Privacy e lavoro

Le regole per il corretto trattamento dei dati personali dei lavoratori da parte di soggetti pubblici e privati

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Privacy e lavoro

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Principi generali

Il datore di lavoro può trattare **informazioni personali** solo se strettamente **indispensabili** all'esecuzione del rapporto di lavoro.

I dati possono essere trattati solo dal **personale incaricato** assicurando **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.

Le informazioni personali trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata dei lavoratori (ad esempio i dati sulla **residenza e i recapiti telefonici**) e dei terzi (ad esempio dati relativi al **nucleo familiare** per garantire determinate provvidenze).

I trattamenti di dati personali devono rispettare il principio di **necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzo di informazioni personali e identificative.

Si deve inoltre rispettare il principio di **correttezza**, secondo cui **le caratteristiche essenziali** dei trattamenti **devono essere rese note ai lavoratori**.

I trattamenti devono essere effettuati **per finalità determinate, esplicite e legittime** in base ai principi di **pertinenza e non eccedenza**.

Il **trattamento** di dati personali anche **sensibili** riferibili 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).

Privacy e lavoro

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Cartellini identificativi

Nelle aziende private e pubbliche il lavoratore può essere dotato di un cartellino di riconoscimento.

Può essere eccessivo riportare per esteso tutti i dati anagrafici o le generalità complete del dipendente: a seconda dei casi **può bastare un codice identificativo** o il solo **nome** o solo **il ruolo professionale**

Comunicazioni

In ambito di **lavoro privato** per comunicare informazioni sul lavoratore ad associazioni di datori di lavoro, ex dipendenti o conoscenti, familiari, parenti occorre il **consenso** dell'interessato.

In ambito di **lavoro pubblico** è richiesta **una norma di legge o di regolamento**.

Bacheche aziendali

Nella bacheca aziendale possono essere affissi **ordini di servizio, turni lavorativi o feriali**.

Non si possono invece affiggere documenti contenenti gli **emolumenti** percepiti, le **sanzioni disciplinari**, le **motivazioni delle assenze** (malattie, permessi ecc.), l'eventuale adesione a **sindacati** o altre **associazioni**

Privacy e lavoro

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

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

In ambito di lavoro privato per pubblicare informazioni personali (**foto**, **curricula**) nella intranet aziendale e, a maggior ragione in internet, occorre il **consenso** dell'interessato.

In ambito di lavoro pubblico, le P.A., possono mettere a disposizione sui propri siti web istituzionali atti e documenti amministrativi (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, solo se la **normativa di settore** preveda espressamente tale obbligo. In tal caso il datore di lavoro pubblico deve selezionare i dati personali da inserire in tali atti e documenti, evitando di divulgare dati eccedenti o non pertinenti, verificando, caso per caso, se ricorrono determinate informazioni che vanno **oscurate** dagli atti e documenti destinati alla pubblicazione.

I soggetti pubblici infatti sono tenuti a ridurre al minimo l'utilizzo di dati identificativi e di tutti gli altri dati personali e ad evitare il relativo trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante **dati anonimi** o altre modalità che permettano di identificare l'interessato solo in caso di necessità.

E' vietata la pubblicazione di qualsiasi informazione da cui si possa desumere lo stato di **malattia** o l'esistenza di **patologie** dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di **invalidità**, **disabilità** o handicap fisici e/o psichici.

In base alla normativa sulla **trasparenza** le P.A. devono pubblicare sui siti istituzionali **curricula**, **emolumenti** o **incarichi** di determinati soggetti (**dirigenti, consulenti, titolari di incarichi di indirizzo politico, ecc.**).

Su questa complessa materia il Garante è intervenuto di recente con **Linee guida** ampie e dettagliate.

Privacy e lavoro

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Dati sanitari

I dati sanitari vanno conservati in **fascicoli separati**.

Il lavoratore assente per malattia è tenuto a 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 limitarsi a comunicare **solo** le informazioni connesse alla **patologia denunciata**.

