CONSIGLIO
REGIONALE
DEL LAZIO

ACCORDO DI CONTRATTAZIONE DECENTRATA INTEGRATIVA CONCERNENTE LA DISCIPLINA IN MATERIA DI METADATI/LOG RELATIVI ALL'UTILIZZO DI POSTA ELETTRONICA, NAVIGAZIONE INTERNET, ALTRI SERVIZI E STRUMENTI ICT NEL CONTESTO LAVORATIVO, AI SENSI DELL'ARTICOLO 4 DELLA LEGGE 300/1970

Vista la legge 20 maggio 1970, n. 300 (Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento) e successive modifiche, di seguito denominato Statuto dei lavoratori, e in particolare l'articolo 4 (Impianti audiovisivi e altri strumenti di controllo);

Visto il regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), di seguito denominato RGPD;

Visto il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla 2 protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE) e successive modifiche, di seguito denominato Codice, e in particolare l'articolo 114 (Garanzie in materia di controllo a distanza), ai sensi del quale resta fermo quanto disposto dall'articolo 4 dello Statuto dei lavoratori;

Visto il decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale) e successive modifiche e in particolare le disposizioni in materia di sicurezza informatica e sull'utilizzo di servizi e strumenti informatici;

Viste le Linee Guida del Garante per la protezione dei dati personali per posta elettronica e internet, adottate con deliberazione n. 13 del 10 marzo 2007, pubblicata sulla G.U. n. 58 del 10 marzo 2007;

Visto il provvedimento del Garante per la protezione dei dati personali n. 364 del 6 giugno 2024 (Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati), che fornisce nuove indicazioni sul trattamento dei metadati della posta elettronica e sui tempi di conservazione, precisando che la raccolta dei metadati per un lasso di tempo più esteso di 21 giorni, anche per finalità di sicurezza informatica e tutela del patrimonio, comporta un controllo a distanza dei lavoratori e richiede l'esperimento delle garanzie previste dal comma 1 dell'articolo 4 dello Statuto dei lavoratori;

Viste le Linee guida per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio pubblicate dall'Agenzia per la cybersicurezza nazionale, le quali prevedono che le politiche di sicurezza adottate per la gestione dei log esistenti, con particolare riguardo all'integrità e alla disponibilità dei log, devono prevedere la loro conservazione in modo sicuro, possibilmente centralizzato, per almeno 24 mesi;

Visto VISTO il decreto del Presidente della Repubblica 16 aprile 2013, n. 62 (Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'art. 54 del D. Lgs. 30 marzo 2001, n. 165) e successive modifiche, e in particolare l'articolo 11 bis che dispone in materia di utilizzo delle tecnologie informatiche, prevedendo, tra l'altro, che l'Amministrazione, attraverso i propri responsabili di struttura, ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati e che le modalità di svolgimento di tali accertamenti sono stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali, ad oggi ancora non adottate;

Dato atto che il Consiglio regionale per il perseguimento delle proprie competenze istituzionali:

- assegna ai dipendenti attrezzature, strumenti informatici e servizi infotelematici e, in particolare, il Consiglio regionale fornisce a tutto il personale almeno un personal computer, un account Microsoft, una casella di posta elettronica aziendale nominativa, l'accesso alla rete intranet e alla rete internet nonché, a seconda delle mansioni svolte dal dipendente, ulteriori strumentazioni e servizi e l'accesso a programmi, servizi e banche dati ICT, in base al ruolo ricoperto nell'organizzazione e necessari per lo svolgimento delle attività assegnate
- gestisce gli strumenti e servizi anche tramite contratti con LazioCrea S.p.A. e altri operatori economici qualificati;
- tali strumenti e servizi telematici generano, anche in via automatica, log tecnici per la funzionalità o log di sicurezza per la salvaguardia dei sistemi informativi;

Dato atto che l'uso degli strumenti e servizi è consentito secondo quanto previsto dalle richiamate disposizioni di legge e del Codice di comportamento. Seppur obbligatorio e indispensabile, espone le attività e il patrimonio informativo dell'Amministrazione a rischi di compromissione e di lesione dei dati personali e del patrimonio informativo dell'Amministrazione stessa, in ragione dei quali è doverosa la messa in campo di azioni e interventi di presidio della cyber sicurezza e della riservatezza;

Dato atto che il Consiglio regionale per:

- garantire il funzionamento e la continuità operativa dei sistemi e dei servizi informatici e di telecomunicazioni;
- verificare la funzionalità del sistema e degli strumenti informatici;
- tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
- evitare che siano reiterati illeciti o per esigenze di carattere difensivo;
- analizzare eventi anche dannosi e rintracciare le cause di tali eventi;

Considerato altresì che, per le suddette finalità e in ragione delle caratteristiche non modificabili degli strumenti e dei servizi infotelematici, l'Amministrazione può conservare i relativi metadati, in

talune ipotesi, per un periodo superiore a 21 giorni e quindi per un tempo superiore a quello indicato dal Garante per la protezione dei dati personali nel sopracitato provvedimento n. 364/2024. Tali log/metadati possono configurarsi come dati personali riguardanti lavoratori, identificati o identificabili,

Tutto ciò premesso, le parti convengono quanto segue:

di approvare, così come previsto dall'allegato A, la disciplina in materia di metadati/log relativi all'utilizzo di posta elettronica, navigazione internet, altri servizi e strumenti ICT nel contesto lavorativo.

