



# Garante Privacy: l'ex dipendente mantiene il diritto di accedere alle sue e-mail aziendali

 24/04/2026

Gaspere Roma  
Adriano Garofalo

**L**e e-mail contenute in *account* aziendali di un ex dipendente, anche quelle di contenuto strettamente lavorativo, mantengono la natura di dati personali dell'interessato, e il datore di lavoro non può, salvo eccezioni tassativamente previste dalla legge, impedire al dipendente di accedervi. È questo il principio cardine affermato dal Garante per la Protezione dei Dati Personali con il provvedimento n. 165 del 12 marzo 2026, reso all'esito del reclamo proposto da un ex dipendente nei confronti dell'ex datore di lavoro per il mancato idoneo riscontro all'istanza di accesso ai dati personali contenuti nella casella di posta elettronica aziendale.

**Il principio di base: il diritto di accesso ai propri dati personali**

La pronuncia del Garante ripercorre, con estremo interesse, alcuni principi cardine del nostro sistema giuridico in materia di *privacy*. Nello specifico, ai sensi dell'art. 15 del Regolamento (UE) 2016/679 (GDPR) - che disciplina il diritto di accesso ai propri dati personali - ciascuno di noi ha il diritto di sapere se un soggetto stia trattando i propri dati personali e, in caso affermativo, di accedervi e riceverne copia, nonché di ottenere ulteriori informazioni circa le finalità per cui i dati sono utilizzati, i destinatari cui i dati sono o saranno comunicati e il periodo di conservazione previsto. Si tratta di un diritto di particolare rilevanza nell'ambito dei rapporti di lavoro, poiché il lavoratore può in qualsiasi momento rivolgersi al proprio datore di lavoro (o ex datore di lavoro) per ottenere un quadro chiaro ed esaustivo dei propri dati personali oggetto di trattamento.



## Il caso

A seguito della cessazione del rapporto di lavoro, l'ex dipendente chiedeva all'ex datore di lavoro di poter accedere ai documenti e alle cartelle personali presenti sul proprio *pc* aziendale e nella casella di posta elettronica aziendale allo stesso riferibile. Nel corso degli incontri tenutisi presso la sede aziendale, la Società consentiva l'accesso al *desktop* e il recupero di alcuni documenti; quanto alle *e-mail*, tuttavia, veniva consegnata *"la posta solamente personale quali scambi con famigliari, CU personali, rimborsi spese"*, mentre non venivano consegnati *"altri messaggi di posta elettronica afferenti all'attività lavorativa e/o documenti ritenuti dai referenti della società non a contenuto personale"*.

L'ex dipendente formulava quindi una formale istanza di accesso ai sensi dell'art. 15 del GDPR, chiedendo copia di tutte le *e-mail* presenti nella casella di posta elettronica aziendale. La Società comunicava all'interessato che la richiesta esulava dal diritto di accesso, in quanto *"i dati e le informazioni presenti nella casella di posta elettronica sono di proprietà della società e la richiesta doveva essere limitata ai soli dati "strettamente personali" contenuti nella casella di posta elettronica"*.

La corrispondenza veniva quindi consegnata all'ex dipendente, a seguito di attività di oscuramento e anonimizzazione effettuata dalla Società sul contenuto della corrispondenza, *"epurata di molti elementi"*. Il caso approdava quindi dinnanzi al Garante, la cui istruttoria faceva emergere ulteriori profili critici, relativi alla conservazione della posta elettronica tramite *backup* quinquennale e all'assenza di adeguate informative rese ai dipendenti.

### L'illecita limitazione del diritto di accesso

Premesso che la totalità delle comunicazioni elettroniche transitate su un *account* di posta aziendale individualizzato, che ricomprendono necessariamente anche i dati relativi all'attività lavorativa, alla luce delle definizioni di *"dato personale"* del GDPR, sono inevitabilmente riconducibili a dati personali dell'assegnatario dell'*account*, il

profilo di maggiore rilevanza della decisione attiene alle limitazioni che il datore di lavoro può legittimamente opporre al diritto di accesso del proprio ex dipendente. Nel caso di specie, la società ha impedito all'ex dipendente di ricevere le *e-mail* con contenuto lavorativo, invocando genericamente l'esigenza di tutelare i diritti dei terzi e i segreti aziendali. Il Garante ha ritenuto illecita tale condotta, ricordando che le limitazioni al diritto di accesso sono ammesse esclusivamente in caso di richieste manifestamente infondate o eccessive o laddove l'esercizio del diritto di accesso possa arrecare pregiudizio alla tutela dei diritti e delle libertà altrui, ivi inclusi, ai sensi del considerando 63 del GDPR, anche il segreto industriale e aziendale e la proprietà intellettuale. Tuttavia, l'Autorità ha ritenuto che *"la generica preoccupazione che, dando seguito alla richiesta di accesso, i diritti e le libertà altrui possano essere lesi non è sufficiente"* per limitare il diritto di accesso: il titolare del trattamento deve essere in grado di dimostrare che, nella situazione concreta, i diritti o le libertà altrui sarebbero effettivamente lesi, così spostando l'attenzione da un rischio meramente potenziale (astrattamente sempre presente in ogni circostanza) ad uno concreto e sostanziale (da verificare caso per caso, a seconda delle circostanze). Nel caso in esame, il Garante ha osservato che i dati riferiti ai terzi erano contenuti in comunicazioni già ricevute e conosciute dallo stesso interessato, rendendo l'attività di oscuramento non necessaria; quanto ai segreti aziendali, la Società non ha prodotto alcun elemento idoneo a dimostrare che dall'accesso potesse derivare un pregiudizio effettivo e concreto.

