Regolamento interno per il corretto utilizzo dei dispositivi informatici, posta elettronica e trattamento degli archivi cartacei

Approvato con verbale del Consiglio di Amministrazione del 20/07/2022

Area Privacy – RISI Rev. 00 del 06.06.2022

Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Dispositivi (PC, notebook, tablet, smartphone, ecc.), espone la società ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e l'utilizzo degli archivi cartacei della nostra azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, si è adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati. Queste norme hanno lo scopo di conciliare le seguenti esigenze:
- da un lato il diritto del lavoratore/utente ad usare liberamente le tecnologie messe a disposizione (anche quale strumento di crescita professionale) ed il diritto al pieno rispetto della propria riservatezza e
- dall'altro il diritto-dovere del Datore di lavoro di far sì che durante l'orario di lavoro non si faccia un uso improprio degli strumenti aziendali messi a disposizione;
- adeguarsi alla Normativa in materia di tutela dei dati personali Regolamento EU 679/2016 ed in particolare agli Artt. 29, 32 che prescrivono al Titolare del trattamento di istruire gli addetti al trattamento e applicare le misure di sicurezza necessarie alla tutela dei dati personali.

Definizioni
Soggetti addetti al trattamento
L'art. 29 del GDPR definisce come Soggetti addetti al trattamento "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile".
Dati
L'incaricato deve essere sempre in grado di individuare il tipo di dato che sta trattando secondo quanto stabilito dalla Legge. Qualora non fosse in grado, deve fare riferimento al Responsabile o al Titolare del Trattamento.
Vengono riportate di seguito le definizioni e i riferimenti normativi per una più chiara comprensione:
• **dati personali**: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
• **dati particolari**: l'Art. 9 del GDPR definisce in tale modo i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'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; sono dati particolari anche i dati genetici e biometrici;
• **dati giudiziari**: tali sono considerati informazioni in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale; questa tipologia di dato è definito dall'Art. 10 del GDPR;

• **dati che presentano rischi specifici**: si tratta di dati che, pur non essendo così delicati come quelli sensibili e giudiziari, presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati, ovvero alle modalità di trattamento o agli effetti che esso può determinare: in considerazione di tale fatto, il loro trattamento è ammesso nel rispetto delle misure e degli accorgimenti, prescritti dal Garante a garanzia dei soggetti interessati. In questa categoria di dati possono ricadere ad esempio le informazioni relative alla capacità di solvibilità del debito, dati biometrici, dati di geolocalizzazione, immagini riprese da impianti di videosorveglianza, ecc.

Istruzioni e raccomandazioni

I dispositivi informatici (personal computer fissi, portatili, tablet, smartphone, stampanti multifunzione, fotocopiatrice, scanner, fax; ecc..) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro il cui utilizzo ricade sotto la responsabilità del Titolare e che possono contenere dati riservati e informazioni personali di terzi.
Vanno custoditi in modo appropriato evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone e possono essere utilizzati solo per fini professionali attinenti esclusivamente alle mansioni assegnate, evitando pertanto usi per fini personali, al di fuori dei casi consentiti ed autorizzati espressamente dai propri responsabili aziendali, tanto meno per scopi illeciti.
Debbono essere prontamente segnalati all'azienda il furto, danneggiamento o smarrimento di tali strumenti. Le impostazioni dei dispositivi informatici sono predisposte dagli addetti informatici addetti sulla base di criteri e profili decisi dalla Direzione in funzione della qualifica del dipendente, delle mansioni cui questo è adibito, nonché dalle decisioni e della politica di utilizzo di tali strumenti stabilita dall'azienda stessa. Tutti gli utenti (di seguito addetti) sono tenuti ad attenersi scrupolosamente alle indicazioni sotto riportate.