Roma, 15 ottobre 2025

Per l'Amministrazione

La Presidente della delegazione di parte pubblica

F.to

La delegazione di parte sindacale

FP CGIL F.to

CISL FP F.to

UIL FPL F.to

CSA RAL F.to

RSU F.to

Allegato A

DISCIPLINA IN MATERIA DI METADATI/LOG RELATIVI ALL'UTILIZZO DI POSTA ELETTRONICA, NAVIGAZIONE INTERNET, ALTRI SERVIZI E STRUMENTI ICT NEL CONTESTO LAVORATIVO

Il Consiglio regionale può dotarsi in ragione delle proprie esigenze organizzative e funzionali, nel rispetto dello Statuto dei lavoratori, di strumenti e servizi, che possono consentire indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e il trattamento di dati personali riferiti o riferibili ai lavoratori mediante sistemi che generano, raccolgono e conservano log. Il Consiglio regionale assicura che mediante i suddetti strumenti e servizi non sono svolti controlli preordinati alla verifica dell'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro (esclusi i sistemi di rilevamento delle presenze) e la correttezza della prestazione lavorativa. Il trattamento dei dati di monitoraggio automatico è svolto solo da soggetti preposti (Amministratori di sistema, autorizzati al trattamento, e dipendenti del fornitore dei servizi, formalmente designati responsabili del trattamento), tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza. È escluso pertanto un controllo diretto del contenuto della posta elettronica da parte degli amministratori di sistema e di altri incaricati del trattamento. Nello svolgimento dei controlli su strumenti e servizi è evitata ogni compressione non giustificata dei diritti e delle libertà fondamentali di lavoratori. L'eventuale controllo verrà svolto nel rispetto dei principi di pertinenza e non eccedenza.

L'utilizzo degli strumenti e delle credenziali ICT fornite sono sotto la diretta responsabilità dell'assegnatario.

La raccolta automatica di metadati e log ha lo scopo principale di assicurare che i sistemi informatici e di telecomunicazioni funzionino in modo efficiente e continuo. Questi dati servono a:

- garantire la sicurezza: Proteggono i sistemi da attacchi e intrusioni;
- tutelare l'integrità: Preservano l'integrità degli strumenti e dei dati;

- prevenire illeciti: Impediscono che le azioni illegali vengano ripetute.

I dati raccolti sono essenziali anche per la gestione di emergenze. Vengono usati per:

- Indagare sugli incidenti di sicurezza: Analizzare le cause e le conseguenze di eventuali violazioni dei dati personali o altri eventi dannosi;
- Migliorare la protezione: Utilizzare le informazioni ottenute per rafforzare la sicurezza del sistema e degli strumenti, a beneficio anche degli utenti;
- Assicurare il rispetto alla normativa sulla cybersicurezza per le organizzazioni che rientrano nel perimetro di cui alla legge 90/2024 e alla direttiva 2022/2555(NIS2).

In linea con le finalità sopra richiamate, sono indicati di seguito i tipi di metadati/log suddivisi per macrocategorie, i tempi massimi di conservazione e le modalità di monitoraggio mediante registrazione di alcuni eventi sui sistemi informatici gestiti dal Consiglio regionale (logging) e di eventuale controllo diretto di eventi anomali. Una volta scaduti i tempi stabiliti, i metadati non possono più essere conservati o utilizzati, a meno che non ci sia un'esplicita richiesta da parte di un'autorità giudiziaria, un contenzioso in corso, un'indagine interna per responsabilità del lavoratore o una specifica normativa che imponga una conservazione più lunga.

