitaria in materia di concorrenza e *antitrust*, e la disciplina nazionale introdotta dalla Legge N. 287/1990 ("*Norme per la tutela della concorrenza e del mercato*").

MTA ritiene che una concorrenza leale in mercati aperti spinga l'Azienda a fare il miglior uso delle proprie risorse e a trovare idee innovative per sviluppare nuovi modi di fare *business* e acquisire clienti. Pratiche commerciali professionali, oneste e dirette sono in grado di proteggere la reputazione di MTA e garantiscono che MTA e i suoi dipendenti e collaboratori non violino le leggi sulla concorrenza, che prevedono sanzioni severe.

La presente Policy è stata redatta nel rispetto delle Linee Guida sulla *compliance antitrust* fornite dell'Autorità Garante della Concorrenza e del Mercato e di Confindustria, al fine di prevenire la commissione di illeciti *antitrust* nello svolgimento dell'attività di impresa.

Affinché il rispetto delle regole di concorrenza costituisca parte integrante della cultura e della politica aziendale, tutti i dipendenti e collaboratori di MTA sono messi nelle condizioni di conoscere approfonditamente le regole in vigore sulla concorrenza e i rischi legati all'*antitrust* connessi alla propria attività grazie allo svolgimento di attività di formazione continua da parte di risorse interne e di consulenti esterni.

MTA si avvale di un processo in quattro fasi per valutare e gestire eventuali rischi inerenti al rispetto delle leggi sulla concorrenza previste dall'ordinamento italiano e in linea con le *best practice* europee:


**Core – *Commitment* alla conformità**: il *Senior Management*, in particolare l'Amministratore Unico, deve dimostrare un impegno chiaro e inequivocabile per il rispetto delle leggi sulla concorrenza, promuovendo il processo volto a prevenire e scongiurare la commissione di infrazioni *antitrust*.
**Fase 1 – Identificazione del rischio**: si identificano i rischi legati al diritto della concorrenza affrontati da MTA.

**Fase 2 – Valutazione del rischio**: si determina la gravità dei rischi identificati (spesso è più semplice valutarli come bassi, medi o alti). MTA valuta quali dipendenti o collaboratori si trovano in aree ad alto rischio, come ad esempio quelli che hanno probabili contatti con *competitor*.
**Fase 3 – Mitigazione del rischio**: si definiscono policy, procedure e formazione adeguate con l'obiettivo che i rischi identificati non si verifichino, assicurandosi al tempo stesso di rilevarli e affrontarli nel caso in cui si verifichino.
**Fase 4 – Revisione**: si rivedono regolarmente le fasi 1-3 ed il *commitment* alla conformità, per garantire l'efficacia del processo. Eventuali revisioni straordinarie, potrebbero rendersi necessarie ad esempio in caso di modifiche sostanziali all'organizzazione o alle modalità di svolgimento dell'attività.

## Pratiche sleali e comportamenti anticoncorrenziali

I dipendenti e i collaboratori di MTA non devono intraprendere o dare l'impressione di intraprendere alcuna azione che possa escludere o ridurre ingiustamente la concorrenza in qualsiasi mercato. I dipendenti e i collaboratori non devono travisare, manipolare, nascondere, utilizzare in modo improprio informazioni riservate e non devono intraprendere discorsi denigratori nei confronti dei *competitor* o pratiche sleali con azionisti, clienti, partner commerciali, *competitor* e altri dipendenti e collaboratori. I dipendenti e i collaboratori devono ottenere informazioni sui *competitor*, sui loro prodotti, servizi, tecnologie, prezzi, campagne di marketing, ecc. solo attraverso mezzi legali ed etici.

Inoltre, i dipendenti e i collaboratori non devono far partecipare MTA ad accordi commerciali o a comportamenti di cartello volti a eliminare o scoraggiare la concorrenza o a conferire un vantaggio competitivo inappropriato. Le attività vietate includono, a titolo esemplificativo e non esaustivo, accordi di fissazione dei prezzi, boicottaggio illegale di fornitori o clienti, manipolazione delle offerte, condotta di cartello, pratiche predatorie, trattative esclusive, abuso di potere di mercato, controllo della produzione o limitazione della fornitura di beni e servizi, pratiche concertate, segnalazione dei prezzi, fissazione dei prezzi per eliminare un *competitor*, stipula di un accordo o di un'intesa con i *competitor* per dividersi un mercato, scambio di informazioni riservate, ecc.

Le forme più comuni di condotta vietata sono descritte di seguito. I dipendenti e i collaboratori devono chiedere consiglio al management in caso di dubbi sul fatto che un'azione possa essere considerata una pratica sleale o un comportamento anticoncorrenziale.

### *Manipolazione delle offerte*

La manipolazione delle offerte si verifica quando due o più *competitor* coordinano le offerte, per cui ad esempio uno o più *competitor* si accordano per non presentare un'offerta, per ritirare un'offerta o per presentare un'offerta raggiunta di comune accordo, senza che l'ente che richiede l'offerta sia informato dell'accordo stipulato tra le parti.

### *Fissazione dei prezzi e segnalazione dei prezzi*

La fissazione dei prezzi è un accordo (scritto, verbale o desunto dal comportamento) tra *competitor* che aumenta, abbassa o stabilizza i prezzi o le condizioni di concorrenza. La fissazione dei prezzi si verifica ogni volta che due o più *competitor* si accordano per intraprendere azioni che hanno l'effetto di aumentare, abbassare o stabilizzare il prezzo di qualsiasi prodotto o servizio senza alcuna giustificazione legittima, o quando alcuni *competitor* si accordano per eliminarne altri. La segnalazione dei prezzi si verifica quando i *competitor* concordano metodi per segnalarsi reciprocamente i prezzi al fine di coordinare le vendite a prezzi uniformi.

### *Ripartizione del mercato*

La ripartizione del mercato si verifica quando i *competitor* si accordano per dividere o assegnare i clienti o i mercati geografici, o per limitare la produzione di un prodotto fissando quote tra i *competitor* o con altri mezzi, piuttosto che prendere decisioni indipendenti su dove operare, da chi rifornirsi e quali clienti perseguire. La

ripartizione del mercato comprende la ripartizione dei clienti per area geografica, l'accordo di non competere per i clienti dell'altro (accordi cosiddetti *no-poach*) e l'accordo di non entrare/espandersi nel mercato di un *competitor*.

### *Scambio anticoncorrenziale di informazioni riservate*

Lo scambio vietato di informazioni riservate (come prezzi, costi o profitti) si verifica quando le parti in concorrenza tra loro, anche se contemplano una transazione o lo scambio di informazioni in un altro contesto, intraprendono discussioni o scambi di informazioni che hanno un impatto negativo sulla concorrenza tra loro.

### *Abuso di posizione dominante*

L'abuso di posizione dominante (o abuso di potere di mercato) si verifica quando un'impresa o un gruppo di imprese in posizione dominante impedisce o riduce in modo sostanziale la concorrenza, compiendo atti volti a eliminare o disciplinare i *competitor* o semplicemente a impedire ai potenziali *competitor* di entrare in un mercato. L'abuso di posizione dominante si verifica anche quando una parte controlla la produzione o limita la fornitura di beni e servizi per limitare la concorrenza. Esempi di atti che possono costituire abuso di posizione dominante sono la compressione sleale dei margini o la vendita di servizi sottocosto per eliminare dal mercato gli altri *competitor*.

