

La privacy per gli operatori del **nolegg**

Guida pratica agli adempimenti obbligatori per le PMI in tema di trattamento dei dati personali. Un argomento di grande attualità, spesso accompagnato da false credenze

L'obiettivo di questo articolo è quello di fare chiarezza, una volta per tutte, su quali siano gli adempimenti obbligatori per le aziende in materia di trattamento dei dati personali. Il D.Lgs. 196/03, meglio conosciuto come Codice della Privacy, prevede una serie di adempimenti obbligatori (misure minime di sicurezza) la cui mancata adozione è sanzionata anche penalmente. E le prescrizioni normative devono essere rilette alla luce delle ultime pronunce dell'Autorità Garante in materia di trattamento dei dati in azienda, in particolare all'interno delle PMI.

Le misure minime di sicurezza

Il primo, obbligatorio, passo da fare è quello di individuare quali siano le misure minime di sicurezza previste dal Codice della Privacy per tutti i soggetti che trattano dati personali, con il solo limite del trattamento effettuato



da persone fisiche per fini esclusivamente personali.

Innanzitutto il titolare del trattamento (il soggetto cui competono le decisioni in materia di trattamento dei dati) - che è l'azienda se si tratta di persona giuridica o l'imprenditore in caso di impresa individuale - deve provvedere a fornire idonea "informativa" ai soggetti di cui tratta i dati (i c.d. "interes-

sati"). L'informativa, che può anche essere data oralmente, deve contenere una serie di informazioni circa il trattamento dei dati effettuato, come prescritto dall'art. 13 del D.Lgs. 196/2003. L'informativa deve essere data prima dell'inizio del trattamento. Contrariamente a quanto si ritiene, la maggior parte dei rapporti commerciali tra imprenditori non richiedono il



consenso al trattamento dei dati, sempre che i soggetti di cui si trattano i dati siano parti all'interno di contratti o in trattative pre-contrattuali.

Le lettere di incarico

Oltre a questo, il titolare del trattamento deve provvedere a fornire "lettere di incarico" ai soggetti che, per suo conto, trattano dati nell'esercizio delle loro funzioni. Ci riferiamo ai dipendenti, ai collaboratori e ai consulenti che con questi abbiano rapporti continuativi. All'interno delle lettere dovrà essere contenuto l'incarico, le modalità e i limiti con cui dovrà essere effettuato il trattamento e la lettera dovrà essere sottoscritta per accettazione da parte dell'incaricato. Per il personale che per conto dell'azienda tratta anche dati sensibili (volti a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale), per lo più i soggetti che si occupano della gestione delle risorse umane, sarà necessaria anche una esplicita autorizzazione. Il Codice della Privacy prevede poi la figura del "Responsabile del trattamento", che può essere interno o esterno. Il responsabile interno è un soggetto che gestisce le politiche di trattamento dei dati per conto del titolare in strutture particolarmente grandi o complesse. Il responsabile esterno è un soggetto, esterno, appunto, all'organigramma aziendale, che in maniera continuativa tratta in



autonomia una serie di dati per conto del titolare (società di consulenza, commercialista, studio paghe, eccetera). Questi soggetti, la cui nomina è facoltativa, devono essere incaricati con apposita lettera descrittiva di poteri, limiti e responsabilità conseguenti all'incarico.

Adempimenti informatici e di formazione

La legge prevede anche una serie di adempimenti di carattere informatico, anch'essi obbligatori per adempiere alle misure minime. Innanzitutto l'art. 34 del Codice della Privacy prevede l'obbligo di proteggere l'accesso ai dati con l'adozione di "password" di autenticazione personale e le password devono essere soggette ad aggiornamento almeno semestrale. Inoltre, i sistemi informatici devono essere dotati, ove possibile, di programmi "antivirus" e protetti contro

accessi non autorizzati. Infine, è necessario dotare il sistema di procedure per il "backup" dei dati, al fine di non perdere dati personali in caso di malfunzionamento o cancellazione accidentale.

Altro adempimento necessario e prescritto come misura minima è l'adozione di un adeguato "programma di formazione" del personale. Il titolare del trattamento deve programmare sessioni periodiche di formazione e aggiornamento per il proprio personale che effettui trattamento dei dati. Infatti, potrà pretendere determinati comportamenti dal proprio personale e tutelarsi in caso di responsabilità verso i terzi solo se avrà adempiuto in modo completo a tale obbligo.

Il Documento Programmatico sulla Sicurezza

Attualmente la redazione del Documento Programmatico sulla Sicurezza è prevista come obbligatoria solo in caso di trattamento di dati sensibili o giudiziari attraverso sistemi informatici (art. 34 comma 1 lett. g insieme alla regola 19 dell'Allegato B del Codice). Il documento, corredato dei contenuti essenziali indicati all'Allegato B del Codice, deve essere redatto a cura del titolare del trattamento o a mezzo di responsabile incaricato, con cadenza annuale entro il 31 di marzo. I contenuti di cui deve essere dotato, a titolo meramente indicativo, sono



l'elenco dei trattamenti, la distribuzione dei compiti e delle responsabilità, l'analisi dei rischi, le misure adottate, le procedure per il ripristino dei dati e il piano di formazione. Il documento, nel suo complesso, deve rappresentare un quadro il più possibile esauriente dei trattamenti dei dati effettuati, dei rischi a cui sono soggetti, delle misure adottate dall'azienda per minimizzarne gli effetti e dei progetti futuri di miglioramento. Personalmente riteniamo che ogni azienda dovrebbe procedere alla sua redazione, che sia obbligata o meno dalla legge a farlo. Il D.P.S., infatti, è un fondamentale strumento di programmazione e controllo delle politiche di trattamento dei dati e il suo aggiornamento permette alle aziende di compiere un'analisi privacy interna almeno una volta l'anno. Sicuramente questo è un bene, visto il livello medio di adempimento degli obblighi previsti dalla normativa.

