Roma, 15 aprile 2024

Garante per la Protezione dei Dati Personali
protocollo@gpdp.it

Oggetto: Contributo alla consultazione pubblica sul "*termine di conservazione dei metadati generati e raccolti automaticamente dai protocolli di trasmissione e smistamento della posta elettronica*" avviata dall'Autorità Garante per la Protezione dei Dati Personali con Provvedimento del 22 febbraio 2024, n. 127

Con la presente le scriventi Assofondipensione, associazione dei fondi pensione negoziali, e Mefop, Società per lo sviluppo del mercato dei fondi pensione, esprimono le seguenti considerazioni in relazione alla consultazione in oggetto.

Termine di conservazione vincolante *erga omnes* e principio di responsabilizzazione

La previsione di un termine di conservazione, tra l'altro estremamente breve, sembrerebbe contrastare con il principio di responsabilizzazione che ha caratterizzato l'evoluzione legislativa europea dalla Direttiva 95/46/CE al GDPR e che di quest'ultimo provvedimento è principio fondante. In forza del predetto principio – da combinare con quanto previsto all'art. 5, par. 1, lett. e), del GDPR –, la normativa europea riconosce in capo ai titolari del trattamento l'onere di individuare un termine di conservazione dei dati personali che sia giustificabile in ragione delle finalità per le quali i dati personali sono trattati.

Il principio di limitazione della conservazione, inoltre, non può essere ritenuto prevalente rispetto agli altri e diversi principi dettati dalla normativa in materia e non richiede al titolare del trattamento di fissare una data di scadenza predeterminata per la conservazione dei dati in forma personale, ma stabilisce che i dati personali siano "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*". La *ratio* della norma appare quella di legare a una finalità specifica la conservazione stessa: la conservazione dei dati è lecita fintantoché la finalità a cui essa è strettamente connessa risulta attuale. Conseguentemente è onere del titolare del trattamento individuare (oltre che dimostrare, se richiesto) i criteri e i termini temporali ritenuti adeguati in ordine alla conservazione dei dati.

Il Garante, mediante il Documento di indirizzo in commento, sembrerebbe quindi aver limitato l'applicabilità del principio di responsabilizzazione nell'ambito della gestione dei metadati delle email, individuando un periodo di conservazione univoco e presuntivamente lecito per tutte le Organizzazioni.

La prescrizione è peraltro rivolta *erga omnes* senza ammettere alcuna deroga in assenza di accordo con le rappresentanze sindacali aziendali e/o nazionali ovvero di autorizzazione dell'Ispettorato del Lavoro (ITL), a norma dell'art. 4, comma 1, della L. n. 300/1970 (strumenti che sembrerebbero avere competenza a svolgere valutazioni in materia di protezione dei dati personali, quanto piuttosto a condividere analisi sotto un profilo meramente giuslavoristico).

Si menziona, in proposito, quanto previsto dall'art. 4, comma 2, della L. n. 300/1970, il quale espressamente afferma che: "*La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*". Tuttavia, non è chiara la motivazione per cui questa disposizione – ad avviso del Garante – non sarebbe applicabile, trascorso il termine imposto di 7 giorni, nell'ipotesi in cui siano conservati esclusivamente i metadati "necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica".
Sul tema, è opportuno effettuare, quindi, una qualificazione precisa e puntuale dei metadati oggetto di siffatta limitazione, anche a fronte dell'attuale impossibilità tecnica di modificare le impostazioni sui termini di conservazione dei metadati, ivi comprese tipologie di metadato e durata, da parte dei *provider* di gestione della posta elettronica comunemente in uso.
Una simile previsione non tiene conto delle peculiarità che ciascun datore di lavoro, Fondo pensione, Fondo sanitario o Cassa previdenza (quindi titolare del trattamento) potrebbe riscontrare, derivanti, per esempio, dal settore di appartenenza o dall'assoggettamento a disposizioni normative in materia di sicurezza informatica che determinano la necessità di maggiori e più incisivi controlli (si pensi, alla normativa NIS, al Digital Operational Resilience Act noto come DORA, al Perimetro di Sicurezza Nazionale Cibernetica, etc.).
Prioritariamente per queste ragioni, si richiede al Garante di voler riesaminare il Documento di indirizzo, al fine di circoscrivere l'ambito oggettivo (tipologia di metadati) e soggettivo (settore lavorativo o categoria di interessati) di applicazione di qualsivoglia termine di conservazione dei metadati della posta elettronica, ribadendo la prevalenza del principio di responsabilizzazione dettato dall'art. 5 del GDPR, idoneo a consentire a ciascuna realtà di valutare il proprio contesto di operatività e di individuare adeguati termini di conservazione nel rispetto di tutte le normative applicabili.

<u>Incongruità del termine di sette giorni</u>

In via subordinata, nella denegata ipotesi in cui il Garante intenda rinnovare la prescrizione di un termine valido *erga omnes* per la conservazione dei metadati contenuti nelle mail, si rappresenta come siffatto termine ("*sette giorni, estensibili, in presenza di comprovate e documentate esigenze che ne giustifichino il prolungamento, di ulteriori 48 ore*") appaia fortemente inadeguato ed eccessivamente stringente a fronte di quanto previsto da numerose disposizioni di legge, alcune dettate anche dallo stesso GDPR.
Il termine, infatti, potrebbe risultare ingiustificatamente restrittivo con quanto previsto dall'art. 32 del GDPR che impone, tanto al titolare del trattamento quanto al responsabile del trattamento, l'adozione di "*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*" individuate sulla base "*dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*".
Questo obbligo, da leggersi unitamente al e quale corollario del principio di responsabilizzazione, ha comportato la scomparsa dalla disciplina in materia di protezione dei dati personali di concetti quali "livello minimo" di misure di sicurezza tipici della Direttiva 95/46/CE e del Codice privacy precedente alle modifiche intervenute con il D.Lgs. n. 101/2018.