Utilizzo dei dispositivi informatici

• I telefoni ed i fax aziendali, non possono essere utilizzati per ricevere o effettuare comunicazioni private; si raccomanda quindi di limitare l'uso del telefono d'ufficio e del fax alle comunicazioni necessarie per lo svolgimento del lavoro, salvo casi eccezionali; il dipendente è tenuto a limitare la ricezione di telefonate personali sulle linee telefoniche dell'ufficio, avendo cura di contenere la durata delle conversazioni al minimo indispensabile;
• durante l'orario lavorativo, limitare alla gestione delle urgenze o per motivi strettamente eccezionali l'utilizzo di smartphone, tablet, ed altri device privati;
• gli addetti non devono violare o tentare di violare i sistemi di sicurezza informatici;
• gli addetti non devono né cercare di ottenere accessi non autorizzati, né favorire analoghe attività da parte di altri utenti, interni o esterni; gli addetti non possono, deliberatamente e in modo non autorizzato, modificare o tentare di modificare dati contenuti nei sistemi in rete. Gli addetti non possono intercettare, tentare d'intercettare o accedere a dati in transito sulla rete aziendale, che non siano loro diretti;
• gli addetti non possono mascherare la loro identità quando usano i sistemi della rete aziendale. Gli addetti non possono inoltre impersonare altri individui;

• non è consentito installare programmi provenienti dall'esterno salvo espressa autorizzazione della Direzione; non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
• 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 consentita l'installazione sui PC a disposizione, di mezzi di comunicazione propri;
• tutti i software caricati sul sistema operativo ed in particolare quelli necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi dagli utenti (salvo quando questo sia richiesto dalla Direzione per compiere attività di manutenzione o aggiornamento);
• non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati al fine di scaricare materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.);
• l'uso della rete aziendale in violazione di norme del Codice Civile o Penale è proibito. Esempi di queste violazioni sono: distribuzione di materiale osceno; ricezione, registrazione, trasmissione o possesso d'immagini pornografiche relative a minori; violazione di copyright;

• ogni utente è tenuto a segnalare con tempestività alla Direzione qualsiasi malfunzionamento degli strumenti informatici in uso;
• non è consentito procedere autonomamente a tentativi di correzione di errori o malfunzionamenti, se non dietro esplicita autorizzazione della Direzione;
• Non si deve procedere ad operare sulle connessioni elettriche o di rete, se non dietro specifica autorizzazione della Direzione. In nessun caso si deve operare sulle connessioni elettriche o di rete quando i dispositivi sono in tensione;
• non è permesso modificare la configurazione del proprio posto di lavoro né dal punto di vista hardware, né dal punto di vista software, senza precedente autorizzazione della Direzione. In particolare non è permesso spostare dispositivi quali unità centrali, unità video o stampanti, scanner, telefoni o fax; non è possibile modificare la configurazione dei personal computer;
• i dispositivi informatici "stand alone" o in 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; l'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni;
• non è consentito utilizzare stampanti con anche funzioni di copia, scansione e fax o qualsiasi altro strumento messo a disposizione dal Titolare, compresa la cancelleria, per scopi non attinenti all'espletamento delle proprie mansioni aziendali;
• ogni comunicazione scritta (interna ed esterna), inviata o ricevuta attraverso strumenti informatici, scanner, fax, ecc. che riguardi o contenga impegni per l'azienda deve essere visionata e autorizzata dalla Direzione.

Utilizzo dei dispositivi mobili

• L'utente è responsabile di dispositivi mobili (PC portatile, tablet, smartphone ecc.) assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.;
• agli stessi si applicano tutte le regole di utilizzo previste per i PC fissi o agli altri dispositivi informatici presenti in azienda;
• i dispositivi mobili utilizzati all'esterno (convegni, fiere, visite, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto. In particolare essi non devono mai essere lasciati incustoditi nell'autovettura neppure nel bagagliaio;
• in caso di furto o smarrimento è obbligatorio comunicare tempestivamente l'accaduto alla Direzione, effettuare denuncia presso l'ufficio di pubblica sicurezza locale e consegnare copia della stessa in Azienda.
• solo gli Utenti che saranno specificatamente destinatari dei relativi fringe benefits potranno utilizzare i dispostivi mobili assegnati per lavoro anche in uso c.d. promiscuo (ossia anche ad uso personale). In tal caso lo strumento di lavoro potrà essere sottoposto a controlli sul corretto utilizzo ai sensi del presente regolamento. Tale controllo verrà di regola svolto solo ed esclusivamente in ipotesi di venuta a conoscenza di presunte gravi violazioni di tipo penale o civile.