## Interazioni con i *competitor*

MTA e i suoi dipendenti e collaboratori devono assicurarsi che le discussioni o lo scambio di informazioni riservate non portino ad accordi illeciti, anche verbali, in particolare in occasione di eventi commerciali e incontri informali e sociali. In tutte le circostanze in cui la discussione tra *competitor* è prevalente, i dipendenti e i collaboratori devono:

a. evitare di scambiare informazioni con un *competitor* su prezzi, costi, profitti, tariffe, termini contrattuali o di offerta, oneri, commissioni o sconti applicabili a clienti, appaltatori o fornitori attuali o futuri; e sull'assegnazione di lavoro, mercati, territori o clienti.
b. evitare di fare dichiarazioni che creino, implichino o suggeriscano ad altri l'esistenza di un accordo anticoncorrenziale con un *competitor*.

Gli accordi di *teaming*, *joint venture* o consorzio sono esempi di collaborazione legale tra *competitor* naturali, che possono svolgere un ruolo positivo in un ambiente di concorrenza leale. Tuttavia, quando si presenta l'opportunità di un rapporto di *teaming*, *joint venture* o consorzio, i dipendenti e collaboratori devono prestare attenzione al tipo di informazioni che vengono scambiate e al momento in cui vengono scambiate.

In generale, le leggi sulla concorrenza vietano tutti gli accordi per fissare i prezzi, ripartire i mercati o limitare la produzione che non siano attuati nell'ambito di una collaborazione, un'alleanza o una *joint venture* legittima.
I dipendenti e i collaboratori non devono scambiare informazioni riservate come prezzi, costi o profitti con i *competitor* senza un'autorizzazione adeguata e devono ottenere la revisione del *management* prima di concordare un prezzo relativo a un'offerta con un *competitor* in qualsiasi circostanza.
Se un dipendente o un collaboratore si trova a partecipare a una riunione o a una conversazione che coinvolge *competitor* in cui si discute di comportamenti o azioni anticoncorrenziali deve immediatamente allontanarsi dalla situazione, quindi documentare la preoccupazione e consultare il *management*, che lo aiuterà a determinare se sono necessarie ulteriori indagini e misure precauzionali.

## Non conformità

MTA applica un approccio "tolleranza zero" a tutte le forme di pratica sleale o comportamenti anticoncorrenziali commessi da dipendenti, collaboratori o partner commerciali che agiscono per suo conto. L'adozione di comportamenti anticoncorrenziali costituisce una violazione del Codice Etico e di Comportamento e della presente Policy e le conseguenze possono comportare l'applicazione di una sanzione disciplinare, compreso il

licenziamento. In aggiunta, la violazione delle leggi sulla concorrenza può avere conseguenze legali e regolamentari, tra cui responsabilità civile e penale, sanzioni per MTA e i suoi dipendenti e collaboratori, danni alla reputazione e l'esclusione di MTA dalle logiche commerciali dei propri clienti.

## Dove rivolgersi per dubbi o ulteriori informazioni

I dipendenti e i collaboratori di MTA possono chiedere chiarimenti al *Senior Management* in caso di dubbi sul fatto che una condotta possa avere natura anticoncorrenziale e circa qualsiasi aspetto connesso alla presente Policy.

## Segnalazione di violazioni sospette

Le informazioni su possibili violazioni di questa Policy da parte di MTA, dei suoi dipendenti o di qualsiasi terza parte con cui MTA conduce o prevede di condurre affari devono essere segnalate tempestivamente. I dipendenti e i collaboratori possono segnalare i sospetti di cattiva condotta al proprio responsabile diretto o al *Senior Management*, anche in modo confidenziale e anonimo.

# Allegato 3 al CODICE ETICO E DI COMPORTAMENTO

# - REGOLAMENTO INTERNO PER UN CORRETTO UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI –

Regole di condotta ed obblighi dei collaboratori in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica redatto anche ai sensi del "Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati" (da ora in poi GDPR) e del provvedimento del Garante della Privacy (Deliberazione n. 13 del 1/3/2007 - pubblicata sulla GU n. 58 del 10 marzo 2007) comprensivo di alcuni controlli richiesti dalla ISO 27001 e note per la gestione dei dati cartacei.

# INDICE DE CONTENUTI

# 1. SEZIONE I – AMBITO GENERALE

## 1.1. Definizioni

Azienda/Organizzazione: La ragione sociale indicata in testata al presente documento.
Dipendente: personale dell'ente assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.
Disciplinare: Disciplinare per l'utilizzo degli strumenti informatici, di internet e della posta elettronica. E' il presente documento.

Device: Qualsiasi computer (workstation o laptop) smartphone, tablet o altro tipo di dispositivo elettronico (comprese chiavette usb, hard disk, smart card o altri sistemi di memorizzazione o di gestione dei dati).

GDPR: Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati.
Incaricato: ogni dipendente, come sopra identificato, ed ogni altra persona fisica (collaboratore, libero professionista, ...) che sotto il controllo dell'Azienda, nell'ambito dell'attività assegnatagli, tratta dati (nell'accezione del capitolo seguente) gestiti dall'Azienda stessa.

NDA: non disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali e con il quale le parti si impegnano a mantenerle segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.

## 1.2. Premessa

L'ambito lavorativo porta la nostra Azienda a gestire una serie di "informazioni", proprie e di terzi, per poter erogare i servizi che le vengono contrattualmente richiesti.

Tali informazioni possono essere considerate, ai sensi del GDPR, "dati personali" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l'Azienda adotti una serie di adeguate misure tecniche ed organizzative atte a proteggere tali dati.

Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "informazioni riservate", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'Azienda è chiamata a garantire la riservatezza, o per NDA, o per una più ampia tutela del patrimonio aziendale.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine "dati" deve intendersi l'insieme più ampio di informazioni di cui un incaricato (dipendente, collaboratore, tirocinante, ...) può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.

Inoltre, nell'ambito della sua attività, l'Azienda tratta "dati cartacei" ovvero informazioni su supporto cartaceo e "dati digitali" ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'Azienda stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita dell'Azienda.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete internet dal computer aziendale espone l'Azienda a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l'Azienda ha adottato il presente Disciplinare diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

Il presente Disciplinare si applica agli Incaricati che si trovino ad operare con dati dell'Azienda.

Una gestione dei dati cartacei, un uso dei Device aziendali o personali nonché dei servizi di internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l'Azienda ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.

Le informazioni contenute nel presente Disciplinare vengono rilasciate anche ai sensi dell'art. 13 del GDPR e costituiscono, quindi, parte integrante dell'informativa rilasciata agli Incaricati.