### La riservatezza della corrispondenza aziendale è protetta dalla Costituzione

Il Garante ha ribadito che il contenuto dei messaggi di posta elettronica, come pure i dati esteriori delle comunicazioni e i file allegati, riguarda forme di corrispondenza la cui riservatezza è protetta dall'art. 15 della Costituzione e dall'art. 8 della CEDU. Tale tutela è ormai consolidata nella giurisprudenza europea ed italiana.

Ne discende che il datore di lavoro non può legittimamente accedere al contenuto della casella di posta elettronica aziendale individualizzata dell'ex dipendente al fine di esaminarne, filtrare o selezionare la corrispondenza, trattandosi di comunicazioni assistite da garanzia di segretezza costituzionale. Qualsiasi attività di accesso preventivo al contenuto delle *e-mail*, anche se motivata dall'intento di individuare informazioni aziendali riservate, si pone in contrasto con i principi fondamentali in materia di protezione dei dati personali e con le garanzie poste a tutela della dignità del lavoratore. Si rammenta, tuttavia, che i principi sopra esposti non trovano diretta applicazione con riferimento ad indirizzi di posta elettronica condivisi tra più dipendenti e non individualizzati (ad esempio, *teamsales@azienda.com*), i quali possono rappresentare un efficace strumento organizzativo per la conservazione delle comunicazioni elettroniche di natura aziendale, garantendo al datore di lavoro la possibilità di accedervi anche successivamente alla cessazione del rapporto di lavoro con i singoli dipendenti.

#### **Gli ulteriori profili di illiceità: *backup* delle *e-mail* e obblighi informativi**

Il provvedimento offre altresì l'occasione per ribadire un principio ormai consolidato nella giurisprudenza del Garante: la conservazione sistematica del contenuto delle caselle di posta elettronica aziendali degli ex dipendenti mediante *backup*, nel caso di specie protratta per un periodo di cinque anni, costituisce violazione della normativa applicabile. Tale conservazione viola i principi base di cui all'art. 5 del GDPR, come quello di minimizzazione e di limitazione della conservazione dei dati. In concreto, com'è noto, le *e-mail* dell'ex dipendente devono essere cancellate definitivamente alla cessazione del rapporto di lavoro (salvo rare eccezioni), senza ingiustificati ritardi. Il provvedimento ha altresì censurato l'inadeguatezza delle informazioni rese al personale. Nel caso di specie, le informative *privacy* e le *policy* aziendali si limitavano a indicare, in termini del tutto

generici, che "*il periodo di conservazione può variare in modo significativo in base a: finalità, tipo di dato trattato, obblighi di legge*", senza fornire alcuna indicazione puntuale in ordine alle concrete attività di trattamento effettuate sulla posta elettronica, ai tempi di conservazione effettivamente applicati e ai relativi presupposti di legittimità. Il Garante ha ritenuto che tali indicazioni generiche non soddisfino i requisiti di trasparenza e specificità imposti dall'art. 13 del GDPR, richiedendo, per l'effetto, la necessità di prevedere specifiche e dettagliate informative tali da realizzare, nel concreto, l'interesse alla trasparenza ed alla piena consapevolezza del trattamento dei propri dati personali, previsto dalla normativa vigente.

#### **Conclusioni**

Il provvedimento in esame conferma con chiarezza che il diritto di accesso ai dati personali, sancito dall'art. 15 del GDPR, si estende alla totalità delle comunicazioni elettroniche transitate su un *account* di posta aziendale individualizzato, ivi comprese quelle di contenuto strettamente lavorativo. Il datore di lavoro non può arrogarsi il potere di selezionare, filtrare o oscurare preventivamente la corrispondenza dell'ex dipendente, subordinando la consegna a una propria valutazione discrezionale circa la natura "*personale*" o "*aziendale*" dei messaggi. Il Garante, però, precisa un ulteriore importante principio, sino ad oggi spesso trascurato dalle organizzazioni aziendali: il diritto di accesso dei dipendenti non si esaurisce con la cessazione del rapporto di lavoro, ma persiste anche oltre tale termine, creando un'importante, e spesso difficile da gestire, dissociazione tra diritti e doveri derivanti dal rapporto di lavoro e quelli attinenti al diritto alla *privacy*. Inoltre, il Garante ribadisce che le limitazioni al diritto di accesso sono ammesse esclusivamente nei casi tassativamente previsti dal GDPR, senza che il datore di lavoro abbia alcuna possibilità di ostacolarlo adducendo generiche e non circostanziate argomentazioni. Il provvedimento rappresenta dunque un monito significativo per tutti i datori di lavoro, chiamati a garantire un riscontro