Gestione degli archivi, file, documenti e cartelle

• Gli archivi, file, documenti e cartelle generati e/o gestiti dagli utenti devono essere memorizzati sui dispositivi di rete. La Direzione garantisce la sicurezza delle informazioni memorizzate sui dispositivi di rete eseguendo periodici backup degli archivi.

• Non è consentita la copia di archivi aziendali di qualsiasi genere o specie né su dispositivi asportabili (CD, DVD, dischi o chiavi USB, tablet, smartphone e simili) né su dispositivi di memorizzazione esterni all'Azienda (ad esempio in server accessibili mediante Internet, aree dati in Cloud tipo Dropbox, Google Drive, ecc.), né via posta elettronica su account non appartenenti al dominio aziendale, se non dietro esplicita autorizzazione della Direzione.

Utilizzo di Internet

La rete internet può e deve essere utilizzata dal dipendente a supporto dell'attività lavorativa nell'ambito delle mansioni ed autorizzazioni assegnategli dal proprio responsabile. Al fine di ridurre il rischio di un utilizzo improprio della rete e allo stesso tempo di evitare per quanto possibile controlli che potrebbero comportare il trattamento di dati personali, l'azienda si riserva di adottare l'utilizzo di sistemi e filtri che possono prevenire determinate operazioni, reputate inconferenti con l'attività lavorativa, quali ad esempio l'upload o l'accesso a determinati siti e/o il download di file o software aventi particolari caratteristiche (quali ad esempio dimensionali o di tipologia di dato), con individuazione di categorie e liste di siti cui non è concesso l'accesso (black list), in quanto non attinenti l'attività lavorativa.
Di seguito sono riportati i principi che devono essere rispettati al fine di assicurare una navigazione internet sicura:
• non è permessa la creazione di siti e di pagine HTML in domini esterni, anche se gratuiti, senza autorizzazione della Direzione;
• non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;

• a maggior ragione non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di Legge;
• non è inoltre consentito navigare in siti che possano rivelare una profilazione dell'individuo definita 'particolare' ai sensi del GDPR: quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente o le sue abitudini sessuali;
• non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal Titolare con il rispetto delle normali procedure di acquisto;
• non è consentito lo scarico di software gratuiti trial, freeware e shareware prelevati da siti Internet, se non espressamente autorizzato dalla Direzione;
• non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) attraverso Internet, web, ftp, servizi di condivisione, ecc.;
• non è consentita la memorizzazione di documenti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
• è vietata ogni forma, anche a titolo personale, di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
• non è permessa la partecipazione, per motivi non professionali a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames). L'accesso a tali fonti di informazione, esclusivamente per motivi professionali, potrà avvenire solo previa autorizzazione scritta da parte della Direzione.

Utilizzo della posta elettronica aziendale

La posta elettronica, sia interna che esterna, è un mezzo di comunicazione che il Titolare mette a disposizione del dipendente esclusivamente per consentirgli lo svolgimento della propria attività lavorativa, pertanto:
• si raccomanda di evitare di utilizzare tali strumenti per motivi non attinenti allo svolgimento delle mansioni assegnate, salvo casi eccezionali di comprovata urgenza e necessità;

• 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;
• la posta elettronica diretta all'esterno della rete informatica aziendale non deve essere usata per inviare informazioni, dati o documenti di lavoro "Strettamente Riservati";
• non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o mail-list; che non siano strettamente inerenti all'attività aziendale;
• non è consentito utilizzare caselle di posta elettronica private per corrispondenza inerente alle attività aziendali;
• è necessario configurare un sistema di risponditore automatico da attivare in caso di prolungata assenza che avvisi il mittente dell'assenza. Si raccomanda di:
• inserire un indirizzo mail aziendale di un collega che il mittente può contattare in caso di urgenza;
• adottare il seguente testo "Mi trovo al momento fuori sede! Potrò risponderti solo a partire da p.v. Per urgenze è possibile inviare una mail all'indirizzo

