

circolare
13 MAGGIO 2015



Studio
Arlati Ghislandi

CONSULENZA
DEL LAVORO E FISCALE

Milano, 13 maggio 2015

Oggetto

Datori di lavoro e privacy: le nuove linee guida dal Garante della privacy

Il Garante della Privacy ha recentemente pubblicato le Linee Guida in cui vengono illustrate le principali regole che caratterizzano la gestione della privacy nel rapporto di lavoro.

Il testo divulgato, pur non innovando rispetto ai precedenti orientamenti, può essere utile per riepilogare in un unico documento le norme in materia di privacy in ambito lavorativo

Preliminarmente viene ribadito il fondamento per il quale il datore di lavoro può trattare informazioni personali solo se strettamente indispensabili all'esecuzione del rapporto di lavoro, altresì specificando che il trattamento dei dati può avvenire solo a cura del personale incaricato, garantendo idonee misure di sicurezza per proteggerli da intrusioni o divulgazioni illecite.

Sul luogo di lavoro va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità delle persone garantendo la sfera della riservatezza nelle relazioni personali e professionali.

I dati personali

Le informazioni personali trattate possono riguardare,

- l'attività lavorativa;
- la sfera personale e la vita privata dei lavoratori (ad esempio i dati sulla residenza e i recapiti telefonici);
- e dei terzi correlati al soggetto (ad esempio dati relativi al nucleo familiare per garantire determinate provvidenze).

I trattamenti di dati personali devono rispettare il principio di necessità secondo il quale il dato acquisito deve essere trattato per il solo tempo necessario alla reale necessità di utilizzo, configurando in tale senso anche i sistemi informativi e i programmi informatici.

Finalità e caratteristiche del trattamento dei dati

Il trattamento dei dati personali, anche sensibili, deve essere effettuato per finalità determinate, esplicite e legittime in base ai principi di pertinenza e non eccedenza.

Pertanto tale trattamento, riferibile a singoli lavoratori è lecito, se finalizzato ad assolvere obblighi derivanti dalla legge, dal regolamento o dal contratto individuale (ad esempio, per verificare l'esatto adempimento della prestazione o commisurare l'importo della retribuzione).

Il Garante dopo avere stabilito i principi generali sopra enunciati, passa in rassegna determinati argomenti, *tra cui*

Cartellini identificativi

Le aziende possono dotare il lavoratore di un cartellino di riconoscimento.

A parere del Garante risulta eccessivo riportare per esteso tutti i dati anagrafici o le generalità complete del dipendente: a seconda dei casi può essere sufficiente un codice identificativo o il solo nome o il ruolo professionale ricoperto dal lavoratore.

Pubblicazioni di dati del lavoratore sui siti web e sulle reti interne

Il Garante ricorda che la pubblicazione di informazioni personali (foto, c.v.) nella intranet aziendale/internet può avvenire solo con il consenso dell'interessato.

Per ogni più dettagliata informazione sul tema, il Garante rimanda alle "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità

di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati” (G.U. n. 134 del 12 giugno 2014).

Dati sanitari

È vietata la diffusione di “dati idonei a rivelare lo stato di salute” del lavoratore.

Sul punto il Garante ricorda anche che

- il lavoratore assente per malattia deve consegnare al proprio ufficio un certificato senza diagnosi ma con la sola indicazione dell’inizio e della durata presunta dell’infermità;
- il datore di lavoro non può accedere alle cartelle sanitarie dei dipendenti sottoposti ad accertamenti dal medico del lavoro.

Nel caso di denuncia di infortuni o malattie professionali all’Inail, il datore di lavoro deve comunicare solo le informazioni connesse alla patologia denunciata.

Dati biometrici

Viene ricordato preliminarmente che i “dati biometrici” sono quelli ricavati, ad esempio, dalle impronte digitali o dalla topografia della mano e che tali trattamenti sono già stati esaminati in un apposito provvedimento generale (doc web n. 3556992 e doc web n. 3563006).

Solo in alcuni casi individuati dal Garante, il datore di lavoro può adottare tecnologie biometriche in assenza del consenso del personale, informando, tuttavia, i dipendenti sui diritti, scopi e modalità del trattamento dei loro dati biometrici.

