

**Nomina autorizzato al trattamento dei dati personali**

La società **P.M. Group srl** (partita IVA 01886000403) in qualità di Titolare del trattamento dei dati personali, ai sensi e per gli effetti dell’art. 4 n. 10 del Regolamento Europeo sulla Protezione dei Dati, n.679/2016, attribuisce a

**{Delegate}**

**le specifiche funzioni relative al trattamento dei dati personali** previste nell’ambito delle funzioni che nella qualità di dipendenteè chiamato a svolgere, così come previsto dall’art. 2 – quaterdecies del D.Lgs. 196/2003, aggiornato dal D.Lgs. 101/2018.

A tal fine, Le vengono qui di seguito fornite una serie di informazioni, nonché le specifiche istruzioni per l’assolvimento del compito assegnatoLe con la presente.

**Premessa**

L’attività di trattamento che Ella è autorizzato a svolgere non riguarderà altresì i dati personali particolari meglio noti come “sensibili” (idonei, cioè, a rilevare origine razziale ed etnica, convinzioni religiose, filosofiche, o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale).

Ella dovrà custodire con la massima diligenza i dati personali raccolti, trattati e/o di cui comunque si trovi in possesso e che siano contenuti su supporti cartacei. Tali dati non potranno e non dovranno essere comunicati, o altrimenti condivisi con nessun soggetto che non sia stato espressamente autorizzato a tal fine dalla Società. I dati ed i relativi supporti non potranno e non dovranno essere lasciati incustoditi per nessuna ragione.

Al termine delle operazioni di trattamento e raccolta affidateLe, Ella è tenuto a restituire alla società i dati, unitamente ai relativi supporti.

In ottemperanza al Regolamento 679/16 e al D.Lgs. 196/2003 che regola il trattamento dei dati personali La informiamo che qualsiasi operazione di trattamento deve essere svolta seguendo i seguenti principi:

* Il trattamento dei dati deve essere effettuato in modo lecito e secondo correttezza.
* I dati personali devono essere raccolti e registrati unicamente per finalità inerenti all’attività svolta.
* È necessario verificare costantemente la correttezza dei dati trattati e, ove necessario, gli stessi devono essere aggiornati.
* È necessario verificare altresì costantemente che i dati trattati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare o dal Responsabile.
* Devono essere rispettate le misure di sicurezza predisposte dalla Società.

In ogni operazione di trattamento deve essere garantita la massima riservatezza. In particolare:

* è fatto espresso ed assoluto divieto di comunicazione e/o diffusione dei dati salvo preventiva autorizzazione del Titolare o del Responsabile;
* l’accesso dei dati dovrà essere strettamente limitato all’espletamento delle Sue ordinarie mansioni nell’ambito del Suo Ufficio;
* nella fase della raccolta dei dati dovrà essere osservata la procedura per il rilascio dell’informativa e l’ottenimento del consenso da parte degli interessati.

In caso di allontanamento, anche temporaneo, dalla postazione di lavoro, dovrà essere verificato che non vi sia possibilità da parte di terzi (anche se soggetti appartenenti alla struttura) di accedere ai dati personali per i quali era in corso una qualunque operazione di trattamento, sia essa mediante supporto cartaceo o informatico. Nel caso in cui le operazioni di trattamento si stiano svolgendo a mezzo di un elaboratore elettronico, questo non dovrà essere lasciato incustodito, né altrimenti reso accessibile durante le singole sessioni di trattamento. Al fine di garantire la massima riservatezza nel trattamento informatico dei dati personali, l’accesso è consentito solamente mediante l’utilizzo di una credenziale di autenticazione consistente in un codice identificativo personale univoco (*ID*) e di una parola chiave (*password*).

L’*ID* e la *password* sono riservate, dovendo pertanto rimanere segrete. Ella dovrà adottare tutte le cautele necessarie a tal fine, astenendosi dal comunicare (o comunque dal consentire la conoscenza) la credenziale di autenticazione assegnateLe a chicchessia.

Le ricordiamo, inoltre, che i dati personali da Lei trattati e contenuti su supporti cartacei sono conservati negli archivi dei Suoi uffici situati all’interno dell’azienda. L’accesso a tali dati è consentito solo agli incaricati del trattamento dei medesimi.

Le ricordiamo che tutto quanto sopra vale sia quanto agli originali sia quanto alle eventuali copie cartacee o informatiche.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere da Lei scrupolosamente osservati anche in seguito all’eventuale cessazione dall’incarico con la presente assegnatoLe ovvero dal rapporto di lavoro attualmente in essere con la Società.

I principi sopra elencati dovranno essere in ogni caso integrati dal rispetto delle disposizioni contenute nel manuale di procedure sulla sicurezza, predisposto dalla società e a suo tempo consegnatoLe.

**Specifiche istruzioni in funzione delle mansioni svolte**

Tutto quanto sopra premesso, in considerazione delle mansioni affidateLe, con la presente, Le viene conferito l’incarico di compiere le operazioni di trattamento elencate con l’avvertimento che dovrà agire sotto la diretta autorità del Titolare e rispettando per ogni singola attività i principi di cui in premessa. Tale incarico dovrà essere espletato senza alcun onere aggiuntivo per la Società e senza nessun pregiudizio per eventuali altri analoghi incarichi che Le siano stati già affidati.

