



## **Indice**

Gentile Cliente,

torna il consueto appuntamento mensile con gli aggiornamenti in relazione alle novità rilevanti in tema di protezione dei dati, sicurezza e GDPR.

Questo mese affrontiamo il tema relativo alle caselle email degli ex dipendenti, esaminando, con un approccio pratico ed operativo, quali sono le corrette condotte che il datore di lavoro deve porre in essere al fine di rispettare la disciplina relativa alla protezione dei dati, anche riguardo agli aspetti giuslavoristici.

Quando un dipendente sceglie di abbandonare il proprio posto di lavoro, a prescindere dai motivi per i quali prende tale scelta, il datore di lavoro deve affrontare una serie di adempimenti molto precisi.

Uno degli adempimenti più rilevanti è sicuramente la gestione della casella email dell'ex dipendente: fino al giorno precedente quest'ultimo ha utilizzato tale canale di comunicazione per scambiare comunicazioni con i clienti, per inviare documenti ed allegati e molto spesso rappresenta l'unico canale di contatto che i soggetti esterni all'azienda (clienti, collaboratori, fornitori, prospect, altri dipendenti etc..) hanno a disposizione per contattare ed interagire con l'azienda stessa.

Si aggiunga inoltre che le caselle email dei dipendenti ospitano file, documenti e materiali di vitale importanza per la continuità del business aziendale che qualora vengano persi, rappresentano nelle ipotesi più gravi un pericolo di danno per il datore di lavoro, nelle ipotesi più lievi costanti rallentamenti dell'attività quotidiana dell'azienda.

Ma andiamo con ordine.

### ***Ma la casella email con il dominio @nomeazienda non appartiene al datore di lavoro e quest'ultimo può farci ciò che vuole?***

No! Questa domanda viene posta molto spesso e rappresenta una "falsa credenza popolare" molto diffusa, che occorre procedere a screditare. La Corte di Cassazione ha avuto modo di specificare più volte e in diverse sentenze il principio secondo il quale una casella email **a nome di uno specifico dipendente (nome.cognome@dominioazienda.it)** il cui accesso sia protetto da una password personalizzata, rappresentano il domicilio informatico del dipendente, che ha il diritto di escludere chiunque dall'accesso (dunque anche il superiore gerarchico o il datore di lavoro).

Diverso è il caso in cui l'indirizzo email sia condiviso tra più lavoratori che vi possano avere accesso (ad esempio indirizzi come info@dominioazienda.it, ufficiovendite@dominioazienda.it, ufficioreclami@dominioazienda.it, urp@dominioazienda.it etc...). In questo caso la casella email non rappresenta il domicilio digitale del singolo lavoratore. La creazione di caselle comuni ad accesso condiviso, in aggiunta alle caselle nominative dei lavoratori, rappresenta già un primo consiglio che possa garantire la continuità delle comunicazioni aziendali anche in caso di assenza/abbandono del posto di lavoro da parte del dipendente.

### ***Quali sono le corrette prassi da seguire per la gestione della casella email del dipendente nel momento in cui quest'ultimo decide di andare via? I dieci comandamenti.***

Qui di seguito si riportano i corretti passaggi delle procedure relative a carico del datore di lavoro rispetto alla casella di posta elettronica del dipendente. I passaggi derivano dalla lettura di specifici

provvedimenti dell'Autorità Garante per la protezione dei dati personali, unitamente a pronunce della Corte di Cassazione (sia in ambito penale che civile).

