METADATI
E
POSTA ELETTRONICA DEI DIPENDENTI

Cos'è successo?

Il 6 giugno 2024 il Garante Privacy ha pubblicato un documento di indirizzo aggiornato dopo la consultazione pubblica.
Il tema? I programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati.

Qual è il problema?

è emerso il rischio che programmi e servizi informatici per la gestione della posta elettronica possano **raccogliere per impostazione predefinita**, in modo preventivo e generalizzato, **i metadati relativi all'utilizzo degli account di posta elettronica** in uso ai dipendenti, **conservando gli stessi per un esteso arco temporale.**

Cosa includono i metadati?

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 e, in certi casi, l'oggetto del messaggio spedito o ricevuto. **Forniscono tutte le informazioni utili per tracciare una email.**

Sono registrati automaticamente dai sistemi di posta elettronica, indipendentemente dalla percezione e dalla volontà dell'utilizzatore.

Perché mi riguarda? Se ho dei dipendenti e i metadati dei miei dipendenti sono utilizzati, devo assicurarmi di essere in conformità con le istruzioni del Garante.

il Garante Privacy ricorda:

- ☑ la necessaria verifica della **liceità** del mio trattamento
- ☑ principio di **responsabilizzazione** → valutare se i trattamenti che intendo realizzare possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche (realizzare possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche (**valutazione d'impatto**)

Ma quindi, cosa devo fare? → analizzare il mio meccanismo interno

Faccio un trattamento di metadati delle email dei dipendenti?
Se la risposata è positiva:

Per quale motivo tratto dei metadati?
Per quanto tempo conservo i metadati?
Ho condotto una valutazione d'impatto?
Ho informato i miei dipendenti?

Quale sono le regole che devo rispettare se i dipendenti sono coinvolti?

L'art. 4 della L. n. 300/197, comma 1 prevede che "Gli **impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori** possono essere impiegati esclusivamente per **esigenze organizzative e produttive**, per la **sicurezza del lavoro** e per la **tutela del patrimonio aziendale** e possono essere installati **previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali.**"

il comma 2 dell'art. 4 della L. n. 300/197, introduce un'eccezione: il restrittivo regime al comma 1 non si applica "agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa"

le e-mail del dipendente possono essere considerate come strumenti utilizzati per rendere la prestazione lavorativa → accordo collettivo non necessario se l'obiettivo è quello di assicurare il funzionamento delle infrastrutture del sistema della posta elettronica

Quali sono i tempi di conservazione?

- ☑ l'attività di raccolta e conservazione dei soli metadati/log **necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica**, all'esito di valutazioni tecniche e nel rispetto del principio di **responsabilizzazione** → si ritiene che possa essere effettuata, di norma, per un periodo limitato a pochi giorni

  a titolo orientativo, tale conservazione non dovrebbe superare i 21 giorni
- ☑ l'eventuale conservazione per un termine ancora più ampio potrà essere effettuata, solo in presenza di **particolari condizioni che ne rendano necessaria l'estensione** (principio di accountability)
- ☑ le 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.**

Cosa devo valutare?

- le mie procedure interne mi permettono di rispettare la scadenza dei 21 giorni?
- i metadati che utilizzo sono essenziali ad accertare un *data breach* o una violazione della sicurezza?
- ci sono adeguate misure interne per mitigare l'impatto in caso di problema di sicurezza?

Ora, qual è la mia missione?

- **verificare i trattamenti interni di metadati**
- **verificare la loro liceità, il loro motivo**
- **valutare la necessità di una valutazione d'impatto**
- **verificare l'adeguatezza delle misure interne di sicurezza informatica**
- **verificare la trasparenza della mia Informativa Privacy**

emlex
eva maschietto
massimo maggiore