E' del tutto vietata la diffusione di "dati idonei a rivelare lo stato di salute" del lavoratore.

Privacy e lavoro

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Dati biometrici

Non è lecito l'uso generalizzato e incontrollato dei cosiddetti "dati biometrici" (quelli ricavati ad esempio dalle **impronte digitali** o dalla **topografia della mano**). Questi particolari trattamenti sono stati **esaminati dal Garante in un apposito provvedimento generale** (doc web n. 3556992 e doc web n. 3563006) **in cui sono state previste anche alcune ipotesi di esonero dall'obbligo della verifica preliminare del Garante**.

Le impronte digitali o della topografia della mano, ad esempio, possono essere usate per presidiare gli accessi ad **"aree sensibili"** (processi produttivi pericolosi, locali destinati a custodia di beni di particolare valore e/o alla conservazione di documenti riservati) **oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati; l'impronta digitale o l'emissione vocale possono essere utilizzate per l'autenticazione informatica (accesso a banche dati o a pc aziendali); la firma grafometrica per la sottoscrizione di documenti informatici**. Ciò nel rispetto, in particolare, di rigorose misure di sicurezza specificamente dettagliate nel provvedimento. In alcuni casi individuati dal Garante, nel rigoroso rispetto delle cautele individuate, il datore di lavoro non è tenuto a richiedere il consenso al personale per adottare tecnologie biometriche, ma deve comunque informare i dipendenti sui loro diritti, sugli scopi e le modalità del trattamento dei loro dati biometrici.

Non è generalmente ammessa la costituzione **di banche dati centralizzate ma è preferibile l'utilizzo di altre forme di memorizzazione dei dati, ad esempio in smart card** ad uso esclusivo del dipendente. 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.

Privacy e lavoro

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Uso di internet / intranet e della posta elettronica aziendale

Spetta al 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.

Il **datore di lavoro** ha l'onere di informare, chiaramente e in modo particolareggiato, i dipendenti su quali siano 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**.

I controlli

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 essere programmati e configurati in modo da **cancellare periodicamente ed automaticamente** i dati personali relativi agli accessi ad internet e al traffico telematico, la cui conservazione non sia necessaria.

I datori di lavoro privati e gli enti pubblici economici, 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 riguarda **i datori di lavoro pubblici** il trattamento dei dati del lavoratore è consentito soltanto per lo svolgimento delle **funzioni istituzionali**, in base al **Codice privacy**, **alle leggi e ai regolamenti**.

Privacy e lavoro

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Internet/Rete interna

Va specificato con chiarezza se **la navigazione in Internet** o la gestione di file nella rete interna **autorizzi o meno** specifici **comportamenti** come il download di software o di file musicali o l'uso dei servizi di rete con finalità ludiche o estranee all'attività lavorativa.

Occorre anche specificare quali **conseguenze**, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica o la rete internet sono utilizzate indebitamente.

Il datore di lavoro per ridurre il rischio di usi impropri di Internet può adottare **opportune misure** che possono prevenire **controlli** successivi sul lavoratore, che possono risultare leciti o meno a seconda dei casi e possono comportare il trattamento di dati sensibili, come le convinzioni religiose, filosofiche, politiche, lo stato di salute o la vita sessuale.

Ad esempio si possono **individuare i siti** correlati o meno alla prestazione lavorativa o configurare **sistemi o filtri** che prevengano determinate operazioni.

Privacy e lavoro

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Posta elettronica aziendale

I contenuti e le informazioni della **posta elettronica** sono tutelati costituzionalmente da garanzie di **segretezza** ma riguardano anche **l'organizzazione del lavoro**.

In questo quadro è opportuno che il datore di lavoro renda disponibili **indirizzi di posta elettronica condivisi** tra più lavoratori (ad es. ufficioreclami@società.com) affiancandoli a quelli **individuali** (ad es. rossi@società.com) e valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad un **uso privato**.

