PROCEDURE
REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI

DOCUMENTAZIONE
PER L'ADEGUAMENTO AL
REGOLAMENTO (UE) 2016/679

MODELLO DOCUMENTALE[1]

DATA	VERSIONE	TITOLARE DEL TRATTAMENTO	LEGALE RAPPRESENTANTE
08/04/2021	1.0	**M.C. Service S.a.s.** Via delle Comunicazioni, 15 - 06135 Balanzano, Perugia (PG) Part. IVA 03708310549	Capponi Marco

[1] Il presente documento viene predisposto e mantenuto costantemente aggiornato in attuazione dell'art. 24, par. 1, del Regolamento (UE) 2016/679 secondo il quale *«tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario»*.

STRUTTURA

STRUTTURA DEL MANUALE

PREMESSA

SCOPO E AMBITO DI APPLICAZIONE

NORME COMPORTAMENTALI

PERSONAL COMPUTER

SUPPORTI DI MEMORIZZAZIONE RIMOVIBILI

ROTTAMAZIONE E RIUTILIZZO DEI DISPOSITIVI INFORMATICI

RETE AZIENDALE

NAVIGAZIONE IN INTERNET

POSTA ELETTRONICA

SMARTPHONE

PASSWORD E LOGIN

SICUREZZA DEI DATI E DEI SISTEMI

CONTROLLI

PREMESSA

SCOPO E AMBITO DI APPLICAZIONE

La progressiva diffusione di nuove tecnologie informatiche espone **M.C. Service S.a.s.** (di seguito anche la "Società") a rischi di un diretto coinvolgimento sia di natura patrimoniale che penale, creando al contempo concrete problematiche di immagine e sicurezza.

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

NORME COMPORTAMENTALI
PERSONAL COMPUTER

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro. Pertanto:

- tali strumenti devono essere custoditi in modo appropriato adottando le precauzioni necessarie ad evitare il furto del materiale ICT messo disposizione dal datore di lavoro;
- tali strumenti possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non anche per scopi personali, tanto meno per scopi illeciti;
- debbono essere prontamente segnalati alla Società il furto, il danneggiamento o lo smarrimento di tali strumenti;
- qualunque anomalia riscontrata nel funzionamento del sistema informatico deve essere tempestivamente segnalata al Referente Privacy del Titolare o all'Amministratore di Sistema.

Ai fini sopra esposti sono, quindi, da evitare atti o comportamenti contrastanti con le predette indicazioni e con quelle di seguito rappresentate.

Onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati. Inoltre:

- non è consentito l'uso di programmi non distribuiti ufficialmente dalla Società;
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non è consentito modificare le configurazioni impostate sul proprio PC;
- non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio i modem);
- sui PC dotati di scheda audio e/o di lettore CD/DVD non è consentito l'ascolto di programmi, file audio o musicali, se non a fini prettamente lavorativi;
- non è consentita la visualizzazione e il salvataggio di testi, immagini o registrazioni a carattere razzista, erotico, pornografico, sessuale, osceno o di natura simile indipendentemente da quale ne sia la fonte (ad esempio da chiavetta USB, da CD, da DVD o da siti Internet).

NORME COMPORTAMENTALI
SUPPORTI DI MEMORIZZAZIONE RIMOVIBILI

Non è consentito scaricare file contenuti in dispositivi/supporti di memorizzazione rimovibili (a mero titolo esemplificativo e non esaustivo CD, DVD, chiavette USB, memory card, ecc.) non aventi alcuna attinenza con la propria prestazione lavorativa. Tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione da parte dell'Amministratore di Sistema.

L'utilizzo di dispositivi di memorizzazione rimovibili (in particolare, chiavette USB) è consentito solo se attinente all'attività lavorativa, ma deve essere preventivamente autorizzato.

I dispositivi di memorizzazione rimovibili forniti dalla Società ed utilizzati per l'archiviazione di documenti contenenti dati personali devono essere custoditi in luogo sicuro e restituiti al termine del trattamento; tali dispositivi non possono essere utilizzati per l'archiviazione di file che non siano attinenti all'attività lavorativa svolta.

NORME COMPORTAMENTALI

ROTTAMAZIONE E RIUTILIZZO DEI DISPOSITIVI INFORMATICI

Prima di rottamare un qualsiasi dispositivo informatico aziendale (PC, notebook, smartphone, tablet, dispositivi/supporti di memorizzazione rimovibili, ecc.) il Referente Privacy, con il supporto dell'Amministratore di Sistema (se designato), deve procedere alla cancellazione sicura di eventuali dati personali in essi contenuti.

In caso riutilizzo o riassegnazione ad altro utente di qualsiasi dispositivo informatico si deve provvedere alla cancellazione sicura dei dati personali in esso contenuti. Se ciò non è possibile, il dispositivo non può essere riutilizzato/riassegnato e deve essere distrutto o reso inutilizzabile al termine del suo utilizzo.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

La Società si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza del sistema ovvero acquisito o installato in violazione del presente Regolamento.