Area Privacy – RISI Rev. 00 del 06.06.2022

Gestione delle credenziali e password

L'accesso ai dispositivi informatici, ai programmi applicativi e alle varie funzionalità messe a disposizione degli utenti per lo svolgimento dell'attività, avviene previa autenticazione, che consiste nella verifica dell'identità del dipendente attraverso l'uso di un codice identificativo e di una parola chiave (password). Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione.
È necessario rispettare l'ambito di competenza (i dati cui poter accedere) ed il profilo di autorizzazione (tipi di trattamento consentito) indicate nella propria nomina ad Incaricato.
Elaborare le password seguendo le istruzioni sotto riportate:
• al primo accesso ad un sistema e/o ad una banca dati, l'incaricato ha la responsabilità di cambiare la password assegnatagli dalla Direzione. Tale password deve essere al minimo lunga 8 caratteri, includere sia lettere, sia cifre e una maiuscola;
• la password per l'accesso alla rete aziendale scade ogni 6 mesi e va obbligatoriamente cambiata;
• la password per l'accesso a sistemi e/o banche dati deve essere modificata dall'incaricato almeno ogni 6 mesi, se non altrimenti specificato;
• la password non deve contenere elementi che possano in qualche modo essere legate all'incaricato come, ad esempio il suo nome, quello di sua moglie/marito, del cane, date di nascita, numeri di telefono etc.;
• la password non deve essere comunicata a nessuno, lo scopo principale del suo utilizzo è assicurare che nessun altro possa accedere alle risorse o sostituirsi all'incaricato;
• l'incaricato ha la responsabilità di custodire con diligenza la propria password, in nessuna circostanza il dipendente è autorizzato a condividere le proprie credenziali di autenticazione con altri addetti o terze persone;
• l'incaricato dovrà informare la Direzione nel caso in cui, abbia fondati motivi di ritenere che possa essere compromessa la riservatezza della password, o comunque che ne sia stato fatto un utilizzo indebito cambiandola immediatamente;
• L'incaricato può nominare un "fiduciario" che in caso di assenza (temporanea o prolungata) possa accedere ai suoi dispositivi informatici, inclusi i messaggi di posta elettronica in entrata e in uscita, al fine di garantire l'ordinaria operatività aziendale o per ragioni di sicurezza. L'incaricato sarà prontamente informato dell'avvenuto accesso il prima possibile, fornendo adeguata spiegazione e redigendo apposito verbale. La password verrà resettata e l'incaricato invitato a formularne una nuova. I

codici identificativi e le password degli addetti saranno disattivate in caso di cessazione del loro rapporto di lavoro.

Custodia dispositivi informatici
I dispositivi informatici non possono essere lasciati incustoditi:
• in caso di allontanamento anche temporaneo dalla postazione di lavoro o comunque dal dispositivo informatico è necessario non lasciare il sistema aperto con la propria password;
• al fine di evitare che persone estranee effettuino accessi non permessi l'incaricato deve eseguire il "log out" della sessione di lavoro o in alternativa attivare funzioni che, trascorso un breve periodo di tempo predeterminato in cui il dispositivo resta inutilizzato, non consentano più l'accesso al dispositivo se non previa imputazione di password.

Area Privacy – RISI Rev. 00 del 06.06.2022
• in particolare i supporti di memorizzazione rimovibili devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: è bene adottare archiviazioni in modo che vengano conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
• una volta cessate le ragioni per la conservazione dei dati, i supporti di memorizzazione rimovibili non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

