All'attenzione della
Spett.le
Autorità Garante
per la protezione
dei dati personali
Pec: protocollo@pec.gpdp.it

Oggetto: **contributo alla consultazione pubblica relativa al Provvedimento del 21 dicembre 2023 - Documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati"**

PREMESSE

- ANORC (Associazione Nazionale per Operatori e Responsabili della Custodia dei dati, delle informazioni e dei documenti digitali- www.anorc.eu) è una realtà senza scopo di lucro - già iscritta all'elenco dei portatori di interesse presso la Camera dei Deputati, il Ministero delle Imprese e del Made in Italy e il Ministero del Lavoro e delle Politiche Sociali - che dal 2007 rappresenta e aggrega le competenze e le esigenze di aziende, enti pubblici, professionisti ed esperti che operano con diversi ruoli nei settori della digitalizzazione e della protezione dei dati;

- ANORC Professioni è iscritta presso il Ministero delle Imprese e del Made in Italy ai sensi della Legge 4/2013 all'elenco delle Associazioni che rilasciano l'attestato di qualità e di qualificazione professionale dei servizi prestati dai Professionisti della digitalizzazione e della privacy;

- Congiuntamente le due Associazioni, stimolate dai numerosi dubbi manifestati dai rispettivi associati relativamente all'interpretazione del Provvedimento del Garante per la protezione dei dati personali dello scorso 21 dicembre 2023 – Documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", hanno ritenuto di aderire alla consultazione pubblica indetta da codesta Autorità per contribuire in modo fattivo e collaborativo a evidenziare quegli elementi che, se confermati dalle intenzioni del Garante, possono risultare non pienamente condivisibili, alla luce delle interpretazioni formulate.

Tanto premesso, le Associazioni hanno invitato i propri associati a fornire un contributo al confronto, al fine di individuare gli elementi sui quali si concentrano maggiormente le perplessità manifestate rispetto al suddetto provvedimento di indirizzo.

Il presente documento è stato stilato a seguito del confronto, e con l'attiva partecipazione, dei seguenti esponenti delle Associazioni:

- Alessia Allegri, avvocato, DPO e professionista privacy di ANORC Professioni;
- Barbara Barbaro, Expert Digital Preservation Archivist e professionista della digitalizzazione di ANORC Professioni;
- Carola Caputo, avvocato, professionista della privacy e professionista della digitalizzazione di ANORC Professioni;
- Anna Dalla Benetta, giurista e professionista della privacy di ANORC Professioni;
- Giovanni Ferorelli, avvocato e professionista della privacy di ANORC Professioni;
- Cesare Gallotti, auditor, consulente in sicurezza delle informazioni e professionista della privacy in ANORC Professioni;
- Fabrizio Ghelarducci, imprenditore e associato ANORC;
- Andrea Infesta avvocato, DPO e associato ANORC;
- Elena Lauritano, archivista digitale e componente del Consiglio direttivo ANORC;
- Andrea Lisi, avvocato, DPO, Chief Digital Officer, professionista della privacy, della digitalizzazione e Presidente di ANORC Professioni, Presidente onorario di ANORC;
- Silvia Loffi, responsabile della conservazione, professionista della digitalizzazione di ANORC Professioni e componente del Consiglio direttivo ANORC;
- Enrico Pelino, avvocato, componente del Comitato tecnico-scientifico e della Commissione di valutazione di ANORC Professioni;
- Flavio Petrino, professionista della digitalizzazione di ANORC Professioni e componente del Consiglio direttivo ANORC;

- Giancarla Porro, responsabile compliance, professionista della digitalizzazione di ANORC Professioni e coordinatore del Consiglio Direttivo ANORC;
- Sabrina Salmeri, avvocato, professionista della privacy, componente del Comitato tecnico scientifico e della Commissione di valutazione di ANORC Professioni;
- Alessandro Selam, giurista e direttore generale di ANORC;
- Sarah Ungaro, avvocato, professionista della digitalizzazione, professionista della privacy e vice Presidente di ANORC Professioni;
- Andrea Zincone, avvocato e professionista della privacy di ANORC Professioni.

A parere delle scriventi Associazioni, il Provvedimento di codesta Autorità - pienamente condivisibile nelle finalità di sensibilizzare e fornire indicazioni su aspetti di natura tecnologica che non sempre sono debitamente trattati con la necessaria attenzione - non risulta centrare, tuttavia, gli obiettivi di chiarezza e consapevolezza, laddove non circoscrive adeguatamente l'ambito di applicazione, formulando con maggiore precisione alcuni concetti espressi nel Provvedimento stesso.
Nello specifico, in effetti, alcuni paragrafi del testo in commento, ove non opportunamente chiariti, potrebbero risultare in contrasto con altre norme primarie dell'ordinamento che prescrivono precise tempistiche di conservazione e qualora non si intervenisse per precisarne il contenuto e per modificarne l'impostazione, potrebbero creare una discriminazione verso i titolari di trattamento sulla base delle tecnologie da questi utilizzate e nei confronti delle quali, nella quasi totalità dei casi, essi non hanno alcun potere decisionale.
Tanto premesso, qui di seguito sono indicati i temi di maggior rilievo che si intendono sottoporre all'attenzione di codesta Autorità.