Per quanto concerne la navigazione in Internet:

a) non è assolutamente consentita né tollerata la navigazione e la registrazione su portali aventi le seguenti caratteristiche e contenuti:

   1. siti pornografici, pedopornografici e osceni;

   2. siti oltraggiosi e/o discriminatori per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

   3. siti ludici, ricreativi, social network (quali, a mero titolo esemplificativo e non esaustivo, Facebook, Instagram, YouTube) o comunque non attinenti all'attività lavorativa, ad eccezione della pausa pranzo o delle pause lavorative;

   4. siti relativi a chat e forum, ad eccezione della pausa pranzo o delle pause lavorative. Nell'orario di lavoro sono esclusi siti di carattere tecnico attinenti all'attività lavorativa;

   5. siti che consentano di scaricare file audio e/o video, in particolare quelli, i cui contenuti siano riconducibili ai portali specificamente indicati ai precedenti punti 1), 2), e 3);

b) non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili, salvo i casi direttamente autorizzati dalla Società e con il rispetto delle normali procedure di acquisto. Il dipendente che effettua simili transazioni si assume la responsabilità dei rischi di frode da esse derivanti. Sono, naturalmente, consentite le transazioni finanziarie tramite sistema di remote banking effettuate dai responsabili preposti per ragioni aziendali (pagamento stipendi, pagamento fornitori, ecc.) e comunque per attività sempre e comunque attinenti e riconducibili alla gestione economica della Società;

c) non è consentito il download di software gratuiti (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dalla Società, ad eccezione dei casi in cui tale operazione risulti necessaria per l'espletamento dell'attività lavorativa e purché vi sia previa autorizzazione da parte del Referente Privacy o dell'Amministratore di Sistema;

d) non è permessa la partecipazione, per motivi non professionali, a forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nickname);

e) 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;

Al fine di evitare navigazioni improprie sui siti indicati alla lettera a), la Società si riserva di configurare, in qualsiasi momento, sistemi e filtri che, senza determinare un controllo

intenzionale a distanza dei lavoratori, impediscano comunque l'accesso ai portali sopra segnalati.

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

a) non è consentito l'utilizzo della casella di posta elettronica assegnata dalla Società per motivi non attinenti allo svolgimento delle mansioni assegnate;

b) non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa (contenenti testi, immagini o registrazioni a carattere erotico, pornografico, sessuale, osceno, ecc.) e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

c) i messaggi e-mail inviati in seno alla Società sono confidenziali e non possono essere inoltrati al di fuori della stessa o ad altri utenti a meno che non debbano essere comunicati per motivi professionali e che il destinatario possa essere qualificato come persona competente;

d) 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". Lo stesso vale per i documenti in arrivo, per i quali è preferibile richiedere l'invio tramite corriere, con ricevuta o voucher, potendo garantirne la ricezione tramite firma;

e) per ogni comunicazione (interna ed esterna) che abbia contenuti rilevanti o contenga impegni per la Società si deve fare riferimento alle procedure in essere per la corrispondenza ordinaria o PEC;

f) non è consentito l'utilizzo dell'indirizzo di posta elettronica assegnato dalla Società per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione in quanto attinenti all'ambito lavorativo;

g) l'aggiunta di una garanzia "disclaimer" alla fine dei messaggi e-mail inviati fuori dalla Società è obbligatoria e deve essere allegata automaticamente a tutte le e-mail in uscita;

h) non è consentito l'invio automatico di e-mail dall'indirizzo privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (ad esempio ferie, malattia, infortunio ecc.);

i) in caso di ferie e/o di assenza prolungata programmata, ogni dipendente è tenuto ad attivare un sistema di risposta automatica ai messaggi in arrivo, attraverso il quale informi della sua irreperibilità il mittente e fornisca l'indirizzo di posta elettronica aziendale a cui inoltrare direttamente le mail, il cui contenuto, nel rispetto di quanto esposto, deve avere carattere professionale;

j) nel caso di malattia improvvisa, il dipendente può anche nominare un proprio collega di fiducia ed autorizzarlo in maniera specifica alla lettura della posta elettronica pervenuta. Il lavoratore nominato inoltrerà al Referente Privacy del Titolare di

riferimento tutti i messaggi ritenuti rilevanti e necessari per lo svolgimento e la continuità dell'attività lavorativa;

k) in ogni caso, risulta assolutamente consentito (come confermato anche dall'attuale orientamento giurisprudenziale) che il datore di lavoro, al fine di garantire la continuità operativa della Società, dando comunicazione al dipendente, abbia la possibilità di accedere alla casella di posta elettronica del dipendente ovvero inoltrare le e-mail ad altro dipendente regolarmente autorizzato;

l) i messaggi elettronici in entrata vengono sistematicamente analizzati nella ricerca di virus. Un messaggio contenente un virus viene automaticamente eliminato; il mittente ed il destinatario ne sono avvisati attraverso un messaggio specifico;

m) non è attribuita ai destinatari alcuna responsabilità per i messaggi ricevuti quando gli stessi non sono stati sollecitati. Per contro, nell'ipotesi in cui i messaggi, contravvenendo al presente Regolamento, fossero inviati a più riprese da un utente, il destinatario deve prendere le misure appropriate affinché l'invio di tali messaggi venga interrotto;

n) sono vietati i tentativi di accesso a messaggi elettronici di utenti o terzi;

o) è vietato inviare posta elettronica a nome di un altro utente, salvo sua espressa autorizzazione;

p) non è consentito l'invio di messaggi a gruppi numerosi di persone (superiori a 100 persone) senza la preventiva autorizzazione dell'Amministratore di Sistema.

