

AREE DIRIGENZA SANITA' E DIRIGENZA FUNZIONI LOCALI

Verbale di intesa in merito all' accordo ex articolo 4, comma 1, della Legge 300/1970 (Statuto dei lavoratori) in materia di trattamento dei metadati della posta elettronica e dei log di navigazione in Internet e relativi tempi di conservazione

Il giorno 22/10/2025 ha avuto luogo l'incontro tra le delegazioni trattanti dell' Aziende USL di Modena e le Organizzazioni Sindacali delle presenti Aree negoziali, nelle persone di:

AZIENDA USL MODENA	
Ferrari Stefania	
Altariva Daniela	
Ciancia Giulia	
Cassanelli Manuela	

OO.SS. AREA DIRIGENZA SANITA'		OO.SS. AREA DIRIGENZA FUNZIONI LOCALI	
ANAAO ASSOMED		FP CGIL	
CIMO		CISL FP	
FASSID		UIL FPL	
AAROI EMAC		FEDIR SANITÀ	
FP CGIL		DIREL	
FVM		DIRER - SIDIRSS	
FESMED		UNSCP	
CISL FP			
UIL FPL			

Al termine dell'incontro le parti sottoscrivono l'allegato verbale di intesa che viene definito come segue.

Modena lì 22/10/2025

Il percorso di sottoscrizione si è concluso definitivamente, per l'Area Dirigenza Sanità il 11 Novembre 2025

Il percorso di sottoscrizione si è concluso definitivamente, per l'Area Dirigenza PTA il 11 Novembre 2025

Verbale di intesa in merito all'accordo ex articolo 4, comma 1, della Legge 300/1970 (Statuto dei lavoratori) in materia di trattamento dei metadati della posta elettronica e dei log di navigazione in internet e relativi tempi di conservazione

Il giorno 22 Ottobre 2025 alle ore 14:30, ha avuto luogo l'incontro congiunto tra la delegazione di parte datoriale della Azienda USL di Modena e le delegazioni sindacali dell'Area Dirigenza Sanità e dell'Area Dirigenza delle Funzioni Locali (nel seguito "le Parti")

Premesso che:

- l'art. 4, comma 1, L. 20 maggio 1970, n. 300, come modificato dal d.lgs. 14 settembre 2015, n. 151, individua le finalità di impiego degli strumenti audiovisivi e di altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, stabilendo precise garanzie procedurali (accordo sindacale o autorizzazione pubblica);
- le suddette misure non si applicano "agli strumenti di registrazione degli accessi e delle presenze", così come "agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (art. 4, comma 2, l. n. 300/1970), in quanto funzionali a consentire l'assolvimento degli obblighi che discendono direttamente dal contratto di lavoro, vale a dire la presenza in servizio e l'esecuzione della prestazione lavorativa;
- l'Azienda USL di Modena (nel seguito anche "Ausl di Modena") ha l'onere di bilanciare il legittimo diritto alla riservatezza dei dipendenti con la necessità di proteggere i dati aziendali critici da accessi non autorizzati, abusi o violazioni, monitorando le attività al fine di individuare comportamenti anomali, prevenire minacce interne ed esterne migliorare la gestione degli incidenti di sicurezza;
- ciò avviene attraverso l'adozione di misure di controllo tecnico che si estendono anche ad alcuni sistemi informatici utilizzati dai lavoratori e che si rendono necessarie, tra l'altro, per adempiere agli obblighi previsti dalla Direttiva (UE) 2022/2555 (c.d. NIS2), recepita in Italia con D. Lgs. 82/2024, concernente la Cybersecurity delle reti e dei sistemi informativi delle imprese rientranti tra gli enti definiti "essenziali" o "importanti";
- il Garante per la protezione dei dati personali (nel seguito "Garante Privacy") ha chiarito che i programmi e i servizi informatici, anche di posta elettronica, commercializzati da fornitori in modalità Cloud possano raccogliere, per impostazione predefinita e indipendentemente dalla volontà dell'utilizzatore, i c.d. "metadati" (detti anche "log di posta elettronica"), da cui è possibile acquisire informazioni riferite alla sfera personale dell'interessato;
- il Garante Privacy, con il provvedimento n. 364 del 06 giugno 2024, ha aggiornato l'atto di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", al fine di fornire ai datori di lavoro indicazioni sul trattamento dei metadati, anche con riferimento all'eventuale periodo di conservazione degli stessi, e ha statuito che la conservazione dei metadati per un periodo di tempo superiore a 21 giorni rende opportuno attivare le garanzie del comma 1 dell'art. 4 dello Statuto dei Lavoratori, in quanto rispondente ad esigenze riconducibili alla sicurezza e alla tutela del patrimonio anche informativo del datore di lavoro e non solamente a finalità strettamente funzionali all'attività lavorativa (che rientrerebbero nella applicazione del comma 2 del medesimo art. 4 dello Statuto dei Lavoratori);
- il Garante Privacy ha inoltre chiarito che anche la raccolta e la successiva conservazione dei log di navigazione in internet da parte dei dipendenti comportano la possibilità di ricostruirne l'attività e di acquisire informazioni riguardanti la loro sfera personale e pertanto

anche i trattamenti di tali dati, effettuati dalla Ausl di Modena per finalità di sicurezza della rete, richiedono il rispetto delle garanzie del suddetto comma 1 dell'art. 4 dello Statuto dei Lavoratori;

- ai fini dello svolgimento delle attività di monitoraggio finalizzato a garantire la sicurezza delle informazioni, la conformità normativa e la tutela del proprio patrimonio anche informativo, l'Ausl di Modena ha la necessità di conservare i metadati di posta elettronica e di navigazione in internet per un lasso di tempo più esteso di 21 giorni