## 1.3. Classificazione delle informazioni

Di seguito vengono classificate le informazioni detenute, secondo il seguente schema:

### 1.3.1. Informazioni pubbliche (open)

| | |
|---|---|
| Tipo: | Informazioni che possono essere distribuite a chiunque senza causare danno all'organizzazione, ai dipendenti o agli stakeholders. La Direzione deve approvare l'attribuzione di questa classificazione su un insieme di informazioni. I documenti in questa categoria possono essere comunicati al pubblico o a persone esterne all'organizzazione. |
| Esempio: | Materiale del Marketing predisposto per la comunicazione al pubblico o per spot, brochures, rendicontazioni annuali, internet, annunci di lavoro, etc. |
| Etichettatura: | nessuna o "pubblico" |
| Responsabilità utilizzatore: | nessuna |
| Duplicazione: | senza vincoli |
| Distribuzione: | senza vincoli |
| Distruzione e riciclaggio: | senza vincoli |

### 1.3.2. Informazioni con accesso ristretto

| | |
|---|---|
| Tipo: | Informazioni che possono essere divulgate ad un gruppo ristretto di soggetti esterni all'azienda. |

| | |
|---|---|
| Esempio: | Documentazione di progetto archiviata e resa disponibile a ristretti gruppi di soggetti esterni o a utenti autorizzati. |
| Etichettatura: | "AZIENDALE" |
| Responsabilità utilizzatore: | Autore: responsabile di verificare che la distribuzione delle informazioni confidenziali sia limitata ai casi di effettiva necessità. |
| Duplicazione: | senza vincoli |
| Distribuzione: | Distribuzione tramite sistemi di controllo di accesso e tracciatura delle attività. |
| Distruzione e riciclaggio: | Cancellazione dal sistema o rimozione della condivisione esterna da parte degli utenti autorizzati. |

### 1.3.3. Informazioni confidenziali

| | |
|---|---|
| Tipo: | Informazioni aziendali, confidenziali o di valore, sia personali che sotto brevetto. Non devono assolutamente essere divulgate all'esterno dell'organizzazione senza l'esplicito permesso della Direzione. |
| Esempio: | Password, codici PIN, certificati di firma digitale, informazioni personali, dati relativi alla contabilità aziendale, altre informazioni altamente confidenziali o di valore. |
| Etichettatura: | "CONFIDENZIALE" |
| Responsabilità utilizzatore: | Autore: responsabile di verificare che la distribuzione delle informazioni confidenziali sia limitata ai casi di effettiva necessità.<br>Utilizzatore: assicurarsi che le informazioni confidenziali siano conservate con tecniche di cifratura o tenute sottochiave. |
| Duplicazione: | L'autore o i suoi delegati possono creare un numero limitato di copie. |
| Distribuzione: | Interna: utilizzare buste sigillate o la consegna a mano.<br>Esterna: tramite busta sigillata anonima consegnata a mano, tramite email registrate/PEC, corrieri di fiducia, etc.<br>Per via elettronica: utilizzando Cifratura. |
| Distruzione e riciclaggio: | Documento cartaceo: fatto a pezzi con tritadocumenti predisposto.<br>Dati elettronici: cancellazione dal sistema o cancellazione tramite smagnetizzazione (degaussing). Inviare CD, DVD, Hard Disk, Portatili etc. al reparto IT per lo smaltimento. |

## 1.4. Esclusione all'uso degli strumenti informatici

All'inizio del rapporto lavorativo o di consulenza, l'Azienda valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari device aziendali, di internet e della posta elettronica da parte degli incaricati.

Successivamente e periodicamente l'Azienda valuta la permanenza dei presupposti per l'utilizzo dei device aziendali, di internet e della posta elettronica da parte degli incaricati.

È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali.

I casi di esclusione possono riguardare:

1. l'utilizzo del COMPUTER o di altri dispositivi;
2. l'utilizzo della posta elettronica;
3. l'accesso a internet.

Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici nonché al principio di necessità di cui al GDPR.

Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo gli incaricati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.

I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare sia tutti i casi sopra descritti, sia solo uno o due degli stessi.

Si informa che tali esclusioni sono divenute necessarie alla luce del Provvedimento del Garante 1° marzo 2007 che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce indicate in questo documento.

In qualsiasi momento, senza preavviso, l'Azienda può concedere o ritirare il permesso all'utilizzo degli strumenti informatici aziendali. Pertanto, in alcuno modo, salvo esplicita dichiarazione scritta da parte dell'Azienda che attesta il contrario, l'incaricato può presupporre di poter utilizzare i device assegnati per scopi personali.

## 1.5. Titolarità dei dispositivi e dei dati

L'Azienda è esclusiva titolare e proprietaria dei Device messi a disposizione degli Incaricati ai soli fini dell'attività lavorativa.

L'Azienda è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali.

L'incaricato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'Azienda.

## 1.6. Trasferimento degli Asset

Apparecchiature, informazioni o software, in linea generale, non devono essere portati all'esterno dell'Azienda senza preventiva autorizzazione.

L'Incaricato che ne avesse necessità deve presentare richiesta alla Direzione che provvede ad autorizzare, in modo esplicito, la tipologia di asset ed i limiti di tempo del trasferimento.

## 1.7. Finalità nell'utilizzo dei dispositivi

I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità dell'Incaricato esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.

Qualsiasi eventuale tolleranza da parte di questa Azienda, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

## 1.8. Restituzione dei dispositivi

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con l'Azienda o, comunque, al venir meno, ad insindacabile giudizio dell'Azienda, della permanenza dei presupposti per l'utilizzo dei device aziendali, gli incaricati hanno i seguenti obblighi:

1. procedere immediatamente alla restituzione dei dispositivi in uso nello stato in cui si trova;
2. divieto assoluto di cancellare o formattare o alterare o manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo, compresa la cifratura dei dati.

## 1.9. Restituzione dei dati cartacei

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con l'Azienda o, comunque, al venir meno, ad insindacabile giudizio dell'Azienda, della permanenza dei presupposti per l'utilizzo di dati cartacei aziendali, gli incaricati hanno i seguenti obblighi:

1. procedere immediatamente alla restituzione dei dati cartacei in loro possesso;
2. divieto assoluto di cancellare o alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.

## 1.10. Trasferimento di dati con supporti digitali

Il trasferimento di dati sia all'interno che all'esterno dell'Azienda attraverso i supporti digitali è generalmente ammesso a patto che siano seguite delle procedure che possano garantire di proteggere le informazioni trasferite da potenziali intercettazioni, copia, modifica errori di instradamento e/o distruzione.

Nell'invio delle e-mail gli utenti devono essere molto attenti nel controllare l'indirizzo del/i destinatario/i prima dell'invio per evitare errori di battitura o errori dovuti all'autocompilazione.

L'invio di comunicazioni deve avvenire solo da device protetti da antivirus onde proteggere le comunicazioni da eventuali malware.

Gli allegati contenenti "dati particolari" ex art. 9 del GDPR o "dati giudiziari" ex art. 10 del GDPR oppure "Informazioni confidenziali" come sopra definite, devono essere oggetto di invio come allegato criptato.

Nel caso di utilizzo di posta elettronica certificata (PEC) vanno seguite le regole stabilite nella sezione specifica del presente Disciplinare.

In caso di trasferte fuori dall'ufficio, utilizzando i device in ambito pubblico, è necessario prestare la massima attenzione che non vi siano terzi non autorizzati che possano accedere ai dati.

# 2. SEZIONE II – PASSWORD

## 2.1. Le Password

Le password possono essere un metodo di autenticazione assegnato dall'Azienda per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.

La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'Azienda nel suo complesso.

Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza.

L'Azienda ha implementato alcuni meccanismi che permettono di aiutare e supportare gli Incaricati in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso al Dominio (ove previsto), è in funzione un sistema automatico di richiesta di aggiornamento delle stesse impostato dall'Azienda secondo il livello di sicurezza richiesto dall'Azienda stesso e, comunque, in linea con quanto richiesto dalla valutazione dei rischi effettuata dall'azienda in base alle richieste del GDPR.

Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria.

Le password che non vengono utilizzate da parte degli incaricati per un periodo superiore ai sei mesi verranno disattivate dall'Azienda.

In qualsiasi momento l'Azienda si riserva il diritto di revocare all'Incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

## 2.2. Regole per la corretta gestione delle password

L'Incaricato, da parte sua, per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:

1. Le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. Occorre cambiare immediatamente una password non appena si abbia alcun dubbio che sia diventata poco "sicura";
3. Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali[1] e numeri;
4. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
5. Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password.
6. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Azienda.

[1] Per caratteri speciali si intendono, per esempio, i seguenti: { } [ ] , . < > ; : ! " £ $ % & / ( ) = ? ^ \ | ' * - + _.

In alcuni casi, sono implementati meccanismi che consentono all'Incaricato fino ad un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti. In caso di necessità contattare il Titolare.

## 2.3. Divieto di uso

Al fine di una corretta gestione delle password, l'Azienda stabilisce il divieto di utilizzare come propria password:

1. Nome, cognome e loro parti;
2. Lo username assegnato;
3. Un indirizzo di posta elettronica (e-mail);
4. Parole comuni (in inglese e in italiano);
5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. Parole banali e/o di facile intuizione, ad es. pippo, security e palindromi (simmetria: radar);
7. Ripetizioni di sequenze di caratteri (es. abcabcabc);
8. Una password già impiegata in precedenza.

### 2.3.1. Alcuni esempi di password non ammesse

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare. Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es.: "NlMzz5DlCmm!", Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo). Decifrare una parola come questa può richiedere giorni, una come "radar" meno di dieci secondi. Alcuni esempi di password assolutamente da evitare:

1. Se Username = "mariorossi", password = "mario", o ancora peggio, password = "mariorossi";
2. Il nome della moglie/marito, fidanzato/a, figli, ecc..anche a rovescio!;
3. La propria data di nascita, quella del coniuge, ecc.;
4. Targa della propria auto;
5. Numero di telefono proprio, del coniuge, ecc.;
6. Parole comuni tipo "Kilimangiaro", “Password”, “Qwerty”, “12345678” (troppo facili);
7. Qualsiasi parola del vocabolario (di qualsiasi lingua diffusa, come inglese, italiano, ecc.).

## 2.4. La password nei sistemi

Ogni Incaricato può variare la propria password di accesso a qualsiasi sistema aziendale in modo autonomo, qualora il sistema in questione metta a disposizione degli Utenti una funzionalità di questo tipo (Change password), oppure facendone richiesta al Titolare. La password può essere sostituita dal Titolare, anche qualora l'Utente l'abbia dimenticata.

## 2.5. Chiavi crittografiche

Eventuali chiavi crittografiche nelle disponibilità dell'azienda devono essere in possesso solo della Direzione, che potrà, di volta in volta, delegare le stesse a personale espressamente autorizzato.

## 2.6. Audit delle password

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica, l'Azienda potrebbe effettuare analisi periodiche sulle password degli Incaricati al fine di verificarne la solidità, le policy di gestione e la durata, informandone preventivamente gli Incaricati stessi.

Nel caso in cui l'audit abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e all'Incaricato richiesto di cambiarla. Tale risultanza potrebbe dar luogo a provvedimenti disciplinari secondo quanto previsto dal CCNL adottato dall'Azienda.

# 3. SEZIONE III – OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO.

In questa sezione vengono trattate le operazioni a carico dell'Incaricato e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.

## 3.1. Login e Logout

Il "Login" è l'operazione con la quale l'Incaricato si connette al sistema informatico aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede un username e una password.

In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico user name e password, l'Azienda potrà assegnare un univoco user name e password per gruppi di incaricati per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

## 3.2. Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.

L'incaricato deve quindi eseguire le operazioni seguenti:

1. Se si allontana dalla propria postazione dovrà mettere in protezione il suo device affinché persone non autorizzate non abbiano accesso ai dati protetti.
2. Bloccare il suo dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
3. Chiudere la sessione (Logout) a fine giornata;
4. Spegnere il PC dopo il Logout;
5. Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo device.

# 4. SEZIONE IV – USO DEL PERSONAL COMPUTER DELL'AZIENDA

## 4.1. Modalità d'uso del COMPUTER aziendale

Il sistema informativo aziendale è composto da un insieme di unità server centrali e macchine client connessi ad una rete locale (LAN), che utilizzano diversi sistemi operativi e applicativi.

I files creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati a fine giornata sul sistema di repository documentale centralizzato. L'Azienda non effettua il backup dei dati memorizzati in locale.

Gli operatori del Reparto Sistemi Informativi possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la Sicurezza sia sui PC degli utenti che sulle unità di rete.

## 4.2. Corretto utilizzo del COMPUTER aziendale

Il computer consegnato all'incaricato è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dall'Azienda. Per necessità aziendali, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alla memoria di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche da remoto.

In particolare, l'Incaricato deve adottare le seguenti misure:

1. Utilizzare solo ed esclusivamente le aree di memoria della rete dell'Azienda ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di rete.
2. Spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché 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. Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dall'Azienda.
4. Non dare accesso al proprio computer ad altri utenti, a meno che siano incaricati con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

## 4.3. Divieti Espressi sull'utilizzo del COMPUTER

All'incaricato è vietato:

1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell'incaricato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere.
2. Modificare le configurazioni già impostate sul personal computer.
3. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell'Azienda.
4. Installare alcun software di cui l'Azienda non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer

consegnato, senza l'espressa autorizzazione dell'Azienda. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.

5. Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate. In particolare non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'Azienda.
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'Azienda, quali per esempio virus, trojan horses ecc.
8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.
9. Effettuare in proprio attività manutentive.
10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'Azienda.
11. Attivare la password d'accensione del BIOS.
12. Riprodurre o duplicare programmi informatici ai sensi delle Legge n.128 del 21.05.2004 ("...recante interventi per contrastare la diffusione telematica abusiva di materiale audiovisivo, nonché a sostegno delle attività cinematografiche e dello spettacolo"), vedi anche Legge n. 633 del 22.04.1941 ("Legge sul diritto d'autore").

## 4.4. Uso di programmi di utilità privilegiati

L'uso di programma di utilità che potrebbero essere in grado di aggirare i controlli applicativi e di sistema sono, in generale, vietati.

Tali programmi possono essere utilizzati solo se sussistono le seguenti condizioni:

1) I programmi in questione sono stati autorizzati esplicitamente dalla Direzione;
2) Gli incaricati ad utilizzare tali programmi sono stati oggetto di esplicita autorizzazione da parte della Direzione;
3) Ogni volta che i programmi devono essere utilizzati è necessario che l'incaricato autorizzato richieda alla direzione l'autorizzazione allo specifico utilizzo;
4) Ogni utilizzo di tali programmi deve essere tracciato;
5) I programmi di utilità devono essere disinstallati una volta terminato l'utilizzo.

## 4.5. Antivirus

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail ...

L'Azienda impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.

L'incaricato, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:

1) Comunicare all'Azienda ogni anomalia o malfunzionamento del sistema antivirus.
2) Comunicare all'Azienda eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all'incaricato:

3) È vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione.
4) È vietato ostacolare l'azione dell'antivirus aziendale.
5) È vietato disattivare l'antivirus senza l'autorizzazione espressa dell'Azienda e anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer.
6) È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani.

Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

# 5. SEZIONE V – INTERNET

## 5.1. Internet è uno strumento di lavoro

La connessione alla rete internet dal device avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.

In particolare, si vieta l'utilizzo dei social network, se non espressamente autorizzati.

## 5.2. Misure preventive per ridurre navigazioni illecite

L'Azienda potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list implementati ad esempio attraverso i sistemi di content filter dei firewall.

## 5.3. Divieti Espressi concernenti Internet

1. È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'Incaricato poiché potenzialmente idonea a rivelare dati personali ai sensi del GDPR.
2. È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. È vietato all'Incaricato il downoload di software (anche gratuito) prelevato da siti Internet.
4. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto.
5. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
6. È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'Azienda, salvo specifica autorizzazione dell'Azienda stessa.
7. È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
8. È vietato all'Incaricato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.
9. È vietato accedere dall'esterno alla rete interna dell'Azienda, salvo specifica autorizzazione e con le specifiche procedure previste dall'Azienda stessa.
10. È vietato, infine, creare siti web personali sui sistemi dell'Azienda nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.
11. È vietato utilizzare internet per attività di file sharing.

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili è posta sotto la personale responsabilità dell'Incaricato inadempiente e può dar luogo a provvedimenti disciplinari secondo quanto previsto dal CCNL adottato dall'Azienda.

## 5.4. Divieti di Sabotaggio

È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'Azienda per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

## 5.5. Diritto d'autore

È vietato utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248 e s.m.i.). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, ...) se non espressamente autorizzato dall'Azienda.

# 6. SEZIONE VI – POSTA ELETTRONICA

## 6.1. La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente.

Gli Incaricati possono avere in utilizzo caselle di posta elettronica appartenenti ai domini aziendali. Gli assegnatari dei singoli account sono responsabili del corretto utilizzo delle stesse.

Le caselle e-mail possono essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, consulenza, ...) per evitare che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito.

Possono altresì essere assegnati indirizzi nominativi che dovranno comunque essere considerati a pieno titolo indirizzi dedicati all'attività lavorativa.

La scelta dell'account mail da assegnare all'incaricato resta in capo all'Azienda.

## 6.2. Archiviazione posta elettronica

La posta elettronica, sia nominale che generica, serve esclusivamente ad inviare e ricevere messaggi; pertanto, non può essere considerata e/o utilizzata come uno spazio virtuale per l'archiviazione di informazioni e documenti rilevanti per l'azienda.

Tutti gli allegati condivisi tramite posta elettronica, così come tutte le informazioni rilevanti per l'azienda (es. informazioni e documenti su clienti, dipendenti, collaboratori, progetti interni, etc.) andranno debitamente archiviati nelle apposite cartelle del sistema di archiviazione in utilizzo.

L'azienda si riserva di monitorare la dimensione delle caselle mail dei lavoratori onde valutare l'inosservanza della presente regola.

## 6.3. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

L'Azienda è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli Incaricati e allo scopo prevede le seguenti misure:

1. In caso di ricezione sulla e-mail aziendale di posta personale si avverte che l'Incaricato deve cancellare immediatamente ogni messaggio personale al fine di evitare ogni eventuale e possibile back up dei dati. Tutti i contenuti non cancellati possono essere soggetti a back up.
2. Avvisare l'Azienda quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

## 6.4. Divieti Espressi

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'Azienda per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'Azienda, nonché utilizzare il dominio dell'Azienda per scopi personali.

2. È vietato redigere messaggi di posta elettronica utilizzando l'indirizzo aziendale, diretti a destinatari esterni dell'Azienda, senza utilizzare il seguente disclaimer nel pedice della mail:

   *Il presente messaggio e gli eventuali suoi allegati sono di natura aziendale, prevalentemente confidenziale e sono visionabili solo dal destinatario di posta elettronica. La risposta o l'eventuale invio spontaneo da parte vostra di e-mail al nostro indirizzo potrebbero non assicurare la confidenzialità potendo essere viste da altri soggetti appartenenti all'Azienda oltre che al firmatario della presente, per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento dell'attività aziendale. Qualora questo messaggio vi fosse pervenuto per errore, vi preghiamo di cancellarlo dal vostro sistema e vi chiediamo di volercene dare cortesemente comunicazione al mittente.*
   *La Vs. mail è in ns. possesso in quanto da Voi fornitaci tramite comunicazione scritta, telefonica, telematica o direttamente oralmente. Essa è utilizzata esclusivamente per fornirVi informazioni sulla ns. attività e sui servizi da noi offerti. Non sarà ceduta a terzi in nessun caso salvo approvazione da parte Vostra. Il Titolare del trattamento è l'Azienda.*
   *I ns. sistemi informativi e le ns. procedure interne sono conformi alle norme e garantiamo la presenza di adeguate misure tecniche ed organizzative costantemente aggiornate.*
   *È possibile in qualsiasi momento richiedere la cancellazione della Vs. mail tramite la semplice risposta alla presente mail con titolo unsubscribe*
3. È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.
4. È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria.
5. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
6. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'Azienda informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.
7. È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni.
8. È vietato l'inoltro di mail, documenti o qualsiasi tipo di informazione aziendale alla propria casella di posta personale
9. Nel caso di mittenti sconosciuti o messaggi inusuali, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.
10. Nel caso di messaggi provenienti da mittenti noti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti ma cancellati.

## 6.5. Posta Elettronica in caso di assenze programmate ed assenze non programmate

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (Auto-reply).

In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, l'Incaricato deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i files necessari a chi ne abbia urgenza.

Qualora l'Incaricato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, l'Azienda, mediante personale appositamente incaricato, potrà verificare il contenuto dei messaggi di posta elettronica dell'incaricato, informandone l'incaricato stesso e redigendo apposito verbale.

## 6.6. Cessazione del rapporto lavorativo

L'Azienda può attivare account di mail relativi sia su caselle di tipo generico (info@, amministrazione@, ufficio@ etc...) sia su caselle di tipo nominale (n.cognome@, nome.cognome@, cognome@, nome@ etc...).

In caso di cessazione del rapporto di lavoro tra l'Azienda e l'incaricato è vietato a quest'ultimo di cancellare i messaggi di mail inviati e/o ricevuti tramite l'account assegnatogli, essendo quei messaggi un patrimonio aziendale.

In caso di cessazione del rapporto di lavoro tra l'Azienda e l'incaricato, il Titolare del trattamento provvede, entro massimo 3 mesi da tale data, alla rimozione dell'account di casella di posta nominale, previa disattivazione dello stesso e contestualmente all'adozione di sistemi automatici volti ad informarne i terzi e a fornire a questi ultimi indirizzi e-mail alternativi, riferiti all'attività professionale del titolare del trattamento, provvedendo altresì ad adottare misure idonee ad impedire la visualizzazione dei messaggi in arrivo durante il periodo in cui tale sistema automatico è in funzione.

## 6.7. Utilizzo Illecito di Posta Elettronica

1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
2. È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. Qualora l'Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'Azienda.