Concetto di "metadato"

In primo luogo si ritiene che sarebbe utile fare chiarezza sulla definizione che codesta Autorità intende attribuire al concetto di "metadato", delimitando la portata del Provvedimento in commento. Se si ritenesse di dover considerare la definizione più ampia di "metadato", oltre ai log dei server e-mail (assumendo, ma attendiamo conferma da codesta Autorità, che i file log delle e-mail contenuti nei server rientrino in tale nozione), si dovrebbero includere negli effetti del Provvedimento anche gli header di ciascuna e-mail con effetti a dir poco devastanti per la gestione e la conservazione dei dati, delle informazioni e dei documenti degli enti privati e pubblici. L'eliminazione degli header da tutte le caselle di posta, infatti, renderebbe le

e-mail inutilizzabili sotto il profilo documentale, prive di una contestualizzazione, non idonee per essere conservate a norma del D.Lgs. n. 82/2005 e delle Linee guida ivi richiamate e impossibili da ricercare e reperire una volta immesse in un sistema di gestione o conservazione. La medesima sorte spetterebbe anche alla Posta Elettronica Certificata (PEC) e alla Registered Electronic Mail (REM).

Configurazione dei rapporti con i grandi cloud provider di posta

Un ulteriore elemento di perplessità risiede nella configurazione dei rapporti con i grandi cloud provider di posta. Tali relazioni contrattuali sono spesso ribaltate rispetto ai modelli di business che caratterizzavano l'innovazione digitale di anni fa e ribadire che occorra genericamente qualificarli come propri "responsabili del trattamento", senza prendere atto di un sinallagma contrattuale purtroppo oggi del tutto squilibrato, rischia di consigliare ai datori di lavoro soluzioni da essi attualmente non praticabili. È senz'altro corretto analizzare la situazione come ha fatto codesta Autorità nel suo autorevole Documento di indirizzo, ma il bersaglio verso il quale indirizzare eventuali adempimenti da adottare devono essere direttamente i grandi provider di soluzioni di posta elettronica in cloud, i quali possono e devono essere considerati in certi contesti alla stregua di titolari autonomi nel trattamento di determinati dati personali, soprattutto quando di fatto non mettono a disposizione del clienti (individuati quali titolari del trattamento) funzionalità e opzioni di servizio che pongano tali soggetti nelle condizioni effettive di scelta circa i mezzi di trattamento, tra cui – nello specifico - le tempistiche e le modalità di archiviazione di alcuni dati trattati mediante i servizi erogati dai provider (i quali, spesso, trattano tali dati anche per finalità ulteriori, riconducibili al perseguimento di propri interessi, non sempre informando chiaramente in tal senso il cliente/titolare del trattamento).

Antinomia con il principio di Accountability

Formalmente denominato come "documento di indirizzo", il Provvedimento del Garante datato 21 dicembre 2023 appare introdurre un obbligo comportamentale per tutti i destinatari, senza riconoscere il principio di proporzionalità e necessità sancito dal Regolamento 679/2016, che pone a fondamento della responsabilità del titolare del trattamento una valutazione cosciente e matura su elementi che incidono sul trattamento stesso, quali lo stato dell'arte e i costi di attuazione, nonché la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, come anche i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, e non da ultimo la determinazione della durata del trattamento (cfr. artt. 5, 13 e 25 GDPR).
Se così fosse, però, ci si troverebbe di fronte a un cortocircuito interpretativo tra il perseguimento del principio di accountability sancito dal GDPR e l'indicazione del Garante italiano. Rischieremmo di riportare il nostro ordinamento, dunque, ad una