Protezione dispositivi informatici
L'azienda adotta adeguati ed aggiornati strumenti e metodologie per la protezione dei dispositivi: segmentazione della rete, firewall, antispam, antiphising, endpoint protection (antivirus), web filtering, per i file scaricati da internet, aggiornamenti automatici di sicurezza dei sistemi operativi, backup periodici ecc. L'incaricato è comunque tenuto ad adottare i seguenti comportamenti per prevenire danni ai sistemi, o ridurne il rischio, dall'esecuzione di software "malevolo":
• utilizzare soltanto programmi provenienti da fonti fidate. Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzare programmi non autorizzati;
• evitare la trasmissione di file eseguibili (.COM, .EXE,. OVL, .OVR) e di sistema (.SYS) tra computer in rete;
• proteggere la memoria di massa rimovibili (dischi, chiavette, ecc.) autorizzati da scrittura quando possibile.
In questo modo è possibile evitare l'accesso e l'utilizzo da parte di software dannoso:
• non trasferire documenti, file, archivi relativi a dati aziendali su dispositivi non aziendali per essere trattati od utilizzati esternamente alla rete aziendale e riportati nella stessa;
• non aprire e non diffondere messaggi email di provenienza dubbia o con mittenti sconosciuti o con oggetto non pertinente alle proprie attività con evidenti errori ortografici o contenenti allegati o link poco chiari o dubbi, cancellandoli tempestivamente;
• nel caso di apertura di messaggi di tale tipo almeno non aprire gli eventuali allegati o non accedere ai link presenti e provvedere a eliminarli tempestivamente;
• in ogni caso, nel dubbio che ci sia in corso un'attività anomala o malevola sul proprio dispositivo spegnere lo stesso e/o staccare il cavo di rete, ed allertare immediatamente la Direzione La tempestività nell'azione di bonifica è essenziale per limitare eventuali danni arrecati al dispositivo e ad altri dispositivi o apparati della rete aziendale.

Riservatezza e cautela nella tenuta e comunicazione dei dati

Tutte le informazioni aziendali sono riservate all'utilizzo ed alla circolazione unicamente all'interno dell'Azienda, tranne nei casi diversi esplicitamente previsti, anche informazioni di normale quotidianità aziendale o ritenute non riservate all'interno dell'interscambio tra addetti, assumono
diversa importanza, e quindi necessitano di una maggiore tutela, se comunicate all'esterno a soggetti terzi.
La salvaguardia delle informazioni e dei dati oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo aziendale, è anche un espresso obbligo di legge nei confronti di qualsiasi

soggetto definito "interessato" e soprattutto se relativi a persone e se sono di carattere sensibile.
A fronte di tali motivazioni è importante ribadire la necessità di osservare ogni cautela nel trasferire all'esterno qualsiasi informazione proporzionalmente al loro contenuto e all'attendibilità dell'interlocutore. ed attenersi a quanto riportato sotto.
Ogni utente ha accesso unicamente ai dati per i quali è stato autorizzato in relazione alle necessità per lo svolgimento delle mansioni assegnate. Questo si riferisce in generale a tutte le informazioni trattate dal Sistema Informativo Aziendale, ed in particolare ai dati personali, per i quali l'Azienda assicura l'osservanza delle normative di legge.
Nessuna informazione deve essere comunicata e diffusa all'esterno dell'Azienda, se non esiste una precisa motivazione per farlo. Autorizzazioni generali di comunicazione ad esterni vengono comunicate insieme alle altre informazioni necessarie per svolgere la propria attività.
In casi diversi deve essere richiesta l'autorizzazione al proprio responsabile. Nessun utente è autorizzato a rispondere a richieste telefoniche o interviste che chiedano notizie dirette o indirette riguardanti il Sistema Informativo. L'unica risposta ammessa in questi casi deve essere la seguente: "Non sono autorizzato a rilasciare questo tipo di informazioni. Dovete rivolgervi direttamente alla Direzione".
Nessun utente è autorizzato a trasmettere alcuna informazione, documento, file o archivio in risposta ad una richiesta proveniente da fonte non accertata e se non espressamente autorizzato dal responsabile del trattamento dello stesso.
In caso di richieste inoltrate da soggetti esterni (telefonicamente, per mail, per posta o altri mezzi) non è consentito dare informazioni sui ruoli ricoperti nell'azienda o altre informazioni relative all'assetto societario e patrimoniale; è necessario, invece, identificare l'interlocutore e individuare le motivazioni delle richieste.