integrale e tempestivo alle istanze di accesso dei propri dipendenti ed ex dipendenti, nel rispetto dei consolidati principi di correttezza e trasparenza che informano la disciplina in materia di protezione dei dati personali. A ciò si aggiunge la necessità di predisporre informative puntuali e specifiche in ordine alle attività di trattamento effettivamente svolte sulla posta elettronica aziendale, non essendo a tal fine sufficienti indicazioni generiche contenute nelle procedure aziendali, nonché la necessità di rivedere accuratamente i regolamenti e le *policy* relativi all'utilizzo dei sistemi informatici (posta elettronica e *internet* su tutti, ma ormai anche intelligenza artificiale), con l'ulteriore obbligo di procedere alla tempestiva cancellazione delle *e-mail* alla cessazione del rapporto di lavoro.

Dal provvedimento in esame ne deriva, in conclusione, l'urgente necessità delle aziende di rivedere attentamente le proprie politiche interne sull'utilizzo dei sistemi informatici, ivi inclusi *e-mail* aziendali ed *internet*, avendo cura di approcciare la tematica in oggetto con una maggiore sensibilità, abbandonando la *standardizzazione* dei formati (soventemente in uso presso gruppi multinazionali) per sposare un approccio *customizzato*. Come più volte ribadito


dall'Autorità, infatti, non è sufficiente rendere al dipendente informazioni generiche sul trattamento suoi dati personali. In sostanza, per usare (o forse *abusare*) di uno *slogan* spesso in uso nella comunicazione, le aziende dovranno iniziare a mettere la *privacy* al centro del rapporto con i propri dipendenti. Ciò non solo al fine di evitare di incorrere in pesanti sanzioni per violazione della normativa sulla protezione dei dati, ma anche per poter legittimamente accedere e utilizzare, ove necessario, i dati e le informazioni personali dei dipendenti presenti sui sistemi di posta elettronica aziendali individualizzati, anche e soprattutto nell'ottica, eventuale ma non certo remota, di specifici contenziosi con i propri *ex* collaboratori.

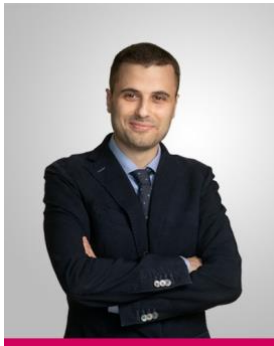
Di certo, il rispetto delle stringenti regole sulla *privacy* costituisce e costituirà sempre più una frontiera sulla quale le due parti contrapposte del rapporto di lavoro saranno chiamate a confrontarsi, anche in sede giudiziale. Proprio per tale ragione, una maggiore attenzione a tali tematiche, sin dall'instaurazione di un rapporto di lavoro, rappresenta senz'altro un utile e saggio approccio di minimizzazione del rischio legale, sempre maggiormente apprezzato dalle aziende di qualunque dimensione.



**Gaspare Roma**  
**PARTNER**


 [g.roma@dejalex.com](mailto:g.roma@dejalex.com)  
 +39 02 72554.1

 Via San Paolo 7  
20121 - Milan



**Adriano Garofalo**  
**ASSOCIATE**

 [a.garofalo@dejalex.com](mailto:a.garofalo@dejalex.com)  
 + 39 02 72554.1

 Via San Paolo 7  
20121 - Milan

**MILANO**  
Via San Paolo, 7 · 20121 Milano, Italia  
T. +39 02 72554.1 · F. +39 02 72554.400  
[milan@dejalex.com](mailto:milan@dejalex.com)

**ROMA**  
Via Vincenzo Bellini, 24 · 00198 Roma, Italia  
T. +39 06 809154.1 · F. +39 06 809154.44  
[rome@dejalex.com](mailto:rome@dejalex.com)

**BRUXELLES**  
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique  
T. +32 (0)26455670 · F. +32 (0)27420138  
[brussels@dejalex.com](mailto:brussels@dejalex.com)

**MOSCOW**  
Potapovsky Lane, 5, build. 2, 4th floor, office 401/12/9 · 101000, Moscow, Russia  
T. +7 495 792 54 92 · F. +7 495 792 54 93  
[moscow@dejalex.com](mailto:moscow@dejalex.com)