SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Modena

INFORMATIVA
AI SENSI DELL'ART. 13 DEL REGOLAMENTO (UE) 2016/679
RELATIVA AI CONTROLLI SUL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI

L'Azienda Ospedaliero-Universitaria di Modena (AOU), in qualità di datore di lavoro, con questo documento, informa dipendenti e collaboratori, sui controlli che effettua per verificare il rispetto delle norme stabilite per il corretto utilizzo, per fini esclusivamente lavorativi, dei servizi informatici aziendali (posta elettronica, Rete internet, telefonia e computer aziendali).
Maggiori informazioni in merito sono contenute nel "Disciplinare per l'utilizzo delle postazioni di lavoro dell'Azienda Ospedaliero-Universitaria di Modena", che tutti i lavoratori sono tenuti ad osservare e reperibile nell' Intranet aziendale e sul sito istituzionale nella sezione: https://www.aou.mo.it/privacy_dipendenti_responsabili_esterni

L'Azienda delega al Servizio Tecnologie dell'Informazione (STI) i controlli tecnici sui sistemi informatici.

Attività di controllo - principi generali

Le attività di controllo e vigilanza da parte dell'Azienda sono fondate sul principio della "proporzionalità" che si concretizza nella pertinenza e non eccedenza del controllo stesso; pertanto, i mezzi e l'ampiezza del controllo sono proporzionati agli scopi che, nello specifico, sono quelli di garantire la sicurezza del sistema informatico e l'appropriato utilizzo delle risorse.
L'Azienda garantisce che i dati informatizzati da essa gestiti, nonché i sistemi di elaborazione dati e gli strumenti di telecomunicazione non saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114, 171 Codice Privacy; artt. 4 e 8, L. 20 maggio 1970, n.300 – Statuto dei Lavoratori), se non nei limiti consentiti dallo Statuto dei Lavoratori, così come modificato dal D. Lgs. 151/2015 [Jobs Act] e comunque previa informativa ai dipendenti interessati.

Accesso alla casella di posta elettronica per ragioni di sicurezza o manutenzione

Quando motivi di sicurezza o di manutenzione lo richiedano, l'Azienda, previo avviso agli utenti interessati, può accedere alla configurazione delle caselle di posta elettronica per esclusive finalità tecniche. L'accesso alla configurazione di posta non comporta la visualizzazione dei messaggi della casella, salvo il caso eccezionale in cui il problema di sicurezza o di manutenzione non possa essere diversamente risolto. In quest'ultimo caso, l'utilizzatore interessato sarà informato prima dell'accesso. L'attività effettivamente eseguita sulle configurazioni (o sui messaggi di posta in caso eccezionale) viene sempre comunicata all'utente interessato al termine dell'intervento.

Rilevazione della posta elettronica

L'Azienda non conserva alcun log relativo al contenuto delle e-mail inviate e ricevute dagli utenti con il servizio di posta elettronica aziendale. L'unico log generato dal sistema è di tipo diagnostico con la finalità di individuare eventuali problemi in invio e ricezione della posta e la sua conservazione è limitata nel tempo a 28 giorni.

Il sistema di posta elettronica tiene traccia di tutte le e-mail inviate e ricevute, conservando nei log:

- identificativo della stazione di lavoro che ha inviato il messaggio
- data e ora
- indirizzo di posta del mittente
- indirizzo del destinatario

Questo log non è oggetto di operazioni di backup.

Rilevazione degli accessi a Internet

Tutti gli accessi a Internet possono essere memorizzati per finalità di sicurezza del sistema in appositi file di log. I log non sono accessibili per la consultazione, non sono oggetto di operazioni di backup e tengono traccia dei seguenti dati per ogni accesso:

- data e ora dell'accesso
- nome del sito richiamato per la consultazione
- esito della consultazione
- tipologia di operazione richiesta e informazioni sugli eventuali file scaricati
- numero di byte trasferiti dall'elaboratore remoto e viceversa

Tali log sono indispensabili all'Azienda per poter costantemente monitorare il corretto funzionamento del sistema nella sua globalità e per poter effettuare statistiche periodiche sull'uso del sistema; entrambe le attività si svolgono su dati anonimi. I log sono trattati e conservati per un massimo di sette giorni, dopodiché sono distrutti a cura dello STI.

Qualora si rilevino le seguenti anomalie:

- traffico superiore del 20% rispetto alla media dell'ultimo semestre;
- utilizzo di porte e/o protocolli non utilizzati dai programmi aziendali;
- contemporanea presenza di sessioni parallele dirette al medesimo sito remoto;
- traffico dati diretto a siti presenti nella black-list

l'Azienda emetterà un avviso generalizzato che informa della sospensione - per un periodo limitato e indicato nell'avviso stesso - dei controlli anonimi e del fatto che i log di sistema verranno utilizzati per l'individuazione di tali anomalie. Durante questo periodo, in aggiunta alle informazioni enunciate in precedenza, verrà rilevato anche l'indirizzo IP di partenza della navigazione. Al termine del periodo di osservazione questi log saranno distrutti a cura dello STI.
I log potranno essere oggetto di provvedimenti da parte dell'Autorità Giudiziaria e Amministrativa e in generale dei soggetti aventi funzioni ispettive e di controllo.