Linee guida per l'utilizzo dei profili social network
L'avvento e la crescente diffusione dei servizi di social network segnalano un cambiamento radicale nell'accessibilità pubblica a dati ed informazioni, secondo modalità e misure sinora sconosciute. Assimilando i mezzi di diffusione del pensiero dei social network (Facebook, Twitter, Linkedin, WhatsApp, Blog, Chat ed altro), alle dichiarazioni rese dall'incaricato a mezzo degli strumenti tradizionali di comunicazione pubblica (giornali, radio, televisione), si ricorda che il diritto di manifestazione del pensiero e di critica in costanza del rapporto di lavoro soggiace a determinati limiti, esplicitazioni dei doveri di fedeltà, di riservatezza ed adesione ai valori della Società, che incombono sull'incaricato in quanto deducibili nella prestazione lavorativa medesima, in particolare attinenti a:
a) continenza verbale;
b) continenza sostanziale: verità dei fatti e del ruolo ricoperto all'interno della Società;
c) divulgazione di qualsiasi tipo di dato o informazione relativo e attinente all'attività dell'incaricato all'interno della Società.
Allorché il "profilo privacy" scelto e adottato dall'incaricato consente la visualizzazione dei suoi "post", commenti, video e foto, anche ad una cerchia di utenti aperta e sostanzialmente indeterminabile, l'incaricato soggiace a valutazioni ed ad azioni di responsabilità disciplinare quando integri una lesione

del rapporto fiduciario che lega l'incaricato alla Società, con evidenti profili di violazione della riservatezza e danno dell'immagine, alla continuità e alla regolarità dell'attività.

Area Privacy – RISI Rev. 00 del 06.06.2022

Controlli aziendali

Il Titolare fermo restando il divieto di monitoraggi sistematici e costanti, deve effettuare periodicamente controlli ed ispezioni, anche a garanzia della sicurezza e riservatezza dei dati personali oggetto di trattamento sempre nel rispetto dell'articolo 4 della Legge n. 300 del 20 maggio 1970.

La Società, quale datore di lavoro, si riserva la facoltà di accedere in qualsiasi momento, nel rispetto della normativa sulla privacy e del presente regolamento, a tutti gli strumenti informatici, telematici e telefonici aziendali assegnati in dotazione ai singoli utenti per l'espletamento delle proprie mansioni lavorative, ai documenti e ai dati personali e alle altre informazioni ivi contenute. Si richiama quanto già indicato anche per i dispositivi portatili assegnati anche in uso c.d. promiscuo.

Resta inteso che la Società si astiene da qualsiasi finalità di controllo sistematico dell'attività lavorativa (vale a dire dal compimento di controlli prolungati, continuativi, intenzionalmente ad elevata frequenza).

Nell'espletare controlli e verifiche le funzioni interne preposte devono garantire la massima riservatezza dei dati conosciuti, anche incidentalmente, in occasione della verifica, pena l'applicazione di sanzioni disciplinari in base alla gravità dell'accaduto.

Le informazioni derivanti dai controlli potranno quindi essere rese disponibili solo ed esclusivamente a soggetti interni o esterni alla Società per cui la comunicazione sia necessaria in relazione alle finalità perseguite con l'accesso, comunque nel rispetto dei principi di correttezza, necessità, pertinenza e non eccedenza previsti dalla legge.

I controlli potranno essere collettivi (es. rete aziendale, funzionamento della posta elettronica) oppure su singoli dispositivi o postazioni o utenti e avverranno, più spesso, in caso di anomalie o
abusi (spot o reiterati). Oltre a ciò la Società si riserva di effettuare specifici controlli sui software e/o applicazioni caricati sui dispostivi informatici aziendali utilizzati dagli addetti, al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stressi alla Normativa vigente e di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che hanno causato danno o che ledono diritti di terzi o che comunque sono illegittime.

I controlli potranno avere luogo con o senza preavviso. Il preavviso potrà essere collettivo od individuale, e sarà comunicato all'utente nel rispetto del principio di gradualità, di cui meglio oltre. Nei casi in cui sia necessario restringere l'ambito della verifica, l'azienda si riserva di poter protrarre l'indagine fino all'individuazione puntuale del singolo utente, secondo il principio di "Graduazione dei controlli" enunciato al punto 6.1(8) in premessa al provvedimento del Garante: "le linee guida del Garante per posta elettronica e internet" – (Gazzetta Ufficiale n. 58 del 10 marzo 2007).