Considerato inoltre che:

- la Ausl di Modena:
 - mette a disposizione sistemi e strumenti informatici quali PC portatili e smartphone aziendali e piattaforme on Premises e Cloud in cui sono presenti applicativi di lavoro utilizzati dall'utente nell'ambito della sua prestazione lavorativa quali, a titolo esemplificativo e non esaustivo: Microsoft Office (Word, Excel, PowerPoint), applicativi di autenticazione informatica necessari per l'accesso in sicurezza alla rete aziendale stessa attraverso credenziali personali, Sistemi di Posta elettronica, ecc.;
 - utilizza i log delle attività svolte su taluni applicativi per esigenze organizzative e di sicurezza derivanti, in particolare, dall'espletamento da parte della Ausl stessa di servizi in tema di cybersecurity per la disamina di comportamenti malevoli e l'analisi e la correlazione di eventi anche occorsi mesi prima;
 - ha individuato, attraverso appositi contratti di assistenza, i soggetti esterni (fornitori) che possono gestire e mantenere le piattaforme tecnologiche aziendali, ivi compresi i log generati da queste ultime designando tali soggetti come "Responsabili del trattamento" ai sensi dell'art. 28 GDPR;
 - si impegna ad effettuare una valutazione dell'impatto sulla protezione dei dati personali (DPIA ex art. 35 GDPR), riguardante il trattamento dei log di posta elettronica e dei log di navigazione in internet, ai fini dell'osservanza e della corretta attuazione degli obblighi e delle prescrizioni derivanti dalla normativa in materia di Data Protection e Cybersecurity.

Tutto quanto sopra premesso e considerato, ravvisata l'opportunità di operare in modo che i tempi di conservazione dei dati siano resi evidenti ai lavoratori e proporzionati alle legittime finalità perseguite, al fine di bilanciare le esigenze di sicurezza aziendale con la tutela dei diritti dei lavoratori stessi, le Parti convengono quanto segue:

- 1) Le premesse formano parte integrante e sostanziale della presente intesa.
- 2) Le Parti concordano che:
 - Per la tutela del patrimonio e della rete aziendale, sono conservati:
 - per un massimo di 90 giorni solari i log (metadati) del sistema di posta elettronica;
 - per un massimo di 90 giorni solari i log di navigazione in internet (web filtering)

I dati di cui sopra, oggetto della presente intesa, sono trattati esclusivamente per:

- garantire la sicurezza informatica e la continuità operativa dei sistemi aziendali;
- tutelare il patrimonio informativo, tecnologico e produttivo della Ausl di Modena da accessi non autorizzati, perdite o attacchi informatici;
- assicurare il corretto svolgimento delle attività di gestione dei sistemi;
- assicurare la continuità operativa dei servizi;

- assicurare le attività di prevenzione, contrasto e recupero, a fronte di incidenti relativi alla sicurezza ICT o di violazioni dei dati personali (Data Breach);
- assicurare il rispetto delle prescrizioni di legge legate alle tematiche di Cybersecurity per le organizzazioni che rientrano nel perimetro di cui alla Legge 90/2024 e di quanto specificato dalla Direttiva (UE) 2022/2555 (c.d. NIS2), recepita in Italia con D. Lgs. 82/2024 e, in particolare, assicurare la raccolta, la generazione e la conservazione sicura e possibilmente centralizzata dei registri di log, in conformità con la determina 164179 del 14 aprile 2025 ACN, per il monitoraggio continuo degli eventi di sicurezza, inclusi gli accessi da remoto e quelli con privilegi amministrativi;
- effettuare una disanima degli eventi dannosi e comportamenti malevoli che possono richiedere l'analisi e la correlazione di eventi antecedenti anche di alcuni mesi, allo scopo di migliorare le attività di verifica e tutelare il perimetro di sicurezza.

Resta esclusa ogni altra finalità, diretta o indiretta, di controllo a distanza dell'attività lavorativa dei dipendenti, fatti salvi i casi di eventuali richieste e/o provvedimenti da parte dell'Autorità Giudiziaria e/o interventi di tutela del perimetro di sicurezza conseguenti.

- 3) La raccolta dei dati è effettuata nel rispetto del principio di pertinenza e non eccedenza, il trattamento dei dati avviene secondo correttezza e per scopi determinati, espliciti e legittimi; inoltre, le disposizioni contenute nella presente intesa, così come le modalità di raccolta e utilizzo dei dati sono indicate nella relativa informativa diffusa ai lavoratori e agli ulteriori interessati al fine di garantire il corretto e trasparente utilizzo dei dati stessi.
- 4) Come disposto dall'art. 4, comma 3 della L. 300/1970 e come indicato dal Garante Privacy i metadati dei sistemi di posta elettronica e di navigazione in internet sono utilizzabili per le finalità connesse alla gestione del rapporto di lavoro nel rispetto delle condizioni e dei limiti previsti dal richiamato comma 1 dell'art. 4 della L. 300/1970 e dunque non potranno costituire supporto all'accertamento dell'obbligo di diligenza del lavoratore, ivi comprese finalità di contestazione disciplinare in tale ambito.
- 5) Con la sottoscrizione del presente Accordo, le Parti si danno reciprocamente atto del pieno rispetto da parte datoriale di quanto previsto dall'art. 4 della Legge n. 300/1970 e dalla vigente disciplina normativa in materia di protezione dei dati personali e tutela di riservatezza e dignità dei lavoratori.

Letto, confermato e sottoscritto.

Modena, li 22/10/2025