Telefonia

Per fini di controllo della spesa telefonica l'Azienda tiene traccia, attraverso i servizi del provider telefonico, delle telefonate effettuate, se queste costituiscono un onere economico per l'Azienda; vengono altresì tracciate le telefonate in ingresso in quanto può essere richiesto da servizi aziendali l'avvenuta ricezione o meno di una chiamata ad un determinato numero interno. In particolare viene registrato:

- il numero del chiamante
- il numero chiamato
- data e ora di inizio della telefonata e data e ora di fine della stessa

Tutti i log sopra citati vengono conservati dall'Azienda per un anno solare in maniera disaggregata per poter confrontare gli andamenti di costo con i dati aggregati degli anni precedenti. I dati disaggregati dal primo gennaio al trentuno dicembre di ciascun anno potranno essere tenuti fino alla fine di marzo dell'anno successivo per i controlli istituzionali; qualora i dati evidenzino anomalie tali da giustificare controlli aggiuntivi, potranno essere ulteriormente approfonditi secondo una gradualità nei controlli che preveda prima il controllo del dato aggregato e la notifica di eventuali anomalie e solo successivamente, qualora il problema persista, un controllo sui dati disaggregati. Qualora l'integrità del sistema tecnologico dell'Azienda o la gravità del fatto lo rendano necessario sarà possibile accedere immediatamente al dato disaggregato; qualora possibile, gli approfondimenti sui dati che si rendessero necessari saranno condotti con verifiche a campione.

In generale tutte le verifiche dovranno rispettare i criteri della pertinenza e non eccedenza rispetto al fine di controllo amministrativo proprio dell'Azienda; qualora le verifiche portino all'accertamento della violazione delle presenti regole o più in generale all'accertamento di utilizzi impropri, l'Azienda si riserva di adottare le opportune misure disciplinari e amministrative.

Rilevazione a fini diagnostici delle attività informatiche e telefoniche

L'Azienda non effettua verifiche che possano configurare il controllo a distanza dell'attività dei lavoratori, quali:

- lettura e registrazione sistematica dei messaggi di posta elettronica o dei relativi dati esteriori, fatto salvo quanto tecnicamente necessario per svolgere il servizio e-mail;
- riproduzione o eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- lettura o registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- analisi occulta di eventuali computer o dispositivi portatili affidati in uso;

Tuttavia, qualora concrete ragioni portino a ritenere che la sicurezza del sistema tecnologico aziendale possa essere minacciata, l'Azienda può effettuare controlli sul corretto utilizzo delle attrezzature informatiche aziendali e sul funzionamento del sistema informatico e di telefonia.
In tali casi l'Azienda, nel rispetto dei principi di liceità, correttezza e trasparenza di cui all'art. 5 del GDPR e del disposto dell'art. 4 della L. 300/1970 (c.d. Statuto dei Lavoratori) procede ai controlli, con esclusione della possibilità del controllo informatico all'insaputa dei lavoratori e in ottemperanza ad un criterio di graduazione, secondo il quale:

- in via preliminare saranno eseguiti controlli su dati aggregati e anonimi, riferiti all'intera struttura lavorativa. In assenza di anomalie non si effettueranno controlli ulteriori.
- nel caso siano rilevate anomalie, sarà diramato un avviso generalizzato. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
- qualora si rilevasse il perdurare delle anomalie, si procederà a controlli su base individuale.
- nel caso di abusi singoli o reiterati si procederà all'invio di avvisi individuali e, in seguito, saranno eseguiti controlli nominativi.

Il riscontrato o reiterato uso non conforme delle risorse informatiche e di telefonia, evidenziatosi secondo la procedura sopra indicata, qualificandosi come violazione degli obblighi del dipendente, comporta l'adozione da parte della Azienda delle opportune misure disciplinari, anche con accesso ai dati di dettaglio necessari per il completamento dell'istruttoria. È esclusa in ogni caso l'ammissibilità di controlli prolungati, costanti o indiscriminati.

Esercizio dei diritti

In qualsiasi momento ciascun dipendente/collaboratore può esercitare il diritto di richiedere l'accesso ai propri dati personali, l'aggiornamento, la rettifica di dati inesatti, la cancellazione e l'integrazione di dati incompleti. Inoltre, nelle ipotesi e per i motivi stabiliti dalla legge, può richiedere la limitazione del trattamento dei suoi dati e può esercitare il diritto di opposizione al trattamento. A tal fine apposita istanza dovrà essere presentata alla Azienda contattando il Responsabile della protezione dati, scrivendo all'indirizzo: dpo@aou.mo.it

Ricorrendone i presupposti, ciascun dipendente/collaboratore ha altresì il diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali, secondo le procedure previste.

Il Titolare del trattamento è l'Azienda Ospedaliero-Universitaria di Modena (AOU), con sede a Modena (MO), in Via del Pozzo, n. 71, PEC: affarigenerali@pec.aou.mo.it ; Sito internet: www.aou.mo.it