Posta elettronica aziendale e metadati delle e-mail dei dipendenti: indicazioni del Garante Privacy e profili di controllo a distanza dell'attività lavorativa

Confindustria Veneto Est

Padova, 8 ottobre 2024

Risvolti operativi delle indicazioni del Garante per le aziende a seguito del Documento di indirizzo del Garante sulla conservazione dei metadati delle e-mail dei dipendenti

Avv. Giovanni Guerra

Come si arriva al Documento di indirizzo …

- indicazioni emerse da accertamenti effettuati dal Garante nei confronti di attività di trattamento dei dati personali in ambito lavorativo (*quali, ad es., i dati generati dall'uso di strumenti, sistemi e servizi aziendali da parte dei dipendenti*)
- rischio che i servizi di posta elettronica, gestiti da fornitori in cloud, potessero raccogliere di default, in modo preventivo e generalizzato, i metadati relativi all'utilizzo degli account di posta elettronica in uso ai dipendenti e conservarli per un ampio arco temporale
- limitazioni poste dai fornitori alla possibilità per le aziende di modificare le impostazioni di tali sistemi o di ridurre il periodo di conservazione di tali dati

La genesi del Documento di indirizzo …

- primo Documento di indirizzo il **21 dicembre 2023**
- **consultazione pubblica** avviata a seguito delle richieste di chiarimenti ricevute
- nuova versione del Documento adottata il **6 giugno 2024**
- apportate varie **modifiche e integrazioni** per agevolare la comprensione dell'ambito dei trattamenti presi in considerazione e delle indicazioni fornite al fine di:
  - **promuovere la consapevolezza delle scelte tecniche e organizzative dei datori di lavoro, in qualità di titolari del trattamento**,
  - **prevenire iniziative e trattamenti di dati in contrasto con la disciplina in materia di protezione dei dati e le norme che tutelano la libertà e la dignità dei lavoratori**

Natura del Documento di indirizzo del Garante sulla conservazione dei metadati delle e-mail dei dipendenti

Come indicato dal Garante, il Documento:

- **non reca prescrizioni né introduce nuovi adempimenti** a carico dei datori di lavoro (titolari del trattamento),
- ma ha **natura orientativa**
  - **intende** cioè **fornire indicazioni** volte ad orientare i datori di lavoro sui criteri da seguire in ordine alla possibilità di trattare tali informazioni per consentire il corretto funzionamento e il regolare utilizzo del sistema di posta elettronica, comprese le essenziali misure di sicurezza informatica, senza necessità di attivare la procedura di garanzia prevista dallo Statuto dei Lavoratori (art. 4.1 l. n. 300/1970, richiamata dall'art. 114 del d.lgs. 196/2003 - Codice Privacy)

Ambito di applicazione del Documento: definizione di metadati o log

I metadati di posta elettronica a cui si riferisce il Documento corrispondono tecnicamente alle **informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica (MTA = Mail Transport Agent)** e **dalle postazioni nell'interazione che avviene tra i diversi server interagenti e, se del caso, tra questi e i client** (le postazioni terminali che effettuano l'invio dei messaggi e che consentono la consultazione della corrispondenza in entrata accedendo ai mailbox elettroniche, definite negli standard tecnici quali **MUA – Mail User Agent**)

Esempi di metadati

Dati relativi alle operazioni di invio e ricezione e smistamento dei messaggi, acquisiti e memorizzati automaticamente in appositi registri/file dai sistemi di posta elettronica nel loro funzionamento (indipendentemente dalla percezione e dalla volontà dell'utilizzatore) quali:

- indirizzi email del mittente e del destinatario,
- indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio,
- orari di invio, di ritrasmissione o di ricezione,
- dimensione del messaggio
- presenza e dimensione di eventuali allegati
- oggetto del messaggio spedito o ricevuto

Il documento non si applica alla conservazione dei messaggi e-mail !

Le indicazioni del Documento relativamente ai tempi di conservazione dei metadati come sopra definiti **non riguardano** invece:

- i **contenuti dei messaggi di posta elettronica (nel corpo o body part)**
- le i**nformazioni tecniche che ne fanno comunque parte integrante riportate nella c.d. envelope o header** (dettagli tecnici parte del messaggio, che documentano l'instradamento del messaggio stesso, la sua provenienza e altri parametri tecnici): informazioni che pur di norma corrispondenti ai suddetti metadati, sono inscindibili dal messaggio, rimanendo nella disponibilità dell'utente/lavoratore, all'interno della casella di posta elettronica attribuitagli.