Nel caso in cui la tecnologia biometrica che si vorrebbe adottare non rientri tra i casi semplificati dal Garante, permane l’obbligo per il datore di lavoro di richiedere un’apposita verifica preliminare prima di iniziare il trattamento dei dati.

Posta elettronica aziendale - Internet e Intranet

È onere del datore di lavoro

- adottare idonee misure di sicurezza per assicurare la disponibilità e l’integrità dei sistemi informativi e dei dati, anche per prevenire utilizzi indebiti
- informare, chiaramente e in modo particolareggiato, i dipendenti circa le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengono effettuati controlli anche in accordo con le organizzazioni sindacali, utilizzando ad esempio un disciplinare interno, chiaro e aggiornato affiancato da un’idonea informativa;
- specificare al dipendente quali sono le azioni consentite in internet (es. scaricare file musicali etc.) e le conseguenze, anche di tipo disciplinare, derivanti dall’utilizzo indebito di internet, posta elettronica.

Delicata la gestione dell’attività di controllo sulle attività dei dipendenti in “rete” e sulle email in quanto potrebbero comportare il trattamento di dati sensibili, come le convinzioni religiose, filosofiche, politiche, lo stato di salute o la vita sessuale.

Nello specifico per quanto riguarda le email, ricorda il Garante che i contenuti e le informazioni della posta elettronica sono tutelati costituzionalmente da garanzie di segretezza ma riguardano anche l’organizzazione del lavoro.

Pertanto, potrebbe essere utile e opportuno che il datore di lavoro

- renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori affiancandoli a quelli individuali e
- valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad un uso privato.

Il datore di lavoro, inoltre, può

- mettere a disposizione di ciascun lavoratore apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le “coordinate” di un altro lavoratore

- consentire al lavoratore di delegare un altro lavoratore (fiduciario) in caso di assenze prolungate, a leggere i messaggi di posta e ad inoltrare al titolare del trattamento quelli ritenuti rilevanti per l'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato.
- in caso di assenze non programmate (ad es. per malattia), incaricare altro personale (ad esempio l'amministratore di sistema) di gestire la posta del lavoratore, avvertendo l'interessato e i destinatari; questo può accadere ove il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail).

I controlli del datore di lavoro

I controlli da parte del datore di lavoro per motivi organizzativi o di sicurezza sono leciti solo se sono rispettati i principi di pertinenza e non eccedenza. I sistemi software devono poter cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad internet e al traffico telematico, la cui conservazione non sia necessaria.

Inoltre, i datori di lavoro possono trattare i dati personali del lavoratore, diversi da quelli sensibili, per il legittimo esercizio di un diritto in sede giudiziaria, a fronte della manifestazione di un libero consenso o per un legittimo interesse.

Per quanto concerne il controllo "a distanza" dei lavoratori, sono vietati trattamenti di dati personali mediante sistemi hardware/software in grado di effettuare proprio tali controlli.

Videosorveglianza e geolocalizzazione

Anche per l'uso di strumenti di controllo quali la videosorveglianza e la geolocalizzazione valgono le medesime considerazioni sopra riportate.

Il richiamo, in questo caso, è alle previsioni di cui all'art. 4 dello Statuto dei lavoratori, il quale prevede che gli impianti e le apparecchiature, dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede la direzione territoriale del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti. In alcuni casi la localizzazione geografica può essere utile per rafforzare le condizioni di sicurezza dei dipendenti.

Sarà pertanto necessario adottare misure volte a garantire che le informazioni visibili o utilizzabili dalla app siano solo quelle di geolocalizzazione, impedendo l'accesso ad altri dati, quali ad esempio, sms, posta elettronica, traffico telefonico. I dipendenti, che devono essere adeguatamente informati in merito (ad es., sui tempi e le modalità di attivazione e sui trattamenti di dati effettuati dalle società), dovranno avere ben "visibile" sullo schermo l'icona che indichi quando la funzione di localizzazione è attiva.

La rilevazione dei dati non deve essere continuativa e deve avvenire in modo che l'ultima rilevazione cancelli quella precedente. Infine, si ricorda che prima di attivare il sistema le società devono notificare all'Autorità il trattamento di dati sulla localizzazione.

Restando a disposizione per qualsiasi eventuale chiarimento, ci è gradita l'occasione per porgere i migliori saluti.

Daniela Ghislandi

Dottore Commercialista
Revisore contabile