## 6.8. Utilizzo della Posta elettronica Certificata

La Posta Elettronica certificata (PEC) è uno strumento o servizio informatico italiano che permette di dare ad un messaggio di posta elettronica lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale, garantendo così il non ripudio, con il vantaggio che la ricevuta di consegna contiene anche il messaggio, gli allegati e le identità del mittente e del destinatario di PEC, anch'essi certificati.

Ogni PEC è registrata e collegata al nominativo di una persona fisica.

La PEC viene utilizzata principalmente per le comunicazioni istituzionali, in particolare per le comunicazioni con gli enti pubblici o in sostituzione della raccomandata anche tra privati.

Le credenziali di accesso alla PEC devono essere nella stretta disponibilità della persona fisica a cui la PEC si riferisce. La stessa può delegare, con atto formale, altri incaricati all'utilizzo della PEC sia in visione che in trasmissione.

# 7. SEZIONE VII – USO DI ALTRI DISPOSITIVI (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

## 7.1. L'utilizzo del notebook, tablet o smartphone.

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "device mobile") possono venire concessi in uso dall'Azienda agli Incaricati che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'Azienda.

L'Incaricato è responsabile dei dispositivi mobili assegnatigli dall'Azienda e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare, i files creati o modificati sui dispositivi mobili devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio e cancellati in modo definitivo dai dispositivi mobili (Wiping). Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'Azienda. I dispositivi mobili utilizzati all'esterno (convegni, visite in azienda, ecc....), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei dispositivi mobili deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l'Azienda che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. Anche di giorno, durante l'orario di lavoro, all'Incaricato non è consentito lasciare incustoditi i dispositivi mobili.

All'Incaricato è vietato lasciare i dispositivi mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

I dispositivi mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciati privi di PIN.

Laddove il dispositivo mobile sia accompagnato da un'utenza, l'Incaricato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, ...) e a rispettarli. Qualora esigenze lavorative richiedessero *requirements* differenti l'Incaricato è tenuto ad informare tempestivamente e preventivamente l'Azienda.

In relazione alle utenze mobili, salvo autorizzazione dell'Azienda, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'Azienda, gli utilizzi all'estero devono essere preventivamente comunicati all'Azienda per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

Alcuni Device mobili, quali smartphone e tablet, possono essere dotati dall'azienda di particolari misure di protezione (MDM o altro).

## 7.2. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ...)

Agli Incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, ...) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, ...).

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

## 7.3. Device personali e BYOD

Ai dipendenti non è permesso svolgere la loro attività con PC fissi, portatili o altri dispositivi personali.

Ai dipendenti, se espressamente autorizzati dall'Azienda, è permesso solo l'utilizzo della posta elettronica aziendale sui loro dispositivi personali.

In tal caso è necessario che il dispositivo abbia password di sicurezza stringenti approvate dall'Azienda e l'eventuale furto o smarrimento del device deve essere immediatamente segnalato anche all'Azienda per eventuali provvedimenti di sicurezza.

Al collaboratore è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, ...).

Alcuni incaricati possono utilizzare i propri dispositivi personali per memorizzare dati dell'Azienda (Bring Your Own Device – BYOD) solo se espressamente autorizzati dall'Azienda stessa e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali dispositivi dovranno essere preventivamente valutati dall'Azienda, per la verifica della sussistenza di adeguate misure di sicurezza.

## 7.4. Utilizzo del cellulare/smartphone personale.

Durante l'orario di lavoro, comprese le eventuali pause, agli Incaricati è concesso l'utilizzo del telefono cellulare personale ma solo per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo.

In caso di trasferte lavorative all'esterno degli uffici dell'Azienda, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con l'Azienda stessa ove fosse necessario.

In questo caso si invita, comunque, a non utilizzarlo per fini personali, in modo particolare alla presenza di clienti o fornitori.

## 7.5. Utilizzo delle stampanti

L'incaricato deve effettuare la stampa dei dati solo se necessaria all'attività lavorativa e deve ritirarla prontamente dai vassoi delle stampanti personali/comuni per evitare che sia visibile o possa essere raccolta da terzi. Al momento del ritiro dei fogli stampati, l'utente deve porre attenzione a prelevare solo le proprie pagine.

L'incaricato, qualora disponga di più dispositivi di stampa, deve utilizzare quello che garantisce un maggior controllo del documento stampato.

## 7.6. Distruzione dei Device

Ogni device ed ogni memoria esterna affidati agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'Azienda che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.

In particolare, l'Azienda provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

Possono essere utilizzate le seguenti procedure:

- Distruzione fisica del supporto
- Cancellazione Logica (Wiping)
- Smagnetizzazione (Degauss)

# 8. SEZIONE VIII – SISTEMI IN CLOUD

## 8.1. Cloud Computing

In informatica con il termine inglese cloud computing (in italiano nuvola informatica) si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.

Le risorse non vengono pienamente configurate e messe in opera dal fornitore apposta per l'utente, ma gli sono assegnate, rapidamente e convenientemente, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciando all'utente parte dell'onere della configurazione. Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel pool condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.

Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone l'Azienda a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nelle server farms di aziende che spesso risiedono in uno stato extraeuropeo, configurando un trasferimento dei dati all'estero. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti.

Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'Azienda, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso dal paese dell'utente.

Nel caso di industrie o aziende, tutti i dati memorizzati nelle memorie esterne sono seriamente esposti a eventuali casi di spionaggio industriale.

## 8.2. Utilizzo di sistemi cloud

È vietato agli incaricati l'utilizzo di sistemi Cloud non espressamente approvati dall'Azienda. Per essere approvati i sistemi cloud devono rispondere ad almeno i seguenti requisiti:

- Essere sistemi cloud di cui si conosce l'esatto posizionamento dei server e per i quali si è predisposto quanto richiesto dalle norme, compreso eventualmente quello che è richiesto per il trasferimento dei dati all'estero.
- L'azienda che fornisce il sistema in Cloud deve essere preventivamente nominata Responsabile al Trattamento dei dati da parte dell'Azienda.
- L'azienda che fornisce il sistema in Cloud deve comunicare all'Azienda, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati.
- Dovranno essere verificate tutte le indicazioni e le prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul Cloud.

# 9. SEZIONE IX – LAVORO DA REMOTO

## 9.1. Smart Working, Telelavoro, lavoro in trasferta

Per determinate situazioni di emergenza o per accordi con i lavoratori, questa Azienda può permettere ad alcuni lavoratori di svolgere la loro attività da remoto, dalla propria abitazione o mentre si trova in trasferta.

In tali situazioni, l'Incaricato dovrà verificare:

1) Di disporre di una connessione internet sicura, attraverso una verifica delle wi-fi casalinga o optando per una connessione mobile protetta.
2) Svolgere la propria attività verificando che non sia possibile per terzi, anche famigliari, accedere o anche solo visionare quanto si stia facendo.
3) Verificare con cura la sicurezza della rete elettrica a cui ci si collega.

# 10. SEZIONE X – GESTIONE DATI CARTACEI

## 10.1. Clear Desk Policy

Gli Incaricati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Gli Incaricati sono invitati dall'Azienda a adottare una "politica della scrivania pulita". Ovvero si richiede agli incaricati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dall'Azienda.

I principali benefici di una politica della scrivania pulita sono:

1) Una buona impressione a clienti e fornitori che visitano la nostra Azienda;
2) La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
3) La riduzione che documenti confidenziali possano essere sottratti all'Azienda.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassettiera, archivio, ...) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell'Azienda.