fase pre-Regolamento, quando ancora non era stato introdotto il concetto di "misure adeguate" (che sono il precipitato del principio di accountability) e si ragionava ancora di "misure assolute" (le c.d. misure minime).
Si osserva, a tal proposito, che i rischi derivanti dalla conservazione dei metadati per un lasso di tempo più esteso rispetto a quello indicato nel Provvedimento, tra i quali il controllo a distanza dell'attività dei lavoratori e l'acquisizione di informazioni riferite alla sfera personale o alle opinioni dell'interessato, potrebbero essere efficacemente attenuati mettendo in atto misure tecniche e organizzative idonee a limitare la possibilità di un uso improprio dei medesimi metadati.
A tal fine, potrebbe prendersi in considerazione la possibilità di limitare l'accesso e la consultazione dei metadati ad uno o più soggetti espressamente designati, in possesso di credenziali ad uso esclusivo, per finalità specifiche e tassative, legate alla sicurezza e alla tutela del patrimonio informativo dell'organizzazione. Tali soggetti, da individuare secondo criteri di esperienza e competenza in materia di sicurezza informatica, oltrechè di affidabilità (alla stregua di un Amministratore di Sistema) non dovrebbero rivestire posizioni apicali all'interno dell'organizzazione di appartenenza o, comunque, svolgere funzioni che possano implicare l'adozione di decisioni che incidano sui diritti dei lavoratori. In tal modo, sarebbe preservata la legittima aspettativa di riservatezza degli interessati e, al contempo, arginata la possibilità di controllo a distanza dell'attività dei lavoratori, anche più efficacemente di quanto potrebbe essere assicurato dall'applicazione delle garanzie procedurali di cui all'art. 4, comma 1, l. 20 maggio 1970, n. 300 (accordo sindacale o autorizzazione pubblica del competente Ispettorato del Lavoro).

Perimetro di applicazione del Provvedimento stesso

Considerato che nel Provvedimento il Garante si riferisce a caselle di posta elettronica atte a trattare dati personali, è bene distinguere i casi nei quali questa situazione si possa palesare.
Il trattamento dei dati personali può avvenire qualora al dipendente venga assegnato un account di posta elettronica ad esso esclusivamente intestato e costituito da nome e cognome (nelle diverse declinazioni) @azienda.it oppure - qualora pur in presenza di account riferito all'ufficio (ad esempio amministrazione @azienda.it) - sia facilmente desumibile che la disponibilità di quell'account spetti a un unico soggetto identificabile.
In ogni caso, secondo le scriventi Associazioni la casella di posta elettronica fornita dal datore di lavoro al dipendente è "strumento di lavoro" che ha la funzione di veicolare la comunicazione tra l'azienda e i propri interlocutori per problematiche tecniche, amministrative e commerciali.

Solitamente le policy aziendali illustrate ai dipendenti e recepite dagli stessi chiariscono che l'uso dello strumento assegnato nell'ambito dell'incarico lavorativo è consentito solo ed esclusivamente nell'ambito lavorativo, appunto, e se ne deprecа l'utilizzo per scopi personali.
In questo senso, il contenuto delle caselle e-mail, che si riferisce alle problematiche tecniche, amministrative e commerciali sopra indicate, costituisce un oggetto informatico attinente all'espletamento delle mansioni lavorative che ha valenza legale per gli impegni assunti nei confronti di clienti, fornitori, business partner e nella regolazione dei rapporti tra datore di lavoro e lavoratore stesso.
La casella di posta elettronica assegnata al lavoratore per rendere la prestazione lavorativa, secondo l'art. 4, comma 2, della Legge 300/1970 (c.d. Statuto dei lavoratori), non può sottostare, quindi, alla disciplina prevista per gli strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori.
Per questa ragione, si ritiene che la posta elettronica del dipendente rientri nella legittima sfera di competenza dell'azienda e i metadati (sia quelli c.d. di utilizzo che quelli c.d. di servizio) devono seguire la medesima sorte. Senza i metadati il messaggio di posta elettronica, infatti, risulta alla pratica inutile perché privo di contestualizzazione, privo degli elementi che ne determinino l'autenticità e impossibile da reperire all'interno di un sistema di gestione o conservazione. Inutile, poi, sottolineare le problematiche di tipo organizzativo che verrebbero a crearsi all'interno di un ente sia pubblico che privato dal decimo giorno dalla ricezione o dall'invio qualora il messaggio di posta elettronica rimanesse privo di queste fondamentali informazioni.

Conservazione dei metadati della posta elettronica

L'ultimo elemento di non facile comprensione, sul quale si ritiene fondamentale un intervento chiarificatore dell'Autorità, è proprio legato al termine massimo di conservazione dei metadati della posta elettronica.
Il termine massimo di 9 giorni (7 + eventuali 2) previsto dal Garante come estensione massima del periodo di conservazione dei metadati legati alla posta elettronica appare, infatti, incompatibile con le disposizioni del nostro ordinamento e in ogni caso inadatto a gestire le conseguenze, ad esempio, di un eventuale data breach o di altri incidenti di sicurezza.
Il nostro ordinamento in tema di conservazione dei documenti informatici contempla una dettagliata normativa - anche tecnica - che prevede tempistiche di conservazione proprio per oggetti informatici complessi (come fascicoli e documenti informatici e relativi metadati): da ultimo le nuove Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici del maggio 2021 (pubblicate il 9 settembre

