CIRCOLARE n. 3/2007
RISERVATA AI CLIENTI E AI CORRISPONDENTI DELLO STUDIO GHIDINI, GIRINO & ASSOCIATI
www.ghidini-associati.it
(N.B. La presente circolare è meramente informativa e non costituisce parere)

PRIVACY E PICCOLE-MEDIE IMPRESE: LE LINEE GUIDA DEL GARANTE

Delibera del Garante per la protezione dei dati personali 24 maggio 2007 – Approvazione del documento "Guida pratica e misure di semplificazione per le piccole e medie imprese"

1. La disciplina

Approvato con delibera 24 maggio 2007 del Garante per la protezione dei dati personali il documento "**Guida pratica e misure di semplificazione per le piccole e medie imprese**" (pubblicato sulla G.U. n. 142 del 21 giugno 2007 e consultabile sul sito www.garanteprivacy.it, nel seguito **la Guida**).

Il documento si propone di fornire agli operatori del settore un *vademecum* operativo avente un **mero valore indicativo ed esemplificativo** rispetto alle disposizioni del d. lgs. 196/2003 – Codice in materia di protezione dei dati personali (nel seguito, Codice Privacy), attraverso la presentazione di **risposte a quesiti pratici** in materia di coordinamento tra tutela dei dati personali e concreta operatività aziendale e di una ***check list*** da utilizzarsi quale strumento di auto-valutazione dell'effettivo livello di adeguamento dell'impresa alle prescrizioni di legge.

La Guida è suddivisa in sette capitoli, ciascuno avente ad oggetto una specifica area tematica inerente la concreta applicazione della normativa *privacy* nelle piccole e medie imprese (soggetti del trattamento, notifica del trattamento, informativa ai soggetti interessati, consenso al trattamento, misure di sicurezza, trasferimento di dati personali in paesi terzi, diritti degli interessati).

2. Soggetti

Nel primo capitolo, il Garante procede sulla base delle definizioni del Codice Privacy alla concreta individuazione dei **soggetti del trattamento** nell'ambito del normale svolgimento dell'attività delle piccole e medie imprese:

(a) **titolare del trattamento**: è il soggetto, persona fisica (es. l'imprenditore individuale) o giuridica (es. la società), che procede al trattamento dei dati personali e che è chiamato ad attuare gli obblighi di cui alla normativa *privacy*;

(b) **responsabile del trattamento**: viene nominato dal titolare del trattamento in presenza di articolazioni produttive dotate di una certa autonomia (es. dirigenti di funzioni aziendali del personale o del settore *marketing*) o, con riferimento a soggetti esterni all'impresa, in caso di ricorso a tecniche di *outsourcing* che implichino il trattamento di dati personali (es. centri di elaborazione dati contabili, società di recupero crediti). La nomina – in ogni caso facoltativa – deve risultare da atto scritto;

(c) **incaricato del trattamento:** è individuato come il soggetto che materialmente effettua le operazioni di trattamento dei dati personali, operando sotto l'autorità del titolare (o del responsabile, se nominato) e attenendosi ad istruzioni scritte (cfr. art. 30 Codice Privacy). Al riguardo, il Garante precisa che per il rispetto della normativa è sufficiente l'assegnazione di un dipendente ad una unità organizzativa, a condizione che le categorie di datti cui il medesimo può avere accesso e gli ambiti del trattamento risultino da espressa previsione scritta.

3. Notifica del trattamento

Di particolare rilievo appare in materia di notifica del trattamento (mediante la quale il titolare comunica al Garante, in via preventiva, l'esistenza di un'attività di raccolta ed impiego di dati personali) la precisazione contenuta nel capitolo 2 della Guida, per cui in linea di principio i **trattamenti ordinari di dati personali** svolti nell'ambito della prassi aziendale delle piccole e medie imprese (con riferimento, ad esempio, a **dati di clienti, fornitori o dipendenti**) **non vanno notificati**. In particolare, deve escludersi la notifica anche per il trattamento dei dati relativi agli inadempimenti della propria clientela raccolti da ciascuna impresa.

In questo contesto, il Garante individua le ipotesi di trattamento da parte delle PMI che, ai sensi dell'art. 37 del Codice Privacy, sono invece soggetti all'obbligo di notificazione:

(a) dati relativi al rischio sulla solvibilità economica, alla situazione patrimoniale, a comportamenti illeciti o fraudolenti;

(b) dati genetici, biometrici o che in ogni caso permettono di localizzare la posizione geografica di persone o oggetti;

(c) dati trattati con strumenti elettronici volti alla definizione del profilo o della personalità degli interessati o all'analisi delle abitudini o scelte di consumo (c.d. profilazione);

(d) dati sensibili registrati a fini di selezione del personale per conto terzi o per sondaggi d'opinione o ricerche di mercato.