A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.

Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.

Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.

E' necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

# 11. SEZIONE XI -APPLICAZIONE E CONTROLLO

## 11.1. Il controllo

L'Azienda, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
2. Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
3. Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e *vulnerability assessment* del sistema informatico. Per tali controlli l'Azienda si riserva di avvalersi di soggetti esterni.
Si precisa, in ogni caso, che l'Azienda non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

## 11.2. Modalità di verifica

In applicazione del GDPR, l'Azienda promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli Incaricati e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.

L'Azienda informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare, eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Incaricati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche. Al contrario possono esserci verifiche programmate ai sensi del principio di Accountability ex art. 5.2 del GDPR.

Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. download di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

## 11.3. Modalità di Conservazione

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

1. ad esigenze tecniche o di sicurezza del tutto particolari;
2. all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;

3. all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di Azienda strettamente correlate agli obblighi, compiti e finalità già esplicitati.

# 12. SEZIONE XII – SOGGETTI PREPOSTI DEL TRATTAMENTO, INCARICATI E RESPONSABILI

## 12.1. Individuazione dei Soggetti autorizzati

L'Azienda ha individuato specifiche figure cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità.

Per quanto riguarda i soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) sono stati appositamente incaricati di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità di sicurezza informatica, senza realizzare attività di controllo a distanza, neanche di propria iniziativa.

I soggetti che operano quali amministratori di sistema o le figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, svolgono un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

# 13. SEZIONE XIII – PROVVEDIMENTI DISCIPLINARI

## 13.1. Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente Disciplinare potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato, tra cui:

1. il biasimo inflitto verbalmente;
2. lettera di richiamo inflitto per iscritto;
3. multa;
4. la sospensione dalla retribuzione e dal servizio;
5. il licenziamento disciplinare e con le altre conseguenze di ragioni e di legge;

Per i dirigenti valgono le vigenti norme di legge e/o di contrattazione collettiva, fermo restando che, per le violazioni di maggior gravità l'Azienda potrà procedere al licenziamento del dirigente autore dell'infrazione.

# 14.SEZIONE XIV – VALIDITA', AGGIORNAMENTO ED AFFISSIONE

## 14.1. Validità

Il presente Disciplinare ha validità a partire dalla data di sottoscrizione da parte del Titolare sotto riportata.

## 14.2. Aggiornamento

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'Azienda o in caso di mutazioni legislative.

Ogni variazione del presente Disciplinare sarà comunicata agli incaricati.

## 14.3. Affissione

Il presente Disciplinare verrà affisso nella bacheca aziendale e/o pubblicato sulla intranet aziendale per la maggior diffusione ed ai sensi del CCNL.

# Allegato 4 al CODICE ETICO E DI COMPORTAMENTO

# - PROCEDURA WHISTLEBLOWING -

## INDICE

## Scopo

Il Legislatore italiano ha pubblicato in Gazzetta Ufficiale, in data 15 marzo 2023, il D.Lgs. 10 marzo 2023, n. 24, provvedendo in questo modo a dare attuazione alla Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019, riguardante la "Protezione delle persone che segnalano violazioni di normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto pubblico o privato".

More Than Access S.r.l. Società Benefit (di seguito "Società") condivide, con i propri dipendenti e collaboratori e con tutti i soggetti con i quali la Società opera, che lavorare in accordo alle regole interne, quali il Codice Etico e di Comportamento, le procedure ed il Modello 231, ed alla normativa applicabile (leggi nazionali ed europee) è un dovere di tutte le parti.

In coerenza alle disposizioni del D.Lgs. 24/2023, obiettivo della presente procedura è pertanto quello di definire ed istituire chiari ed identificati canali informativi idonei a garantire la ricezione, l'analisi e la gestione di segnalazioni – anonime e riservate – relative a ipotesi di condotte illecite rilevanti nei seguenti settori/ambiti:

- violazioni del Modello 231 e Codice Etico adottato dalla Società;
- condotte illecite rilevanti ai sensi del D.Lgs. 231/2001;
- illeciti amministrativi, contabili, civili o penali.

Inoltre, la presente procedura è tesa a:

- garantire la riservatezza dei dati personali del Segnalante e del presunto responsabile della violazione (Segnalato), ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione, o comunque i procedimenti disciplinari in caso di segnalazioni effettuate in male fede;
- tutelare adeguatamente il Segnalante contro condotte ritorsive e/o, discriminatorie dirette o indirette per motivi collegati "direttamente o indirettamente" alla Segnalazione;
- assicurare per la Segnalazione un canale specifico, indipendente e autonomo.

## Definizioni e abbreviazioni

- ***"Gestore della segnalazione":*** persona o ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, ovvero è affidata a un soggetto esterno, anch'esso autonomo e con personale specificamente formato.
- ***"Modello 231"***: Modello di Organizzazione, Gestione e Controllo adottato da More Than Access Società Benefit e che definisce un sistema strutturato ed organico di principi, norme interne, procedure operative e attività di controllo, con lo scopo di prevenire comportamenti idonei a configurare fattispecie di reato e illeciti previsti dal D.Lgs. 231/2001.
- ***"Segnalante"***: Persona fisica che effettua la segnalazione interna od esterna o la Divulgazione pubblica di informazioni su violazioni acquisite nell'ambito del proprio contesto lavorativo.
- ***"Segnalato"***: Persona menzionata nella segnalazione interna o esterna, ovvero nella Divulgazione pubblica, intesa come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente.
- ***"Segnalazione"***: Comunicazione scritta od orale di informazioni su violazioni, compresi i fondati sospetti riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse in

More Than Access S.r.l. Società Benefit, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni.

- ***"Violazioni"***: Comportamenti, atti od omissioni che violano la disciplina 231 e/o il Modello 231 adottato alla Società, di cui i soggetti Segnalanti siano venuti a conoscenza in un contesto lavorativo pubblico o privato.

## Campo di applicazione

La nuova disciplina prevista dal D.Lgs. 24/20223 si applica alle Violazioni rilevanti per la disciplina 231 o violazioni del Modello 231.

Sotto il **profilo oggettivo**, le segnalazioni possono avere ad oggetto:

I. condotte illecite rilevanti ai sensi del D.Lgs. 231/2001 e violazioni del Modello 231 e del Codice Etico e di Comportamento adottato dalla Società;
II. illeciti amministrativi, contabili, civili o penali.

Sono escluse le contestazioni:

I. legate a un interesse personale del Segnalante, che attengono ai rapporti individuali di lavoro;
II. in materia di sicurezza e difesa nazionale;
III. relative a violazioni già disciplinate in via obbligatoria in alcuni settori speciali (servizi finanziari, prevenzione riciclaggio, terrorismo, sicurezza nei trasporti, tutela dell'ambiente, concorrenza e aiuti di Stato).

Le segnalazioni possono riguardare, a titolo esemplificativo e non esaustivo:

- violazioni relative alla tutela dei lavoratori, ivi inclusa la normativa antinfortunistica;
- presunti illeciti, tra quelli previsti dal Modello 231 della Società, da parte di esponenti aziendali nell'interesse o a vantaggio della Società;
- violazioni del Codice Etico e di Comportamento, del Modello 231, delle procedure aziendali;
- comportamenti illeciti nell'ambito dei rapporti con esponenti delle pubbliche amministrazioni;
- violazioni in materia di tutela della vita privata e violazione dei dati personali.

