Alla cortese attenzione delle UUOO

Affari Generali e Legali

Sviluppo e Gestione Risorse Umane

Information & Communication Technologies (ICT)

dell'Ospedale Policlinico San MArtino

**Oggetto: gestione delle caselle email aziendali e cancellazione dei metadati generati – Autorità Garante per la protezione dei dati personali: provv. 06 giugno 2024.**

Con la presente nota si provvede ad informare l'Ospedale Policlinico San Martino (di seguito anche solo Policlinico), con particolare attenzione alle strutture direttamente coinvolte, circa la situazione in tema di gestione della posta elettronica del lavoratore sulla base di quanto previsto dall'Autorità Garante per la protezione dei dati personali.

Si ricorda, anzitutto, che la gestione della posta elettronica degli operatori aziendali costituisce attività di trattamento dei dati personali e pertanto è assoggettata ai principi fondamentali previsti dal Regolamento UE 679/2016 ("GDPR"), nonché dalla correlata normativa nazionale di cui fanno parte anche specifici provvedimenti dell'Autorità Garante per la protezione dei dati personali.

Con preciso riferimento all'attività di gestione del rapporto lavorativo in ambito pubblico, occorre anzitutto sottolineare, così come specificato nelle *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico* del 14 giugno 2007, alle quali integralmente si rimanda *("Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico")*, che *«il datore di lavoro pubblico può lecitamente trattare dati personali dei lavoratori nella misura in cui ciò sia necessario per la corretta gestione del rapporto di lavoro»*, nonché nel rispetto dei principi dettati dallo Statuto dei Lavoratori, il quale all'art. 4 espressamente prevede un generale divieto di controllo del lavoratore da parte del datore di lavoro, pur con una specifica deroga relativa agli strumenti strettamente necessari a svolgere l'attività lavorativa e all'interno dei quali è possibile ricomprendere anche la posta elettronica.

A tal riguardo, il Garante per la protezione dei dati personali è intervenuto con il Provvedimento del 6 giugno 2024 *("Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati")*, allo scopo di richiamare l'attenzione su taluni punti di intersezione tra la disciplina della protezione dei dati e le norme che stabiliscono le condizioni per l'impiego degli strumenti tecnologici nei luoghi di lavoro.

All'interno del provvedimento – in cui si fa riferimento alternativamente ai *"metadati di posta elettronica"* o *"log di posta elettronica"* – viene specificato che i metadati hanno la caratteristica di essere registrati automaticamente dai sistemi di posta elettronica (indipendentemente dalla percezione e dalla volontà dell'utilizzatore) e *"corrispondono tecnicamente alle informazioni registrate nei log generati dai sistemi server*

*di gestione e smistamento della posta elettronica […] e dalle postazioni nell'interazione che avviene tra i diversi server interagenti e, se del caso, tra questi e i client […]".*

Tali informazioni – assistite da garanzie di segretezza, tutelate anche costituzionalmente (artt. 2 e 15 della Costituzione), *"intese ad assicurare protezione al nucleo essenziale della dignità della persona e al pieno sviluppo della sua personalità nelle formazioni sociali"* – possono comprendere gli indirizzi email del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell'instradamento, gli orari di invio e ricezione, la dimensione del messaggio nonché la presenza e la dimensione di eventuali allegati e, in certi casi, anche l'oggetto del messaggio.

Le indicazioni del Garante non riguardano il contenuto dei messaggi di posta elettronica né le informazioni tecniche che ne fanno parte integrante, che rimangono nell'esclusivo controllo dell'utente (mittente o destinatario dei messaggi).

Al fine del migliore adeguamento rispetto ai principi stabiliti dal Garante si rimanda integralmente al suddetto documento, provvedendosi tuttavia a richiamarne i passaggi fondamentali, per cui:

- per consentire il corretto funzionamento e il regolare utilizzo del sistema di posta elettronica, comprese le essenziali garanzie di sicurezza informatica, senza necessità di attivare le garanzie procedurali del comma 1 dell'art. 4 dello Statuto dei Lavoratori (accordo sindacale o autorizzazione dell'Ispettorato Nazionale del Lavoro), l'Autorità ritiene che la raccolta e la conservazione dei metadati/log necessari ad assicurare il funzionamento delle infrastrutture del sistema di posta elettronica possa essere effettuata, di norma, per un periodo di pochi giorni, non superiore – a titolo orientativo – a 21 giorni;
- per la suddetta finalità,
    - l'estensione del tempo di conservazione potrà avvenire solo in presenza di particolari condizioni che la rendano necessaria, comprovando opportunamente – in applicazione del principio di accountability – le specificità della realtà tecnica e organizzativa del titolare;
    - spetta, in ogni caso, al titolare l'adozione di tutte le misure tecniche e organizzative per assicurare:
        - il rispetto del principio di limitazione della finalità del trattamento dei metadati;
        - l'accessibilità selettiva da parte dei soli soggetti autorizzati e adeguatamente istruiti;
        - la tracciatura degli accessi effettuati;

- diversamente, la generalizzata raccolta e la conservazione dei log di posta elettronica per un lasso di tempo più esteso richiede la sottoscrizione di un accordo sindacale o l'autorizzazione dell'Ispettorato Nazionale del Lavoro, poiché dalle suddette attività può derivare un indiretto controllo a distanza dell'attività dei lavoratori;
- i tempi di conservazione dei metadati devono essere, comunque, proporzionati rispetto alle legittime finalità perseguite: finalità connesse alla sicurezza informatica e alla tutela del patrimonio informatico giustificano la conservazione dei metadati per un arco temporale congruo rispetto all'obiettivo di rilevare e mitigare eventuali incidenti di sicurezza, adottando tempestivamente le opportune contromisure;

- ad ogni buon conto, il titolare è tenuto a:
    - informare adeguatamente i lavoratori, rendendoli consapevoli sulle caratteristiche complessive del trattamento dei dati personali relativi alle comunicazioni elettroniche che li riguardano;

- redigere una valutazione di impatto sulla protezione dei dati, stante la particolare "vulnerabilità" degli interessati nel contesto lavorativo, nonché il rischio di "monitoraggio sistematico", inteso come "trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti";
- adottare misure volte ad assicurare il rispetto dei principi della protezione dei dati fin dalla progettazione del trattamento e per impostazione predefinita durante il ciclo di vita dei dati;
- verificare la conformità alla normativa in materia di protezione dei dati di programmi o servizi di gestione della posta elettronica realizzati da terzi, impartendo le necessarie istruzioni al fornitore del servizio.

Tenendo presente che anche i fornitori devono contribuire – già dalla fase di progettazione e sviluppo di applicazioni, servizi e prodotti basati sul trattamento di dati personali – a far sì che i titolari del trattamento possano adempiere ai loro obblighi di protezione dei dati, è necessario che il Policlinco, per il tramite dei soggetti preposti allo scopo, verifichi con la dovuta diligenza che i programmi e servizi informatici di gestione della posta elettronica in uso ai dipendenti – specialmente nel caso di prodotti di mercato in modalità cloud o as-a-service – possano consentire al datore di lavoro di modificare le impostazioni di base, impedendo la raccolta dei predetti metadati o limitando il periodo di conservazione secondo le indicazioni del Garante e chiedendo al fornitore di cancellare o anonimizzare i metadati raccolti nei casi in cui non si intenda rendere la loro conservazione maggiormente estesa.

Cordiali Saluti

Il DPO

Avv. Isabella Lucati