{Date} Firma dell’autorizzato per accettazione

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Regolamento interno per un corretto utilizzo dei sistemi informatici aziendali**

La progressiva diffusione di nuove tecnologie informatiche espone l'azienda a rischi di un coinvolgimento sia patrimoniale sia penale, creando al contempo problemi di immagine e sicurezza.

È proprio a quest'ultimo fine che la società **P.M. Group srl** (di seguito denominata anche, semplicemente, “Società” o il “Titolare”) ha provveduto con riferimento, in particolare, alle misure di sicurezza imposte per il trattamento di dati personali dal Regolamento europeo n. 679/2016, a dare idonee indicazioni e istruzioni a tutto il personale interessato dalle predette misure.

Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi ai principi di diligenza e di correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, si ritiene indispensabile adottare ulteriori regole interne di comportamento comune, dirette ad evitare comportamenti inconsapevoli e o scorretti.

**I sistemi informatici aziendali**

Il dispositivo informatico (fisso o mobile, cellulare o tablet) ed i relativi programmi e o applicazioni affidate al destinatario della presente sono, come è noto, strumenti di lavoro, e pertanto:

1. vanno custoditi in modo appropriato;
2. possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non anche per scopi personali, tanto meno per scopi illeciti;
3. ci si deve attenere scrupolosamente e rigidamente a quanto provvisto dall'azienda in materia di UserName e Password in fase di accesso ai sistemi, nei momenti di sospensione dell'attività e a fine sessione;
4. il furto, danneggiamento o smarrimento di tali strumenti debbono essere prontamente segnalati all'azienda.

Ai fini sopra esposti sono, quindi, da evitare atti o comportamenti contrastanti con le predette indicazioni come, ad esempio, quelli cui di seguito richiamati a titolo indicativo.

**Utilizzo del personal computer o dispositivi informatici (es. tablet, smart phone)**

1. E' consentito esclusivamente l'uso di programmi forniti dalla nostra Azienda ed installati dal responsabile IT o persona delegata;
2. Non è consentito utilizzare strumenti software e o hardware al fine di intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni (come per esempio email) e o documenti informatici;
3. Non è consentito modificare le configurazioni impostate sul proprio PC o dispositivo;
4. Non è consentito l'installazione sul proprio PC o dispositivo di mezzi di comunicazione propri;
5. Non è consentito l'utilizzo di periferiche hardware che non siano fornite dall’Azienda;
6. Sui PC o dispositivi dotati di scheda audio e o di lettore CD/DVD non è consentito l'ascolto di programmi, files audio o musicali se non a fini prettamente lavorativi.

**Utilizzo di supporti magnetici**

1. Non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
2. Tutti i files di provenienza esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte dell’amministratore di sistema o persona delegata.

**Utilizzo della rete aziendale**

1. Le unità di rete o locali sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi e o personali. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;
2. L'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per a sicurezza del sistema ovvero acquisiti o installati in violazione del presente regolamento;
3. L’azienda si riserva la facoltà di verificare la tipologia di dati salvati sulla rete aziendale o sulle postazioni aziendali;
4. Non possono essere per nessun motivo collegati alla rete aziendale PC personali.

**Utilizzo della rete internet e dei relativi servizi**

*Navigazione in internet:*

1. Non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate e soprattutto in quelli che possono rivelare le opinioni politiche, religiose o sindacali del dipendente;
2. Non è consentita l'effettuazione di nessun genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dalla Direzione Generale o persona delegata e con il rispetto delle normali procedure di acquisto;
3. Non è consentito lo scarico di software gratuiti (freeware) e shareware prelevato da siti Internet;
4. È vietato ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
5. 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.

*Posta elettronica:*

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

1. Non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate;
2. Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e o discriminatoria per sesso lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e o politica;
3. Non è consentito eliminare messaggi ritenuti importanti per una corretta gestione del rapporto con clienti, fornitori e candidati (messaggi atti a gestire richieste o informazioni da parte di clienti, fornitori o soggetti comunque collegati alla gestione delle relazioni con clienti e fornitori);
4. La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti di lavoro “strettamente” riservati;
5. Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o mail list salvo diversa ed esplicita autorizzazione del proprio responsabile.

Poiché in caso di violazioni contrattuali e giuridiche, sia l'azienda, sia il singolo lavoratore, sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'azienda verificherà nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistemi informatico.

La non osservanza del presente Regolamento può comportare sanzioni disciplinari, civili e penali.

**{Delegate}** dichiara di aver letto e compreso il Regolamento interno per un corretto utilizzo dei sistemi informativi aziendali e dichiara di essere a conoscenza che la mancata osservanza del suddetto regolamento potrebbe causare l'interdizione all'uso dei PC o dispositivi aziendali ed inoltre potrebbe essere causa di azioni disciplinari.

{Date} Firma dell’autorizzato per accettazione

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_