In caso di anomalie, il personale dell'IT effettueranno pertanto, di regola, controlli che si concluderanno con avvisi e richiami generalizzati diretti a tutti i soggetti dell'area o del settore o altra unità organizzativa in cui si è rilevata l'eventuale anomalia.

Ulteriori controlli aventi base individuale potranno avvenire:

a) in caso di ulteriori e anomalie o abusi successivi/ all'avviso precedente, o comunque

b) anche fin dall'inizio, nel caso in cui, sulla base degli elementi conoscitivi disponibili, il Titolare abbia ragionevole motivo di sospettare che l'utilizzo degli strumenti aziendali da parte del singolo individuo, in assenza di immediati specifici controlli possa arrecare un pregiudizio anche solo potenziale alla
stessa (controlli aventi scopo cd. "difensivo") e/o determinare eventi che le finalità stesse del controllo mirano a prevenire od a contrastare.

Area Privacy – RISI Rev. 00 del 06.06.2022

Il Titolare si riserva la possibilità di inoltrare avvisi individuali (per email o telefono). Tali avvisi possono essere ad esempio sospesi o ritardati laddove se immediati comportino un pericolo di elusione anche

parziale, da parte dell'utente, degli accertamenti o provvedimenti aziendali, cioè di alterazione, distruzione od occultamento delle informazioni che i controlli sono diretti a raccogliere e/o a consentire, oppure causino un rischio di aggravamento del danno o la compromissione della difesa o dell'accertamento di diritti, responsabilità giudiziali o attività istituzionali della Società. Nei casi testé menzionati, l'informazione potrà/dovrà essere data a posteriori.
Gli avvisi preventivi possono altresì essere omessi per i controlli difensivi o richiesti da Pubbliche Autorità (Polizia Postale, Autorità Giudiziaria, ecc.) o in caso di incidenti che necessitino di interventi immediati ed urgenti secondo la valutazione del personale preposto alla loro gestione.

Gestione documenti cartacei contenenti dati personali
Per il trattamento dei documenti cartacei è necessario rispettare sempre le indicazioni del Titolare o del Responsabile in merito agli archivi a cui poter accedere e ai documenti che è possibile trattare: non trattare nessun documento al di fuori delle autorizzazioni.
Una volta presi in carico, gli atti e i documenti, contenenti dati personali, non devono essere lasciati senza controllo per un tempo indefinito, ma occorre provvedere in qualche modo a controllarli e custodirli, per poi restituirli al termine delle operazioni affidate.
In caso di affidamento di atti e documenti contenenti dati sensibili o giudiziari, il controllo e la custodia devono avvenire in modo tale, che ai dati non accedano persone prive di autorizzazione. A tale fine, è quindi necessario dotarsi di cassetti con serratura, o di altri accorgimenti aventi funzione equivalente, nei quali riporre i documenti contenenti dati sensibili o giudiziari prima di assentarsi dal posto di lavoro, anche temporaneamente.
Assicurare l'accesso a tali archivi alle sole persone autorizzate da specifico e scritto profilo di autorizzazione ricordando loro di non abbandonare mai tali documenti e di riconsegnarli non appena terminato l'incarico che ne ha determinato il trattamento.

Interruzione del rapporto di lavoro
In caso di interruzione del rapporto di lavoro, il Titolare, provvederà a attuare le seguenti operazioni al fine di garantire il rispetto del principio di correttezza dei trattamenti e di tutela della dignità della persona:
• sarà consentito all'interessato di partecipare alla ricognizione (e, se del caso, alla consegna) di documenti o di oggetti collocati all'interno degli uffici, soprattutto in caso di assegnazione di spazi e postazioni ad uso di un singolo e per un periodo significativo di tempo;
• all'interruzione del rapporto di lavoro, l'interessato dovrà restituire alla Direzione tutti i dispositivi informatici aziendali affidati dalla Società, per questo motivo e per quanto non sia consentito il c.d. uso personale dei dispositivi aziendali, si raccomanda di eliminare preventivamente ed esclusivamente i contenuti "personali" eventualmente presenti sui dispositivi e dall'account di posta elettronica aziendale;
• l'account di posta elettronica (ove direttamente riconducibile all'interessato) verrà disattivato nello stesso giorno di cessazione del rapporto di lavoro e per un periodo di 6 mesi la Direzione provvederà