Le ultime pronunce del Garante

Da ultimo si vuole sottolineare come, negli ultimi mesi, l'Autorità Garante abbia emanato una serie di provvedimenti che dimostrano una sempre maggiore attenzione verso le problematiche privacy delle aziende, fissando utili linee guida in grado di orientare l'imprenditore nelle scelte operative. A novembre 2006 il Garante ha emesso le "Linee Guida in materia di trattamento dei dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati", con lo scopo di fornire indicazioni e raccomandazioni circa il trattamento dei dati dei lavoratori all'interno di aziende private. Sono stati ricordati i principi generali che devono animare il trattamento (liceità, pertinenza e trasparenza), le finalità per cui sono raccolti i dati devono essere rispettate e sono stati regolati i rapporti col medico aziendale, l'uso di dati biometrici e i limiti per comunicazione e diffusione dei dati personali dei dipendenti. Oltre a questo sono state indicate le misure di sicurezza da adottare all'interno delle aziende in relazione al trattamento dei dati dei dipendenti.

In sintesi

- Le Misure Minime di Sicurezza, adempimenti obbligatori penalmente sanzionati:
 - Informativa preventiva sul trattamento dei dati
 - Lettere di incarico per i soggetti interni che trattano i dati
 - Individuazione di eventuali responsabili esterni del trattamento
 - Misure informatiche: password, antivirus e backup dei dati
 - Formazione del personale in materia di privacy
- Il Documento Programmatico sulla Sicurezza dei dati: obbligatorio solo per chi tratta dati sensibili su rete informatica. Ma è un valido strumento di controllo per l'imprenditore.
- Ultime pronunce del Garante: massima attenzione al mondo delle imprese in relazione ai dati dei dipendenti, all'uso di Internet e posta elettronica e alla semplificazione degli adempimenti per le PMI.

A marzo 2007 sono state emanate le "Linee Guida del Garante per posta elettronica e Internet", con l'intento di fare chiarezza sull'utilizzo dei mezzi di comunicazione aziendale e i relativi poteri di controllo del datore di lavoro. In passato alcune pronunce di merito avevano concesso il potere al datore di lavoro di accedere alla casella di posta aziendale del dipendente senza alcun limite, motivando tale potere col fatto che la "mailbox" fosse un bene materiale di proprietà dell'azienda. Le Linee Guida invece limitano tale potere di controllo, anche in materia di "log file Internet", e impongono al titolare di procedere alla redazione di un disciplinare interno che regoli l'uso di tali strumenti e i relativi controlli. Il provvedimento ribadisce il divieto di installare apparecchiature la cui unica finalità sia quella di controllare a distanza i dipendenti mentre ammette, previo assenso di lavoratori e rappresentanze sindacali, quelli che svolgono controlli indiretti, purché giustificati da esigenze produttive. Oltre a questo deve essere individuato dal dipendente stesso un collega "fiduciario", delegato all'apertura della posta elettronica in sua assenza e in caso sia necessario visionarla, la procedura dovrà essere verbalizzata. Il denominatore comune di tutto il provvedimento è l'ostilità del Garante verso controlli personali successivi del comportamento del lavoratore, mentre devono essere preferiti regolamenti preventivi in grado di evitare l'uso

scorretto di tali strumenti di lavoro quotidiano.

Infine, deve essere fatto cenno al recentissimo provvedimento dal titolo "Guida pratica e semplificazione per le piccole e medie imprese". Lo scopo del documento è quello di chiarire alcuni punti circa gli adempimenti obbligatori e cercare di "semplificare la vita" alle piccole e medie imprese.

La Guida si apre con una serie di precisazioni terminologiche circa le figure del titolare del trattamento, del responsabile e degli incaricati ma non aggiunge nulla di nuovo a quanto già contenuto nel Codice della Privacy. In seguito tratta della notificazione al Garante, oggi non più obbligatoria se non in casi specifici, e poi di informativa e consenso al trattamento.

Anche qui si precisa che il consenso, nella prassi dei rapporti commerciali, il più delle volte non è necessario. Il provvedimento poi rivolge la sua attenzione al documento programmatico sulla sicurezza e al trasferimento dei dati all'estero, anche qui non aggiungendo alcun elemento di novità rispetto alla normativa vigente.

Può essere molto utile per l'imprenditore prendere visione della Guida perché, in termini molto semplici e diretti, aiuta a comprendere quali siano gli adempimenti obbligatori facendo chiarezza su alcuni punti effettivamente suscettibili di fraintendimento. La normativa aggiornata può essere reperita sul sito www.garanteprivacy.it. 