Pertanto, i messaggi email ricevuti ed inviati dai dipendenti, con i relativi contenuti ed allegati, possono continuare ad essere conservati secondo le regole e policy definite dalla Società!

Tempi di conservazione dei soli metadati

All'esito di valutazioni tecniche, il Garante ritiene che:

- l'attività di conservazione dei s**oli metadati/log necessari ad assicurare il funzionamento delle infrastrutture del sistema di posta elettronica**, possa essere svolta, di norma, **per un periodo limitato a pochi giorni: a titolo orientativo non superiore ai 21 giorni**

- ove così impostata, tale attività di conservazione dei metadati **può essere effettuata anche in assenza di accordo sindacale o di autorizzazione pubblica** (garanzie previste per i c.d. strumenti di controllo a distanza dell'attività dei lavoratori: art. 4, comma 1, St. Lav.), in quanto funzionale a consentire l'assolvimento degli obblighi che discendono direttamente dal contratto di lavoro, ovvero **necessaria per l'esecuzione della prestazione lavorativa** (art. 4, comma 2) – *rinvio alla successiva relazione sui profili giuslavoristici*

Conservazione dei metadati per un tempo superiore …

- nel rispetto del principio di limitazione della conservazione (v. l'art. 5 del GDPR)
- in presenza di particolari condizioni che ne rendano necessaria l'estensione, comprovando adeguatamente le specificità della propria realtà tecnica e organizzativa
- rischio di indiretto controllo a distanza dell'attività dei lavoratori (art. 4.1 L. n. 300/1970):
  - documentare le esigenze organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale per le quali sia essenziale la conservazione dei metadati per un periodo superiore
  - procedere ad un accordo con le RSA o ottenere una autorizzazione dal competente Ispettorato territoriale del lavoro

Limitazione della conservazione dei metadati

- I tempi di conservazione dei metadati (che siano inferiori o superiori ai 21 giorni) devono in ogni caso essere proporzionati rispetto alle legittime finalità perseguite - principio di "limitazione della conservazione" (art. 5, par. 1, lett. e), del GDPR).
- Necessario **definire in ogni caso un tempo di conservazione dei metadati congruo rispetto all'obiettivo di rilevare e mitigare eventuali incidenti di sicurezza,** adottando tempestivamente le opportune contromisure
- Ruolo del DPO

RISVOLTI OPERATIVI PER LE AZIENDE

Il datore di lavoro/titolare del trattamento deve:

- individuare, anche con la collaborazione del fornitore, i **sistemi, servizi, archivi o database in cui sono generati e registrati solo i metadati per garantire il buon funzionamento della posta elettronica** (separati da quelli di gestione e conservazione dei messaggi e-mail ricevuti ed inviati, inclusi contenuti e allegati)
- verificare se si tratti di **sistemi gestiti on-premise (su infrastrutture/apparati aziendali) o in cloud (su infrastrutture del fornitore)**
- per i sistemi così individuati, **verificare anche con il fornitore gli attuali tempi di conservazione dei metadati e le ragioni, finalità od esigenze funzionali e tecniche che li giustificano**

Conservazione dei metadati su sistemi aziendali on-premise

Per i metadati presenti in sistemi on-premise del titolare, ove siano conservati per più di 21 giorni, valutare se:

- Il **più esteso periodo di conservazione sia necessario per finalità od esigenze strettamente connesse al corretto funzionamento e alla sicurezza degli strumenti** utilizzati dal lavoratore per rendere la prestazione lavorativa e, in caso di risposta affermativa, motivare la propria scelta tramite apposito documento
- risulti necessario per altre finalità/esigenze (ad es., organizzative, funzionali, tecniche o difensive), per le quali si renda necessario per l'azienda avviare le attività previste dall'art. 4, comma 1, Statuto dei lavoratori (se del caso, procedendo nelle more ad adottare gli interventi volti, cautelativamente, a bloccare o limitare la conservazione dei metadati) – RUOLO DEL DPO

CONSERVAZIONE DEI METADATI SUI SISTEMI IN CLOUD DEL FORNITORE

Ove i metadati siano conservati sui sistemi in cloud del fornitore per un periodo superiore a 21 giorni, sarà necessario richiedere al fornitore :

- precise informazioni su finalità ed esigenze di mantenimento dei dati per un tempo più ampio, così da effettuare le verifiche precedentemente indicate
- quali siano le eventuali iniziative o azioni adottate per adeguarsi agli orientamenti del Garante (verifica obblighi e responsabIlità contrattuali – RUOLO DI DATA PROCESSOR - DPA)