Le segnalazioni prese in considerazione sono soltanto quelle che riguardano fatti riscontrati direttamente dal Segnalante, non basati su voci correnti. Sono inoltre escluse dall'ambito di applicazione del sistema di whistleblowing le Segnalazioni aventi ad oggetto lamentele e reclami di carattere personale dei Segnalanti o richieste che attengono al rapporto di lavoro o ai rapporti con i colleghi e superiori gerarchici. Segnalazioni di carattere personale o attinenti il rapporto di lavoro potranno essere condivise e gestite con i propri superiori. Il Segnalante non deve utilizzare del whistleblowing l'istituto per scopi meramente personali, per rivendicazioni o ritorsioni, che, semmai, rientrano nella più generale disciplina del rapporto di lavoro/collaborazione o dei rapporti con il superiore gerarchico o con i colleghi.

Sotto il **profilo soggettivo**, la presente procedura si applica ai Destinatari del Modello 231 e/o del Codice Etico e di Comportamento della Società ossia a tutto il personale dipendente della Società che svolga le attività individuate "a rischio" di commissione di un reato presupposto nonché ai collaboratori esterni, intesi sia come persone fisiche, sia come persone giuridiche che collaborino con la Società per la realizzazione delle proprie attività.

## Contenuto della segnalazione

Il Segnalante è tenuto a fornire tutti gli elementi disponibili e utili a consentire ai soggetti competenti di procedere alle dovute ed appropriate verifiche ed accertamenti a riscontro della fondatezza dei fatti oggetto di Segnalazione, quali:

- una chiara e completa descrizione dei fatti oggetto della Segnalazione;
- le circostanze di tempo e di luogo in cui sono stati commessi i fatti oggetto della Segnalazione;
- le generalità o altri elementi che consentano di identificare il/i soggetto/i che ha/hanno posto in essere i fatti segnalati (ad es. qualifica, sede di servizio in cui svolge l'attività);
- gli eventuali documenti a supporto della Segnalazione;
- l'indicazione di eventuali altri soggetti che possano riferire sui fatti oggetto di Segnalazione;
- ogni altra informazione che possa fornire utile riscontro circa la sussistenza dei fatti segnalati.

## Canali di segnalazione interna e gestione delle segnalazioni

La Società ha attivato propri canali di segnalazione che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona Segnalante, della persona coinvolta e della persona comunque menzionata nella Segnalazione, nonché del contenuto della Segnalazione e della relativa documentazione.

Le Segnalazioni possono essere effettuate attraverso i seguenti Canali di Segnalazione interna. In particolare, qualora un soggetto Segnalante abbia il ragionevole sospetto che si sia verificato o che possa verificarsi una delle violazioni indicate al precedente paragrafo 2, ha la possibilità di effettuare una Segnalazione nelle seguenti modalità.

### I. In forma scritta

Il Segnalante può accedere al canale di comunicazione implementato da More Than Access S.r.l. Società Benefit e raggiungibile all'indirizzo internet *https://morethanaccess.trusty.report/* ed effettuare la Segnalazione seguendo le istruzioni ivi riportate.

### II. In forma orale

Il Segnalante ha la possibilità di segnalare una violazione richiedendo un incontro in presenza al Gestore della segnalazione incaricato dalla Società e segnatamente a Muriel Bertomoro.

I Canali di Segnalazione Interna garantiscono la riservatezza dell'identità del Segnalante, del soggetto segnalato e delle persone coinvolte o menzionate nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione, in conformità al Decreto Whistleblowing, al Codice Privacy, al GDPR e alle altre leggi vigenti in materia di protezione dei dati personali.

L'accesso per la gestione dei Canali di Segnalazione Interna è riservato unicamente alla persona incaricata come Gestore delle Segnalazioni, salvo quanto diversamente previsto dal Decreto Whistleblowing.

Le segnalazioni non possono essere utilizzate dal Gestore delle Segnalazioni e dagli altri soggetti eventualmente coinvolti nella gestione oltre quanto necessario per dare adeguato seguito alle stesse.

Ricevuta una Segnalazione, la persona incaricata come Gestore delle Segnalazioni:

- rilascia al Segnalante un avviso di ricevimento della Segnalazione (entro 7 giorni dalla ricezione della Segnalazione);
- valuta la pertinenza all'ambito di applicazione del D.Lgs. 24/2023. La inoltra tempestivamente all'Organismo di Vigilanza della Società qualora abbia ad oggetto segnalazioni relative a condotte illecite rilevanti ai sensi del D. Lgs. 231/2001;
- si accerta che venga dato seguito alla Segnalazione, verificando che siano mantenute le interlocuzioni con il Segnalante e collabora con l'Organismo di Vigilanza per le opportune indagini interne volte a verificare la sussistenza dei fatti segnalati;
- verifica che sia fornito un riscontro al Segnalante nel più breve tempo possibile e, in ogni caso, entro 3 mesi dal ricevimento della Segnalazione; il riscontro consiste nella comunicazione di informazioni relative al seguito dato o che si intende dare alla Segnalazione, inclusa la comunicazione dell'eventuale assenza di presupposti per procedere nell'indagine e relativa archiviazione della Segnalazione;
- archivia e custodisce le segnalazioni (anche anonime) nonché i documenti, per un anno, se archiviate perché ritenute infondate e, negli altri casi, per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza sanciti dal Decreto Whistleblowing, dal Codice Privacy, dal GDPR e/o di altre leggi in materia di protezione dei dati personali applicabili.

Tutte le comunicazioni tra la persona incaricata come Gestore delle Segnalazioni e l'Organismo di Vigilanza (o tra il Gestore delle Segnalazioni e altre funzioni interne e/o consulenti esterni) avvengono con modalità tali da garantire la tutela della riservatezza dell'identità del Segnalante e delle persone coinvolte o menzionate nella segnalazione, in osservanza di quanto previsto dal Decreto Whistleblowing, dal GDPR, dal Codice Privacy e/o da altre disposizioni di legge vigenti e applicabili in materia di protezione dei dati personali.

## Misure di protezione

In caso di segnalazioni di violazioni rilevanti ai sensi del Decreto Whistleblowing trovano applicazione le seguenti misure di protezione:

- tutela della riservatezza del Segnalante e degli altri soggetti protetti, del soggetto Segnalato e delle persone menzionate nella Segnalazione, nonché del contenuto della Segnalazione e della relativa documentazione, in conformità alle leggi vigenti in materia di protezione dei dati personali;
- tutela da eventuali misure ritorsive: la Società vieta ogni ritorsione – anche solo tentata o minacciata – nei confronti dei Segnalanti e degli altri soggetti protetti, posta in essere in ragione della Segnalazione interna, che provochi o possa provocare, in via diretta o indiretta, un danno ingiusto a tali soggetti; i Segnalanti e gli altri soggetti protetti che ritengono di aver subito una ritorsione potranno darne comunicazione ad ANAC tramite il Canale di Segnalazione Esterna come previsto dal Decreto Whistleblowing;
- limitazioni della responsabilità rispetto alla rivelazione e alla diffusione di alcune categorie di informazioni indicate nel Decreto Whistleblowing;
- misure di sostegno fornite a titolo gratuito da parte di enti del "Terzo Settore" iscritti nell'elenco istituito presso l'ANAC.