Infatti, nell'ottica di una maggiore responsabilizzazione del titolare del trattamento, la valutazione di adeguatezza delle misure tecniche e organizzative implementate, individuate sulla base dei rischi di volta in volta riscontrati è affatto demandata, caso per caso, al titolare stesso o al responsabile del trattamento.
Il GDPR pone molta attenzione sul concetto di "*adeguatezza*" che diventa fondamento delle valutazioni che ogni entità interessata effettua in merito alla rispondenza delle misure di sicurezza implementate al dettato normativo ("*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio"*).
Con riferimento a ciò, è stato già più volte affrontato a livello dottrinale, il carattere intrinsecamente "relativo" della nozione di "*adeguatezza*", definibile molto genericamente come "*capacità di soddisfare una qualità o un risultato posto come un obiettivo"*. È possibile, a livello concreto, equiparare quest'ultimo all'implementazione di misure tecniche e organizzative che consentano di raggiungere un livello di sicurezza "accettabile", sia da un punto di vista tecnico (misure di sicurezza pertinenti) sia da un punto di vista qualitativo (misure di sicurezza efficaci). Anche in siffatto contesto, l'"accettabilità" delle misure di sicurezza deve essere frutto di una attenta valutazione del titolare o responsabile del trattamento, da effettuarsi sia sulla base dei principi sanciti dal GDPR medesimo (es. principi di necessità, pertinenza, proporzionalità), sia sulla base dei già menzionati "parametri" di valutazione espressamente indicati dal Legislatore nell'incipit dell'art. 32 del GDPR (*stato dell'arte; costi di attuazione; natura, oggetto, contesto e finalità del trattamento; rischio di pregiudizio per i diritti e le libertà delle persone fisiche*).
Appare opportuno rappresentare – inoltre – come l'individuazione di un termine di conservazione dei metadati afferenti all'utilizzo della posta elettronica di 7 giorni (anche nel caso di estensione per ulteriori 48 ore) non possa essere in alcun caso condivisa sulla scorta di circostanze di fatto rilevanti per la sicurezza informatica.
Per queste ragioni, si evidenzia che l'adeguatezza delle misure organizzative e la determinazione del termine di conservazione dei metadati devono essere il frutto di un'analisi approfondita e contestualizzata, condotta dal titolare del trattamento. Questo approccio non solo è in linea con il principio di responsabilizzazione sancito dal GDPR, ma si dimostra anche essenziale per affrontare efficacemente i rischi associati agli incidenti informatici.

<u>Contrasto con i principi in materia di diritto penale</u>

Per quanto concerne più precipuamente tutte le finalità connesse alla prevenzione dei reati e di difesa che sono protette da diverse norme codicistiche ed extra-codicistiche, la previsione di un termine stringente di 7 giorni per la conservazione dei metadati associati alle e-mail dei dipendenti in assenza di stipula di accordo sindacale/autorizzazione all'ITL impedirebbe alle organizzazioni di esercitare adeguatamente non solo la propria difesa, ma anche quella dei propri dipendenti, rischiando peraltro di risultare coinvolte o ritenute responsabili di condotte rilevanti penalmente, con conseguenze prevedibili in termini sia di attività istituzionale sia di immagine.

<u>Profili di diritto civile e costituzionale</u>

In ultima istanza, il Documento di indirizzo sembra estendere la nozione di metadati afferenti all'utilizzo della posta elettronica, ricomprendendo – a differenza dei precedenti interventi dello

stesso Garante – informazioni che gli enti in genere sono tenuti a conservare, a norma dell'art. 2220 c.c.. La norma prevede, infatti, la conservazione per dieci anni delle scritture contabili obbligatorie, degli originali delle fatture e della corrispondenza ricevuta, nonché delle copie delle fatture e della corrispondenza spedita, estendendo la propria portata anche alla corrispondenza effettuata a mezzo e-mail e PEC.
In questa prospettiva, sarebbe opportuno che il Garante fornisse una definizione certa di metadato afferente all'utilizzo della posta elettronica, tale da consentire di conciliare gli obblighi in materia di protezione dei dati personali con quelli di natura civilistica, consentendo così ai titolari del trattamento di comunicare istruzioni di dettaglio a fornitori dei servizi di posta elettronica, al fine di procedere esclusivamente alla cancellazione dei dati non necessari per ottemperare a obblighi di diversa natura.
Inoltre, il medesimo termine decennale di conservazione potrebbe trovare applicazione, sempre a norma del diritto civile oltre che nel rispetto dell'art. 24 della Costituzione, laddove una non chiara determinazione dell'esatto contenuto dei metadati afferenti all'utilizzo della posta elettronica costringesse gli enti a procedere alla cancellazione di comunicazioni essenziali tanto alla tutela giudiziale nei confronti di utenti e fornitori quanto nei confronti dei dipendenti e/o collaboratori di diversa natura.

L'occasione è gradita per porgere cordiali saluti.

Assofondipensione

Mefop