1. Impostare un messaggio di risposta automatico sulla casella dell'ex dipendente con lo scopo di avvisare i terzi, mittenti dei messaggi, che la casella alla quale stanno scrivendo non è monitorata e che la richiesta non potrà avere visibilità per l'azienda, fornendo contemporaneamente un indirizzo alternativo al quale il mittente potrà inoltrare nuovamente il messaggio e indicando una tempistica entro la quale l'indirizzo dell'ex dipendente verrà disattivato permanentemente.
2. NON impostare in alcun caso sistemi di reindirizzamento automatico dei messaggi ricevuti sulla casella dell'ex dipendente verso altri indirizzi.
3. NON accedere in alcun caso alla casella email del dipendente, nemmeno qualora il datore di lavoro conosca ILLEGITIMAMENTE le credenziali di accesso a quella casella.
4. NON procedere a modificare le credenziali di accesso dalla dashboard di controllo del dominio email per poter continuare ad accedere alla casella.
5. NON effettuare la copia integrale dei messaggi presenti all'interno della casella email dell'ex dipendente.
6. Fornire, in costanza di rapporto di lavoro e non al termine dello stesso (preferibilmente già in sede di assunzione dei dipendenti) un disciplinare sull'uso degli strumenti IT, al fine di informare preventivamente i dipendenti circa le caratteristiche essenziali dei trattamenti che il datore di lavoro intende effettuare, anche con riferimento all'utilizzo della casella email. Tale documento deve essere redatto in modo chiaro e senza formule generiche, deve essere pubblicizzato adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro o tramite condivisione nella rete intranet aziendale) che spieghi quali sono le regole adottate dall'azienda in relazione a tali aspetti.
7. Specificare all'interno del disciplinare quali sono le condotte tollerate per l'uso della casella di posta elettronica (ad esempio non può essere utilizzata per comunicazioni private del dipendente, ma solo per comunicazioni afferenti alla mansioni lavorative dello stesso).
8. Specificare all'interno del disciplinare reso disponibile per i dipendenti quale sia la politica dell'Azienda in relazione al periodo di conservazione del contenuto delle caselle email; la politica scelta deve tenere in debita considerazione i principi data-protection indicati all'articolo 5 del GDPR (liceità, correttezza e trasparenza, minimizzazione dei dati, esattezza, limitazione della conservazione e integrità e riservatezza).
9. Specificare all'interno del disciplinare se sono state impostate modalità di accesso alla casella email all'abbandono del dipendente, accesso, lo si ribadisce, non integrale, ma esclusivamente tramite specifici criteri di ricerca per parole chiave attinenti al business dell'azienda, al fine di reperire documenti aziendali e comunicazioni contenute nella casella email. In tale caso, molto delicato e da discutere previamente con un legale, occorre anche specificare quali sono le garanzie che verranno adottate nell'estrazione (verbalizzazione dell'evento, impostazione e scelta delle parole chiave, intervento di altri dipendenti quali garanti delle operazioni effettuate etc...)
10. Come suggerito poco sopra, rendere disponibili indirizzi condivisi tra più lavoratori (divisi per funzioni aziendali e non nominali) ed invitare i dipendenti a inserire in copia conoscenza alle comunicazioni inoltrate e ricevute tali indirizzi a seconda della competenza ed esclusivamente per comunicazioni strettamente correlate al business aziendale, senza alcun riferimento a fatti di vita provata del dipendente, in modo che documenti aziendali, comunicazioni con clienti, fornitori e prospect, unitamente a richieste specifiche di questi, non vadano perdute a seguito dell'abbandono del posto di lavoro da parte del dipendente.

### ***Un caso recente: il provvedimento dell'Autorità Garante del 4 dicembre 2019.***

Il Garante ha ritenuto **illecita la condotta di un'azienda che, dopo la cessazione del rapporto di lavoro, aveva mantenuto attivo per un lungo periodo l'account di posta elettronica aziendale dell'ex dipendente**: in questo caso, quindi, vi era da un lato l'interesse dell'azienda a non disperdere dati ed informazioni utili contenute nell'account di posta elettronica aziendale dell'(ex)

dipendente (come ad es. mantenere vivi contatti che l'ex dipendente aveva intrattenuto coi clienti della società), dall'altro il diritto alla tutela della riservatezza della corrispondenza dell'interessato, per quanto riguarda la propria corrispondenza presente sull'account aziendale.

Nel caso di specie, l'ex dipendente ha contestato al datore di lavoro, in particolare, **l'accesso ai messaggi ricevuti sul suo account** e la **mancata disattivazione dell'e-mail aziendale**. Il dipendente era venuto a conoscenza di questi fatti per caso, nel corso di una causa di lavoro promossa nei suoi confronti dalla sua ex azienda.

Il Garante, ricevuto il reclamo da parte dell'ex dipendente, ha effettuato gli accertamenti necessari, da cui è emerso che **l'account di posta era rimasto attivo per oltre un anno e mezzo dopo la conclusione del rapporto di lavoro prima della sua eliminazione**, e che l'eliminazione era avvenuta solo dopo la diffida presentata dal lavoratore. In questo periodo la società aveva avuto accesso alle comunicazioni che vi erano pervenute, **alcune anche estranee all'attività lavorativa del dipendente**.

Oltre a dichiarare illecito il trattamento, il Garante ha **ammonito la società a conformare** i trattamenti effettuati sugli account di posta elettronica aziendale dopo la cessazione del rapporto di lavoro alle disposizioni e ai principi sulla protezione dei dati ed ha disposto **l'iscrizione del provvedimento nel registro interno delle violazioni istituito presso l'Autorità**. Tale iscrizione costituisce un precedente per la valutazione di eventuali future violazioni.

Per ulteriori informazioni [soluzioneprivacy@fulcri.it](mailto:soluzioneprivacy@fulcri.it)