Il datore di lavoro 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.

Si può altresì 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), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il datore di lavoro può incaricare altro personale (ad esempio **l'amministratore di sistema**) di gestire la posta del lavoratore, avvertendo l'interessato e i destinatari.

Privacy e lavoro

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Controllo a distanza dei lavoratori

E' **vietato** ai datori di lavoro privati e pubblici di effettuare trattamenti di dati personali mediante sistemi hardware e software che mirano al **controllo a distanza dei lavoratori**.

Tale divieto vale anche per l'uso di strumenti di controllo quali la **videosorveglianza e la geolocalizzazione**

Videosorveglianza e geolocalizzazione

Non devono essere effettuati **controlli a distanza** al fine di verificare l'osservanza dei **doveri di diligenza** stabiliti per il **rispetto dell'orario di lavoro** e la **correttezza** nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul **badge**).

Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza o la geolocalizzazione sono rese necessarie da **esigenze organizzative o produttive**, o sono richieste per la **sicurezza del lavoro**.

In tali casi, ai sensi dell'art. 4 della l. n. 300/1970, 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 l'Ispettorato del lavoro* [oggi DTL Direzioni territoriali del lavoro], *dettando, ove occorra, le modalità per l'uso di tali impianti"*.

Privacy e lavoro

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Videosorveglianza e geolocalizzazione (2)

In taluni casi la **localizzazione geografica** può essere utile a **rafforzare le condizioni di sicurezza dei dipendenti** permettendo l'invio mirato di soccorsi in caso di difficoltà. Si possono ad esempio utilizzare i dati di localizzazione geografica, rilevati da una **app** attiva sugli **smartphone** in dotazione ai lavoratori, purché vengano adottate adeguate cautele a protezione della loro vita privata. [vedi doc. web n. 3505371 e 3474069].

Occorre infatti 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.

Il sistema deve essere configurato in modo tale che sullo schermo dello smartphone compaia sempre, ben visibile, **un'icona che indichi ai dipendenti quando la funzione di localizzazione è attiva**.

I dipendenti dovranno essere **ben informati** sulle caratteristiche dell'applicazione (ad es., sui tempi e le modalità di attivazione) e sui trattamenti di dati effettuati dalle società.

Sono inoltre necessarie cautele circa la rilevazione dei dati di **geolocalizzazione** che **non deve essere continuativa** e deve avvenire in modo che **l'ultima rilevazione cancelli quella precedente**.

Prima di attivare il sistema le società **devono notificare all'Autorità** il trattamento di **dati sulla localizzazione**.

Privacy e lavoro




GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Documenti di riferimento

Linee guida per il trattamento di dati dei dipendenti privati – 23 novembre 2006
doc. web n. 1364099

Linee guida per il trattamento di dati dei dipendenti pubblici – 14 giugno 2007
doc. web n. 1417809

Linee guida del Garante per posta elettronica e internet – 10 marzo 2007
doc. web n. 1387522

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 – 12 giugno 2014
doc. web n. 3134436

Provvedimento generale prescrittivo in tema di biometria – 12 novembre 2014
doc. web n. 3556992

All. A al Provvedimento 513 del 12 novembre 2014 - Linee-guida biometria
doc. web n. 3563006

Provvedimento in materia di videosorveglianza – 8 aprile 2010
doc. web n. 1712680

Provvedimento Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro – 4 ottobre 2011
doc. web n. 1850581

Provvedimento Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Wind Telecomunicazioni s.p.a. - 9 ottobre 2014
doc. web n. 3505371

Provvedimento Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Ericsson Telecomunicazioni s.p.a. - 11 settembre 2014
doc. web n. 3474069

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Per informazioni presso l'Autorità

Ufficio relazioni con il pubblico
Lunedì-Venerdì, ore 10-13
Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696772917
e-mail: urp@gpdp.it
pec: urp@pec.gpdp.it

A cura del Servizio relazioni
con i mezzi di informazione

Aprile 2015