2020, poi modificate con Determinazione n. 371/2021 del 17 maggio 2021 e da attuare obbligatoriamente entro il 1° gennaio 2022) .
In estrema sintesi, possiamo riferire che la posta elettronica, in quanto documento elettronico che contiene una rappresentazione informatica di atti, fatti e dati giuridicamente rilevanti (definizione di documento informatico secondo il D.Lgs. 82/2005) deve rispettare le regole tecniche previste nel nostro ordinamento, contenute appunto nelle prima citate Linee Guida AgID, e che contemplano la memorizzazione di tutti i metadati che sono parte integrante dell'oggetto informatico da conservare (in questo caso messaggi di posta elettronica ed eventuali allegati) e, come previsto nella descrizione del processo di conservazione, devono essere nella disponibilità del Responsabile della conservazione, che non corrisponde senz'altro al singolo dipendente.
Con riferimento alle tempistiche di conservazione, si evidenzia che in generale tutta la documentazione dei soggetti privati che ha rilevanza contabile (e quindi anche la corrispondenza), ai sensi del Codice civile, deve essere "conservata a norma" per 10 anni e rimanere nella disponibilità dell'azienda almeno per tale periodo. Per le amministrazioni pubbliche vige, diversamente, una normativa ancora più stringente, che prevede che tutta la documentazione (e, quindi, anche la corrispondenza informatica) sia conservata, fatta salva l'attivazione della procedura di scarto sottoposta alla vigilanza della Sopraintendenza archivistica territoriale o all'Archivio di Stato.
Nello specifico, poi, non possono non ricordarsi anche le previsioni del D.Lgs. 109/2008, (Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE), che stabiliscono che i tempi di conservazione imposti ai provider anche per i log che si riferiscono alla posta elettronica, non siano inferiori ai 6 mesi.
Prendendo spunto dalla ratio che è alla base del sopra citato D.Lgs. 109/2008, non si comprende per quale ragione il Provvedimento in commento abbia a oggetto esclusivamente i metadati della posta elettronica. Non si può non notare, infatti, che il rischio che programmi e servizi informatici possano raccogliere per impostazione predefinita, in modo preventivo e generalizzato, dati personali conservando gli stessi per un esteso arco temporale, non si limita esclusivamente ai servizi di posta elettronica, ma dovrebbe essere ampliato ai browser, ai servizi di telefonia, ai firewall, ecc. Pertanto, non si comprende perché i fornitori in modalità "cloud" di prodotti e servizi "as a service", e soprattutto i titolari del trattamento che si avvalgono dei loro servizi, dovrebbero ritenersi maggiormente esposti al rischio di

censura per violazioni dei principi del GDPR (e dello Statuto dei Lavoratori) rispetto ai fornitori e agli utilizzatori di soluzioni che determinano rischi simili.
Non si comprende, peraltro, perché la raccolta e la conservazione dei "metadati" necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica sarebbe legittima e consentita solo se limitata a poche ore e comunque entro non oltre sette giorni, estensibili al massimo ad ulteriori due giorni, mentre superato tale limite temporale la conservazione di tali informazioni configurerebbe tout court un indiretto controllo a distanza dell'attività dei lavoratori. Ed invero, disponendo per tutti i titolari lo stesso termine di durata di conservazione, si avrebbe il paradosso che per alcuni la conservazione potrebbe legittimamente durare per un arco temporale "superiore" alle necessità del caso di specie e per altri, invece, per un arco temporale inferiore al tempo necessario al conseguimento delle finalità giustificative del trattamento, in evidente discordanza con le previsioni degli artt. 5, 24 e 25 GDPR.

***

Ciò esposto, e manifestando la disponibilità per eventuali approfondimenti che codesta Autorità ritenesse di attivare, le scriventi Associazioni auspicano che si possa addivenire a un aggiornamento del Provvedimento di indirizzo che tenga conto delle indicazioni segnalate e, in particolare, si auspica che:

a) in pieno accordo con i citati principi di proporzionalità e accountability, si possa eliminare dal Documento di indirizzo qualsiasi preciso riferimento temporale vincolante per i datori di lavoro;

b) in ogni caso, considerato il rovesciamento del sinallagma contrattuale in atto nei rapporti tra datori di lavoro e grandi provider di posta, valutare di indirizzare eventuali adempimenti e obblighi che si riterranno opportuni verso i soggetti che si trovano, di fatto, in una posizione tale da limitare l'autonomia decisionale dei titolari del trattamento e, cioè, i provider di posta elettronica.
Restando disponibili a ulteriori confronti o richieste di delucidazione e grati per l'apertura manifestata dall'Autorità verso il mondo dell'impresa e delle professioni, si porgono i nostri saluti più cordiali.

Lecce, 12 aprile 2024

La Direzione

Sede legale: Via Vito Mario Stampacchia n°21 – 73100 Lecce
Tel. e fax: 0832-256065 – E-mail: segreteria@anorc.it
www.anorc.eu - C.F.: 09747511005 – P.IVA: 04367590751