"AZIENDA OSPEDALIERA DEI COLLI"
Monaldi-Cotugno-CTO
Via L. Bianchi s.n.c. - 80131- Napoli
C.F/P.I. 06798201213

INFORMATIVA UTILIZZO POSTA ELETTRONICA E INTERNET

PREMESSA

L'utilizzo della posta elettronica e di internet sono disciplinati dal **"REGOLAMENTO AZIENDALE SULL'UTILIZZO DEI SISTEMI INFORMATICI (Posta Elettronica, Rete Intranet/Internet, Postazioni di Lavoro)**" pubblicato sul sito aziendale e pertanto deve avvenire nel rispetto totale di quanto in esso previsto e con la piena responsabilità dei soggetti a cui tale utilizzo è assegnato.

L'accesso alla posta elettronica aziendale, nonché l'accesso a internet vengono forniti al personale autorizzato al fine di svolgere le attività lavorative o per adempiere ad obblighi di contratti di collaborazione con persone esterne all'azienda e pertanto, essendo l'utilizzo di essi legato ai vincoli contrattuali, possono essere oggetto di monitoraggio da parte dell'Azienda.

A tal proposito l'Azienda, per gli eventuali controlli sull´uso degli strumenti elettronici, eviterà qualsiasi interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure dei soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. L´eventuale controllo sull'utilizzo degli strumenti aziendali avverrà nel pieno rispettato dei principi di pertinenza e non eccedenza e, per quanto possibile, sarà effettuato preliminarmente su dati aggregati riferiti all´intera struttura lavorativa o a sue aree. Nel caso di rilevazione di un utilizzo anomalo degli strumenti aziendali, un eventuale controllo anonimo verrà comunicato e concluso con un avviso generalizzato con l´invito ai dipendenti ad attenersi scrupolosamente a compiti assegnati e alle istruzioni impartite. L´avviso sarà circoscritto a dipendenti afferenti all´area o settore in cui è stata rilevata l´anomalia, salvo casi specifici di estrema rilevanza dove verrà esteso all'intera struttura aziendale.

POSTA ELETTRONICA

L'Azienda gestisce gli account di posta elettronica, ovvero le caselle di posta elettronica come ***account nominativi*** composti da "nome e cognome" accompagnati dal dominio aziendale: *nome.cognome@ospedalideicolli.it*. L'accesso alle suddette caselle di posta elettronica avviene attraverso il criterio di autenticazione a doppio fattore che consiste nella richiesta di un ulteriore elemento di verifica oltre alla normale password. Per impostazione predefinita questo elemento aggiuntivo di verifica, ossia fattore di autenticazione di secondo livello, può consistere, a scelta dell'operatore:

- in un codice (OTP) da ricevere via SMS sul proprio smatphone da digitare dopo la password all'atto dell'accesso alla casella di posta;
- nell'approvare una notifica ricevuta tramite l'app Microsoft Authenticator installata sul proprio smartphone o in un codice di verifica generato da tale app da immettere dopo la password.

Gli account di posta elettronica come sopra definiti sono a tutti gli effetti **"dati personali"** (ex art 4 del GDPR) per cui L'Azienda A.O. Dei Colli, in qualità di Titolare del Trattamento dati, li tratterà per le sole finalità qui illustrate e nella corretta applicazione delle tutele imposte dalla relativa normativa in materia (Reg. UE 2016/679 e Codice Privacy così come modificato dal D.Lgs. 101/2018), nonché nel rispetto del diritto alla riservatezza del lavoratore (artt. 2, 3, 4, 7 e 8 dello Statuto dei Lavoratori, L. 300/70).

A tal proposito si ritiene opportuno, come indicato nel succitato regolamento, ribadire al lavoratore che **l'utilizzo *dell'account* nominativo deve avvenire per soli fini aziendali**, vietandone l'utilizzo privato e pertanto risulta opportuno specificare nei messaggi di posta elettronica la *natura non personale*

dei messaggi stessi. È bene, infatti, tenere presente che un uso promiscuo, o non disciplinato, *dell'account* genera, senza dubbio, dati personali del tutto estranei al contratto di lavoro instaurato dalle parti e pertanto esclusi dal presente contesto (i dati contenuti nelle caselle di posta elettronica – che possono essere strettamente personali, particolari o relativi a questioni riservate del lavoratore – inevitabilmente saranno salvati su server della società, su backup ecc.).

Come richiamato dal Garante nelle **"Linee guida per posta elettronica e internet del 10 marzo 2007"**, il contenuto dei messaggi di posta elettronica, compresi i cosiddetti dati "esteriori" e i "file allegati", sono forme di corrispondenza assistite da garanzie di segretezza tutelate a più livelli: costituzionale, legislativo, anche penale, regolamentare, etc. (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.).