ad attivare un sistema di risponditore automatico allo scopo di avvisare eventuali mittenti che il lavoratore/utente non è più in forza alla società e quindi nel caso verrà fornito un indirizzo alternativo (interno alla società) al quale inviare eventuali comunicazioni;
• i dati esterni e il contenuto della corrispondenza relativa all'account di posta elettronica disattivato, riconducibile all'Utente saranno conservati:
• per 12 mesi dalla cessazione del rapporto/disattivazione dell'account, limitatamente al perseguimento di finalità organizzative, produttive e di sicurezza;

Medí Società di Mutuo Soccorso
C.F.: 90162310271 | R.E.A. n. 370990

Sede Legale:
Via Mameli 10/12 Padova 35131

Telefono: 800 90 34 35
E-mail: info@medimutua.org
Pec: pec@pec.medimutua.org
Sito: www.medimutua.org

Sedi Operative:
Via Goffredo Mameli 10/12, 35131 Padova
Via Soperga 14/A, 20127 Milano
Via Saffi 4, 60121 Ancona

per la parità di genere
Sistema di gestione per la parità di genere
UNI/PdR 125:2022 certificato
Certified gender equality management system

• per un periodo massimo di 10 anni, dalla cessazione del rapporto/disattivazione dell'account, per l'esclusiva finalità di tutela dei diritti del Titolare in sede giudiziaria, nei limiti di cui all'art. 160-bis del D.lgs. 196/2003, come modificato dal D.lgs. 101/2018.
• la Direzione provvederà alla formattazione completa dei device restituiti, avendo cura di eliminare eventuali copie dei contenuti presenti nei back-up aziendali;
• i dati dell'interessato saranno conservati per il tempo necessario a garantire il rispetto degli obblighi legislativi.

Applicabilità e responsabilità degli utenti
Il presente regolamento si applica a tutto il personale dipendente e a chiunque, qualsiasi sia la forma contrattuale che lo collega alla Società e lo abilita ad utilizzarne i sistemi informatici, abbia accesso autorizzato alle risorse informatiche aziendali.
Il regolamento si applica a tutti gli utenti senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).
Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (professionista) in possesso di specifiche credenziali di autenticazione.
Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.
Tutti gli addetti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Titolare del trattamento.

Formazione sulla protezione dei dati personali
Il Titolare del trattamento è tenuto ad erogare specifica formazione in materia di Privacy (Artt. 29, 32 del GDPR). In particolare relativamente a:
• profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle relative attività, e conseguenti responsabilità che ne derivano;
• rischi che incombono sui dati;
• misure disponibili per prevenire eventi dannosi;
• modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare;
• conseguenze disciplinari e non derivante dal mancato rispetto del presente regolamento.

Area Privacy – RISI Rev. 00 del 06.06.2022
Informativa agli utenti ex art. 13 Regolamento UE n. 2016/679
Il presente Regolamento, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici aziendali, e in relazione ai trattamenti di dati personali svolti dal Titolare e finalizzati alla effettuazione di controlli leciti (come definiti nell'apposito paragrafo), vale quale informativa ex art. 13 del Regolamento UE n. 2016/679

Entrata in vigore del regolamento
Il nuovo regolamento entrerà in vigore a partire dal 20/07/2022, data di approvazione con verbale del Consiglio di Amministrazione.
Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalla presente.

Medí Società di Mutuo Soccorso
C.F.: 90162310271 | R.E.A. n. 370990

Sede Legale:
Via Mameli 10/12 Padova 35131

Telefono: 800 90 34 35
E-mail: info@medimutua.org
Pec: pec@pec.medimutua.org
Sito: www.medimutua.org

Sedi Operative:
Via Goffredo Mameli 10/12, 35131 Padova
Via Soperga 14/A, 20127 Milano
Via Saffi 4, 60121 Ancona

per la parità di genere
Sistema di gestione per la parità di genere
UNI/PdR 125:2022 certificato
Certified gender equality management system