1) **Tipi di metadati/log**	**tempi di conservazione**
2) posta elettronica (le operazioni di invio, ricezione e smistamento dei messaggi generano log che possono includere gli indirizzi e-mail del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio, i tempi di invio, ritrasmissione o ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati (non il file allegato) e l'oggetto del messaggio inviato o ricevuto)	Max 90 giorni
3) account Microsoft 365 e analoghi (nome, cognome, e-mail, giorno e ora relative al cambio password, tipologie di componenti software utilizzati dall'utente e	90 giorni

giorno/ora di utilizzo, ip sorgente, area geografica approssimativa dell'utente, informazioni sul dispositivo utilizzato, tipo di autenticazione utilizzata (semplice, MFA, ecc)	
4) Log del Sistema di Identity & Access Management relativamente al Sistema Pubblico di Identità Digitale (SPID), secondo quanto previsto dall'art. 13, comma 2 del DPCM 24 ottobre 2014 recante "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese'	24 mesi
navigazione Internet: ip sorgente, ip destinazione/url, nome utente, data/ora dell'operazione, tipo di dispositivo utilizzato, porte/protocolli utilizzati	max 90 giorni: successivamente i log possono essere mantenuti per max 12 mesi solo previa anonimizzazione in modo che l'utente non sia identificabile. Il trattamento del nome utente e degli altri log di sicurezza è effettuato da diversi soggetti (ciascuno dei quali pertanto accede solo ad alcuni log e non a tutti), a ulteriore garanzia della possibilità di trattamento dell'informazione riferita a un determinato soggetto. Al di fuori dei casi di rilevamento di anomalie nel traffico che potrebbero segnalare potenziali attacchi o particolari punti di debolezza del sistema regionale ovvero di esplicita richiesta del dipendente per ragioni connesse all'utilizzo della rete (es. impossibilità di raggiungere un sito), solamente l'Autorità Giudiziaria può richiedere la corrispondenza tra user anonima e utilizzatore unendo le informazioni in possesso dei Gestori ICT.
log delle segnalazioni ed alert di tutte le tipologie di sistema antimalware: nome macchina, ip sorgente, ip destinazione/url, data/ora dell'operazione, malware rilevato,	6 mesi

azione eseguita (es. rimozione, messa in quarantena)	
log di accesso degli operatori al sistema di rilevazione presenze	6 mesi

L'Amministrazione si impegna a definirne progressivamente la conservazione dei log non oltre 180 giorni solari, fatto salvo il caso degli Amministratori di sistema per i quali i log sono conservati per 365 giorni. Per i metadati che diventano parte di documenti trovano applicazione le norme e i tempi definiti in materia di conservazione dei documenti della pubblica amministrazione.

Raccolta e monitoraggio ed eventuali controlli

Gli strumenti e i servizi informatici sono dotati di sistemi di monitoraggio automatico per garantire la sicurezza e il corretto funzionamento. Questi sistemi bloccano automaticamente le operazioni rischiose e raccolgono log tecnici e metadati. La gestione di questi dati rispetta pienamente le normative sulla privacy.

Il primo livello di sicurezza si basa su filtri preimpostati per ridurre i rischi. Ad esempio:

- Firewall/Web Security Gateway: blocca l'accesso a siti web pericolosi o illeciti;
- Filtri antispam: impediscono che e-mail contenenti virus o minacce arrivino agli utenti.

Questi sistemi generano in automatico degli avvisi di anomalia (ad esempio, download di virus) che possono essere analizzati in un secondo momento dal personale tecnico autorizzato. È importante notare che il controllo automatico si limita ai filtri e non è svolto direttamente da altre figure o enti sui contenuti della posta degli utenti.

Le analisi più dettagliate vengono eseguite solo in caso di anomalie gravi o ripetute che potrebbero compromettere l'integrità dei sistemi, come l'accesso a siti illegali. In caso di anomalia (ad esempio un'infezione da virus) o di segnalazione da parte dell'utente, il personale tecnico può intervenire per:

- bloccare l'accesso alla rete o a specifici servizi per contenere il problema;
- analizzare lo strumento per identificare la causa e pianificare le contromisure;
- imporre il cambio password dell'account dell'utente;

- analizzare i log per individuare accessi non autorizzati.

Queste verifiche possono avvenire su dati aggregati (anonimi) per un'intera area lavorativa. Se necessario, si può emettere un avviso generale per sensibilizzare gli utenti sull'uso corretto degli strumenti.

In linea di massima, i controlli individuali sono eseguiti solo in casi eccezionali e motivati. Se un'analisi individuale si rende necessaria, si cerca di svolgerla, quando possibile, in presenza dell'utente per garantire massima trasparenza e dialogo. L'utente e il suo ufficio sono tenuti a collaborare con i tecnici per risolvere l'incidente il più rapidamente possibile. Se l'utente non è presente e l'intervento è urgente, l'operazione deve essere autorizzata dal dirigente dell'ufficio ICT e dal Responsabile della protezione dei dati.

I log e le verifiche non possono essere usati per il controllo a distanza dell'attività lavorativa dei dipendenti. Qualsiasi uso diverso da quelli previsti è escluso, a meno che non sia richiesto da disposizioni di legge o da un'autorità competente.

In caso di violazioni delle norme interne, gli uffici competenti avvieranno le procedure del caso. Il Consiglio regionale si riserva comunque il diritto di agire in situazioni di emergenza che comportino un rischio immediato per il sistema informatico, come nel caso di un attacco hacker.