Il datore di lavoro, quale titolare del trattamento, anche quando utilizza prodotti o servizi realizzati da terzi, deve verificare la conformità ai principi applicabili al trattamento dei dati (art. 5 GDPR), adottare le opportune misure tecniche e organizzative e impartire le necessarie istruzioni al fornitore del servizio (cfr. artt. 5, par. 2, 24, 25 e 32 GDPR)

Privacy by design e by default

Occorre verificare, anche quando si utilizzano prodotti o servizi realizzati da terzi, che siano disattivate le funzioni che non sono compatibili con le proprie finalità del trattamento o che si pongono in contrasto con specifiche norme di settore previste dall'ordinamento (commisurando adeguatamente anche i tempi di conservazione dei dati ovvero chiedendo al fornitore del servizio di anonimizzare i metadati raccolti nei casi in cui non si intenda effettuare una conservazione più prolungata degli stessi)

Adozione delle misure organizzative e tecniche idonee a garantire la sicurezza dei metadati (accessi da parte dei soli soggetti autorizzati, autenticazione e tracciamento accessi, ecc.)

Valutazione di impatto sulla protezione dati

Il datore di lavoro/titolare del trattamento deve valutare se l'attività di trattamento dati che intende porre in essere possa presentare un rischio elevato per i diritti dei lavoratori, circostanza che rende necessaria una preventiva valutazione di impatto sulla protezione dei dati personali (principio di "responsabilizzazione"- artt. 5, par. 2, e 24 GDPR).

Tale necessità ricorre in caso di raccolta e memorizzazione dei log della posta elettronica, alla luce della particolare "vulnerabilità" degli interessati nel contesto lavorativo e del rischio di "monitoraggio sistematico", inteso come "trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti"

NECESSARIO EFFETTUARE O RIESAMINARE LA DPIA ED AGGIORNARE IL REGISTRO DEI TRATTAMENTI !

Informativa ai dipendenti sulla conservazione dei metadati delle e-mail

Il datore di lavoro – titolare del trattamento deve assicurarsi che i lavoratori siano stati adeguatamente informati sul trattamento dei dati personali relativi alle comunicazioni elettroniche che li riguardano (principi di correttezza e trasparenza - artt. 5, par. 1, lett. a), 12, 13 e 14 del Regolamento).

E' necessario aggiornare, integrare o rivedere **l'informativa privacy rivolta ai dipendenti e la policy, regolamento o disciplinare aziendale sull'utilizzo degli strumenti informatici**, prevedendo una descrizione completa e intellegibile del trattamento e della conservazione dei metadati delle e-mail dei lavoratori.

E' importante che gli interessati (i dipendenti) siano resi pienamente consapevoli delle complessive caratteristiche del trattamento (specificando i tempi di conservazione dei dati, gli eventuali controlli, ecc.), delle modalità d'uso degli strumenti e di effettuazione di eventuali controlli.

Obiettivi della Policy aziendale e della Informativa privacy

Policy -> Dare istruzioni ai dipendenti sulle misure di sicurezza e sulle regole di comportamento da rispettare per il corretto uso degli strumenti elettronici, dei servizi informatici, di posta elettronica e internet ed indicazioni sulle finalità e modalità dei controlli da parte del datore di lavoro, nonché informazioni sui correlati trattamenti dei dati personali dei dipendenti (pubblicazione per valenza disciplinare)

Informativa privacy -> Indicare le finalità e modalità del trattamento dei dati (log, metadati) relativi agli accessi fisici ed informatici, credenziali di autenticazione, accessi a sistemi, data base e rete aziendale, servizi e-mail ed internet (esigenze di funzionamento, sicurezza, manutenzione, assistenza, ecc.)

Principali temi da inserire nella Policy aziendale

Norme di riferimento (Codice Civile, Statuto Lavoratori, D.Lgs. 231/2001, Comunicazioni Elettroniche, GDPR, Codice Privacy, ecc.)

Modalità di utilizzo di computer o pc, tablet, smartphone (aziendali o personali, nonché di cartelle e documenti elettronici e di accesso ad archivi o database aziendali

Modalità di connessione ad internet e di uso di piattaforme aziendali e di utilizzo di internet, e-mail, social network

Controlli antivirus ed altre misure di protezione/sicurezza (proxi, antispam, DLP, SOC)

Raccolta, registrazione e memorizzazione di dei dati generati dall'uso della risorse informatiche e telematiche (metadati, log)

Finalità, modalità e tempi di conservazione di tali dati

Finalità e modalità degli eventuali controlli (fini organizzativi, tecnici, di sicurezza, difensivi, ecc.)

Domande?

Grazie per la Vostra attenzione!