4. Informativa ai soggetti interessati

Il Garante specifica nel capitolo 3 i caratteri dell'informativa sul trattamento, che a norma dell'art. 13 Codice Privacy deve essere effettuata - prima dell'inizio del trattamento - nei confronti degli interessati. L'informativa, si legge, deve essere resa con **chiarezza** e senza inutili formalità, anche in modo **sintetico e colloquiale**.

Per quel che concerne, in particolare, i dati di **dipendenti, clienti e collaboratori**, l'Autorità ha cura di precisare che l'informativa non deve essere resa in occasione di ogni contatto: è sufficiente infatti che la medesima sia resa con una formulazione di carattere generale al momento dell'inizio del rapporto.

E' poi espressamente ammessa la possibilità di rendere agli interessati l'informativa in **forma semplificata,** anche oralmente o utilizzando uno spazio all'interno dell'ordinario materiale cartaceo e della corrispondenza.

5. Consenso dell'interessato

Il capitolo 4 della Guida si sofferma sulle ipotesi in cui, ai sensi dell'art. 24 Codice Privacy, il trattamento di **dati personali** non richiede il preventivo consenso degli interessati. Si tratta di fattispecie concernenti, fra l'altro, l'adempimento di obblighi contrattuali o di legge e il trattamento di dati provenienti da elenchi pubblici o relativi allo svolgimento di attività economiche.

Con riferimento, viceversa, al trattamento **di dati sensibili** (vale a dire quelli concernenti informazioni idonee a rivelare l'origine razziale o etnica, le convinzioni religiose o filosofiche, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazione a carattere religioso, filosofico, politico o sindacale, nonché dei dati personali idonei a rivelare lo stato di salute o l'identità sessuale), il Garante, dopo aver ribadito che, in linea di principio, il medesimo presuppone sempre sia il consenso scritto dell'interessato che l'autorizzazione dell'Autorità di controllo, ha cura di precisare che in concreto quest'ultima difficilmente si renderà necessaria,
avendo l'Authority già rilasciato **sette autorizzazioni generali** che comprendono tutti i trattamenti normalmente effettuati nell'ambito della normale operatività PMI (in particolare, rapporti di lavoro, stato di salute e vita sessuale, trattamento da parte di associazioni e fondazioni, liberi professionisti, investigatori privati e altre categorie di titolari; trattamento di dati a carattere giudiziario da parte di privati, enti pubblici economici e soggetti pubblici).

6. Misure di sicurezza

Quanto all'obbligo del titolare del trattamento di apprestare misure di sicurezza idonee a ridurre i rischi di distruzione o perdita anche accidentale dei dati o di accesso non

autorizzato o non consentito ai medesimi, il Garante fornisce una interpretazione qualificata dell'art. 34, comma 1, lett. g) del Codice Privacy, pervenendo ad affermare che la redazione del **Documento Programmatico per la Sicurezza (DPS)** si rende necessaria per le PMI esclusivamente nelle ipotesi di **trattamento di dati sensibili e giudiziari attraverso sistemi informatici**. Ferma restando la valenza meramente indicativa delle linee-guida, l'affermazione del Garante è particolarmente significativa se si considera che l'interpretazione letterale della disposizione deporrebbe, viceversa, nel senso di una estensione dell'obbligo di redazione del DPS.

Occorre peraltro dare atto, sul punto, che l'art. 29 comma 1 del disegno di legge sulle liberalizzazioni, attualmente al vaglio delle Camere, in materia di dati personali trattabili senza il consenso degli interessati esclude dalla soggezione agli obblighi di sicurezza le piccole imprese e quelle con numero di addetti inferiore a quindici. L'eventuale conferma di siffatta semplificazione in sede di promulgazione determinerebbe, con tutta evidenza, l'automatica caducazione delle indicazioni formulate nella Guida in materia di misure di sicurezza.

7. Trasferimento di dati personali in Stati extra UE

Per quel che concerne, poi, il trasferimento di dati all'estero, l'Authority precisa che la disciplina dettata dagli artt. 43 ss. del Codice Privacy trova applicazione principalmente con riferimento ai **flussi di dati personali nei confronti degli Stati non facenti parte dell'Unione Europea**, considerato che gli Stati membri, in attuazione della direttiva 95/46/CE, hanno adottato specifiche normative in materia di protezione dei dati personali, il cui rispetto è considerato idoneo per il trasferimento dei dati all'interno della UE (art. 42 Codice Privacy).

8. Diritti degli interessati ai sensi dell'art. 7 del Codice Privacy

Nel capitolo conclusivo della Guida, in materia di **diritto di accesso e altri diritti riconosciuti agli interessati dall'art. 7 del Codice Privacy** e dei correlativi oneri posti in capo al titolare (o al responsabile) del trattamento, la Guida si limita a richiamare – senza fornire alcuna interpretazione "mirata" in favore degli operatori del settore PMI - le disposizioni di legge.

STUDIO GHIDINI, GIRINO E ASSOCIATI
Via S. Sofia 12 - 20122 Milano (Italia)
Tel. 0258300433 Fax 0258301508
URL: www.ghidini-associati.it