Gestione account di posta in caso di interruzione temporanea del rapporto di lavoro

Pertanto, con specifico riferimento all´impiego della posta elettronica nel contesto lavorativo e in ragione della veste "esteriore" attribuita all´indirizzo di posta elettronica, l'Azienda, nell'ottica di ottemperare ai principi di liceità, riservatezza, pertinenza e non eccedenza del trattamento dei dati dei lavoratori e nel contempo assicurarsi che gli stessi, in qualità di destinatari o mittenti, utilizzino la posta elettronica operando quale espressione dell´organizzazione datoriale e non ne facciano un uso personale, ma soprattutto per potere accedere al fine di una continuità aziendale ai contenuti dell'account in assenza del lavoratore, adotterà gli accorgimenti di seguito illustrati:

- a ciascun lavoratore, tramite apposite funzionalità di sistema, sarà offerta la possibilità di inviare automaticamente, in caso di assenze, anche improvvisa, (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti i riferimenti di contatto (elettronici o telefonici) di un altro soggetto o altre utili modalità di contatto della struttura[1];
- in caso di eventuali assenze non programmate (ad esempio per malattia), qualora il lavoratore non possa attivare la funzionalità suddetta (anche avvalendosi di servizi webmail) e perdurando l´assenza oltre un determinato limite temporale, l'Azienda potrà disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l´amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l´attivazione di un analogo accorgimento di cui al punto precedente, avvertendo gli interessati;
- qualora in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all´attività lavorativa, l'Azienda debba conoscere il contenuto dei messaggi di posta elettronica, l´interessato potrà delegare, mediante apposito modulo, un altro lavoratore (fiduciario) che provvederà a verificare il contenuto di messaggi ricevuti inviando al Responsabile dell'Unità di appartenenza solo quelli ritenuti rilevanti per lo svolgimento dell´attività lavorativa[2].
- Nel caso fossero attivate caselle di posta elettronica condivise (c.d. "impersonali" come ad esempio denominazione U.O@ospedalideicolli.it) utilizzate contemporaneamente da più unità di personale afferente alla struttura titolare della casella di posta, queste andranno gestite con una particolare procedura che consentirà di avere una specifica profilazione per ogni utente autorizzato e contestualmente a ciascuno di essi di monitorare e inviare mail dalla cassetta condivisa. Quando un utente del gruppo risponde a un messaggio inviato alla cassetta postale condivisa, il messaggio di risposta figurerà inviato dalla cassetta postale condivisa, non dal singolo utente[3].

[1] **Funzionalità "Risposte automatiche"** attivabile dalla sezione *"Impostazioni > Visualizza tutte le impostazioni di outlook"*.
[2] **Funzionalità "Gruppi"** attivabile dalla sezione *"Impostazioni > Visualizza tutte le impostazioni di outlook"*, previa inserimento dell'account di posta da associare in apposito gruppo dell'ulteriore destinatario (fiduciario, Responsabile ICT/Responsabile UOC/UOSD).
[3] **Cassetta postale condivisa (c.d impersonale)** le cassette di posta condivise vengono usate quando più dipendenti/collaboratori devono accedere alla stessa email aziendale. Sono attivabili, a seguito di Profilazione utenze ad opera della UOC SIA , dalla sezione outlook cartella>Aggiungi cartella condivisa> inserire indirizzo della cassetta postale condivisa di cui si è membri.

Gestione account di posta in caso di cessazione del rapporto di lavoro

In conformità ai principi in materia di protezione dei dati personali, dopo la cessazione del rapporto di lavoro il datore di lavoro, provvederà a rimuovere gli account di posta elettronica aziendali riconducibili a persone identificate o identificabili, nei tempi e nei modi di seguito illustrati:

- la disattivazione degli account sarà preceduta dalla adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi, attraverso un meccanismo di reindirizzo delle mail in arrivo, indirizzi alternativi riferiti all'attività professionale del titolare della casella (ad esempio l'indirizzo del responsabile della funzione di Information Technology o del Responsabile della UOC/UOSD di appartenenza)[1]-[2];
- le misure tecnologiche ed organizzative adottate consentiranno di contemperare l'interesse del titolare ad accedere alle informazioni necessarie all'efficiente gestione della propria attività e a garantirne la continuità con la legittima aspettativa di riservatezza sulla corrispondenza da parte di dipendenti/collaboratori nonché dei terzi;
- gli account nominativi di posta elettronica verranno disattivati nei termini minimi richiesti per la predisposizione di quanto sopra e non oltre sei mesi dalla data di cessazione del rapporto di lavoro;
- nel caso di prevista cessazione del rapporto di lavoro, il dipendente potrà comunicare ai clienti dell'azienda i riferimenti aziendali del nuovo account di posta (se predisposto) dove inviare nel prosieguo la posta di competenza;
- il datore di lavoro assicura di "aprire e leggere solo le mail provenienti dalla propria clientela, non anche mail personali" indirizzate al dipendente in cessazione di rapporto.