NORME COMPORTAMENTALI
SMARTPHONE

È espressamente vietato l'uso di smartphone per scopi personali nel corso dello svolgimento dell'attività lavorativa, salvo in casi particolari ed urgenti di necessità.

Durante l'orario di lavoro, e ad eccezione della pausa pranzo e delle pause lavorative, non sono consentite comunicazioni a carattere personale, né la consultazione di siti Internet o applicazioni ludiche o ricreative ed è fatto espresso divieto di utilizzare i social network.

La ricezione o effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza. Eventuali ed imprescindibili esigenze personali dovranno essere preventivamente autorizzate.

NORME COMPORTAMENTALI

PASSWORD E LOGIN

L'accesso agli elaboratori della Società è protetto da un sistema di autenticazione (User ID e password). Lo User ID permette di identificare l'utente all'interno del sistema informatico in modo specifico.

Le credenziali personali di accesso assegnate della Società ad ogni utente non devono essere divulgate e devono essere custodite dall'assegnatario con la massima diligenza.

È severamente vietato usare la password e lo User ID di un altro utente.

Qualunque utente che acceda al sistema informatico della Società, indipendentemente dalla modalità, è responsabile dell'uso che fa di tale sistema, in conformità con il presente Regolamento.

Le postazioni di lavoro informatiche non possono essere abbandonate per lunghi periodi senza che siano protetti gli accessi alle applicazioni.

È severamente vietata la diffusione di informazioni confidenziali relative alla Società ad uno o più utenti, clienti o terzi, a meno che tale diffusione sia debitamente giustificata da motivazioni di carattere professionale.

Poiché in caso di violazioni contrattuali e giuridiche sia la Società sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, **M.C. Service S.a.s.** si riserva la facoltà di verificare, nei limiti consentiti dalle norme legali e contrattuali, e per ragioni esclusivamente organizzative, il rispetto delle regole e l'integrità del proprio sistema informatico.

Tali controlli, in osservanza a quanto previsto dall'art. 4, comma 2, della legge 20 maggio 1979, n. 300 (Statuto dei lavoratori) e dalla delibera n. 13 del Garante per la protezione dei dati personali del 1° marzo 2007, saranno effettuati gradualmente e secondo le seguenti modalità:

- in caso di riscontrate anomalie nell'utilizzo della posta elettronica e della navigazione in Internet, si procederà in prima battuta a mettere in atto verifiche di reparto e ad effettuare le dovute comunicazioni scritte indirizzate all'area aziendale;

- se, nonostante i controlli effettuati a livello di reparto, le anomalie dovessero persistere, si procederà in seconda battuta a mettere in atto verifiche di ufficio e per gruppi di lavoro al fine di individuare l'area aziendale, che deve esser richiamata all'osservanza delle regole, sempre mediante le dovute comunicazioni scritte indirizzate all'ufficio e/o al gruppo di lavoro;

- qualora le verifiche effettuate con le modalità descritte nei punti precedenti non fossero state sufficienti ad eliminare le anomalie riscontrate nell'utilizzo corretto di Internet e della posta elettronica, si procederà, in ultima battuta, ad effettuare verifiche sulle singole postazioni.

Eventuali controlli destinati ai personal computer verranno effettuati esclusivamente per ragioni di carattere tecnico e di salvaguardia degli strumenti elettronici aziendali. I suddetti controlli non potranno mai essere attivati per realizzare verifiche a distanza delle attività dei lavoratori.

I dipendenti saranno, comunque, preavvertiti puntualmente qualora le postazioni loro assegnate fossero oggetto di accesso remoto da parte del Referente Privacy del Titolare o dell'Amministratore di Sistema.

Il presente Regolamento verrà trasmesso a tutti i dipendenti ed ai collaboratori della Società autorizzati al trattamento dei dati personali per opportuna conoscenza e presa visione.

L'osservanza delle norme del Regolamento deve considerarsi parte essenziale delle obbligazioni contrattuali dei dipendenti e dei collaboratori di **M.C. Service S.a.s.** ai sensi e per gli effetti dell'art. 2104 del codice civile.

La violazione delle norme del Regolamento potrà costituire inadempimento alle obbligazioni primarie del rapporto di lavoro o illecito disciplinare, con ogni conseguenza di legge, anche in ordine alla conservazione del rapporto di lavoro e potrà comportare il risarcimento dei danni dalla stessa derivanti.