Nel caso la risoluzione contrattuale fra lavoratore e datore di lavoro avvenga in tronco (dimissioni o licenziamento per giusta causa) per cui risulta impossibile organizzare alcun passaggio di consegne, al fine di assicurare la necessaria continuità aziendale del lavoro sino a tale momento svolto dall'ex dipendente, il datore di lavoro **manterrà attivo il precedente account per un periodo limitato** e provvederà, in linea con quanto suggerito dal Garante, a **disattivare l'account nominativo aziendale con le modalità e i tempi sopra indicati.**

In tale ipotesi, e in ogni altro caso di necessità di continuità aziendale a seguito di interruzione o sospensione del rapporto di lavoro, la casella di posta dell'utente, con i relativi device/fattori di autenticazione, potrebbe subire modifiche sostanziali fino alla disattivazione di tutti i metodi di autenticazione ad essa collegati. Ovviamente la conseguente disattivazione della casella di posta comporterà la rimozione immediata di tutti i device ad essa associati utilizzati per la Multi-Factor Authentication (autenticazione a più fattori).

INTERNET

La navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento dell'attività lavorativa del dipendente e pertanto, è assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. Va ribadito, inoltre, che la navigazione in internet debba avvenire nel pieno rispetto di quanto previsto nell'apposito regolamento aziendale di cui in premessa.

Pertanto l'utente non potrà utilizzare internet per:

- l'upload o il download di software, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità

dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale dell'UOCSIA);

- ogni forma di registrazione e accesso a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche (è un'utilità interattiva che permette ai visitatori di un sito web di poter lasciare firme e commenti) anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile del Servizio.

Inoltre, nell'ottica di migliorare la sicurezza informatica, e tenuto conto delle disposizioni impartite dal Ministero per la pubblica Amministrazione e l'Innovazione Tecnologica, dall'Autorty per l'informatica e dagli atri organismi del settore, l'Azienda si dota di appositi strumenti hardware e software (firewall, antivirus, VulnerabiltyAssesment) opportunamente predisposti e configurati per impedire accessi non autorizzati alla rete aziendale (haker, spoofing, sniffing, hijacking) e attacchi di tipo virale o malware (worm, syware, trojan, dialer, ramsonware,, backdoor, etc.).

Il titolare effettua eventuali controlli sul traffico internet esclusivamente in linea con le modalità indicate dal Garante nelle **"Linee per posta elettronica e internet del 10 marzo 2007"**, ovvero:

- individuando categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
- configurando i sistemi e l´utilizzo di filtri in modo che prevengano determinate operazioni;
- effettuando il trattamento di dati in forma anonima o tale da precludere l´immediata identificazione degli utenti mediante opportune aggregazioni;
- conservando, eventualmente, di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza.

Nello specifico, sempre nell'ottica di migliorare la sicurezza informatica ed in osservanza dei principi dettati dal D.Lgs. 14 settembre 2015 n. 151, che modifica l'art. 4 della legge 300/1970, e nel rispetto di quanto disposto dal Regolamento UE 679/2016 e dal D. Lgs. 196/2003 e ss.mm.ii., l'Azienda, in relazione agli strumenti utilizzati dal lavoratore per rendere le prestazioni lavorative, può disporre, sempreché non prolungati e previa adeguata informativa fornita al lavoratore, eventuali controlli senza necessità di accordi sindacali preventivi, compiuti dal personale incaricato della UOC SIA, mirati alla verifica di eventuali violazioni alle predette disposizioni. Tali interventi potranno avvenire mediante un sistema di controllo dei contenuti (Web Filtering) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati per il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

CONSERVAZIONE DEI DATI

La conservazione dei dati personali relativi agli accessi ad Internet o al traffico di posta elettronica, registrati nei file log, avviene con le modalità e i tempi indicati nelle **"Linee Guida per la Gestione e Conservazione dei Log"** dell'Azienda.
Il Titolare potrà predisporre un eventuale prolungamento dei tempi di conservazione in via del tutto eccezionale in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all´indispensabilità del dato rispetto all´esercizio o alla difesa di un diritto in sede giudiziaria;
- 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 (tenendo conto, con riguardo ai dati sensibili, delle

prescrizioni contenute nelle autorizzazioni generali nn. 1/2005e 5/2005 adottate dal Garante) sarà limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate e sarà effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

NAPOLI, MAGGIO 2023

IL TITOLARE DEL TRATTAMENTO