LINEE GUIDA PER L'APPLICAZIONE DELLA NORMATIVA SULLA PRIVACY

Decreto Legislativo 30 giugno 2003 n.196

Aggiornamento Aprile 2012

ACTA Area Software

www.actaareasoftware.com

LE PRESENTI LINEE GUIDA SI RIVOLGONO ESSENZIALMENTE A:

- Piccole e Medie Imprese
- Liberi Professionisti
- Artigiani

Per altre attività come i soggetti pubblici o specifici settori che trattano dati particolari per tipo, quantità e modi, sono necessari approfondimenti specifici.

SCOPO DELLA LEGGE

Proteggere i dati personali ed evitarne la diffusione.

- **DATI PERSONALI**: qualunque informazione relativa a persona fisica e NON a persona giuridica
- **DATI SENSIBILI:** quelli relativi a origine razziale o etnica, stato di salute, vita sessuale, scelte politiche, religiose o ideologiche, ecc.
- **DATI GIUDIZIARI:** quelli relativi ai provvedimenti giudiziari, carichi pendenti, sanzioni amministrative da reato, posizione di imputato o indagato, ecc.

CHI DEVE METTERSI IN REGOLA

TUTTI !

- Non esiste attività economica che non tratti dati personali

COME DEVONO ESSERE TRATTATI I DATI

- In modo lecito e secondo correttezza.
- Raccolti per scopi determinati, espliciti e legittimi.
- Esatti.
- Pertinenti e non eccedenti rispetto alle finalità.
- Conservati per un periodo non superiore agli scopi previsti.

I RUOLI

IL TITOLARE DEL TRATTAMENTO DATI

E’ sempre il titolare o i titolari dell’attività in quanto a lui competono le decisioni sulle finalità del trattamento dati.

Non può essere demandato ad altri.

IL RESPONSABILE DEL TRATTAMENTO DATI

- E’ preposto alla corretta applicazione della normativa.
- La nomina del responsabile in ogni caso non esonera le responsabilità del titolare e non è obbligatoria.
- Può essere anche una persona giuridica.

GLI OPERATORI O INCARICATI

Sono le persone fisiche che accedono ai dati, sia informatizzati che non informatizzati.

- Le nomine devono essere scritte ed accettate.
- Gli incaricati devono essere istruiti, formati e seguire procedure scritte.
- Devono firmare un obbligo di riservatezza sui dati trattati.

GLI INTERESSATI

Sono le persone fisiche a cui si riferiscono i dati personali.

GLI AMMINISTRATORI DI SISTEMA

Sono tutti coloro che si occupano della gestione e manutenzione del sistema informatico.

- Attenzione: hanno un accesso privilegiato ai dati.
- Devono essere nominati e identificati in forma scritta.
- I loro accessi devono essere registrati.

LE MISURE MINIME DI SICUREZZA

IL TITOLARE È TENUTO AD ADOTTARE IDONEE MISURE DI SICUREZZA PER RIDURRE AL MINIMO I RISCHI DI:

- perdita dei dati
- accesso non autorizzato
- trattamento non consentito
- trattamento non conforme

Sono le normali misure di sicurezza da adottare anche per salvaguardare il proprio lavoro

IL TRATTAMENTO INFORMATIZZATO DEI DATI

- Ogni incaricato deve avere il proprio account e la propria password esclusiva e riservata per accedere ai dati
- Usare sempre password di almeno 8 caratteri
- Cambiare le password periodicamente
  - 3 mesi per dati sensibili o giudiziari
  - 6 mesi per dati normali
- Salvaschermo automatico con sblocco con password

IL TRATTAMENTO INFORMATIZZATO DEI DATI

- Stabilire procedure di archiviazione e di sicurezza.
- Impostare partizioni e/o cartelle ad accesso riservato.
- Accesso ai dati sensibili ai soli autorizzati, meglio se cifrati.
- Fare ciclicamente il backup dei dati, almeno settimanale.
- Copie di backup con accesso protetto e/o cifrato.
- Utilizzare antivirus aggiornati e firewall.
- Usare i gruppi di continuità, come minimo sul server

IL TRATTAMENTO INFORMATIZZATO DEI DATI

- Determinare le procedure di utilizzo dei computer, della rete dati, della posta elettronica e di Internet.
- Stabilire chi è responsabile, di che cosa e come.
- I **consulenti informatici** esterni per l'applicazione delle misure di sicurezza devono rilasciare una descrizione scritta dell'intervento effettuato che ne attesta la **conformità** alle disposizioni della normativa.

L'ARCHIVIO CARTACEO

- Nei luoghi non aperti al pubblico o presidiati bastano le classiche scaffalature a giorno.
- Nei luoghi non presidiati (sale d'aspetto, corridoi di passaggio) servono armadi chiusi a chiave.
- Non bisogna scrivere dati personali sulla costa dei faldoni.
- Per i dati sensibili armadi chiusi a chiave o ripostigli con serratura con accesso ai soli autorizzati e con procedure di trattamento definite.

LA SICUREZZA DEI LUOGHI

- Le misure dovranno essere proporzionate al tipo di dati posseduti.
- Basta garantire quel minimo di sicurezza contro eventuali intrusioni, non esistono regole, ma:
  - Porta blindata
  - Grate alle finestre
  - Cavetti d'acciaio per computer e hard disk
  - Videosorveglianza
- Non dimenticare le misure antincendio.
- Copie di backup in luoghi sicuri, meglio se altrove.

LE ATTREZZATURE IN COMUNE

- L'utilizzo del fax posto nel corridoio o del plotter e della stampante condivisa deve essere regolamentato.
- Gli utilizzatori delle attrezzature comuni devono rilasciare l'uno all'altro apposita garanzia scritta sul non utilizzo dei dati e un obbligo di riservatezza sugli stessi.
- Non posizionare attrezzature che possano rivelare dati personali in luoghi accessibili al pubblico.

LE COMUNICAZIONI

- **L'INFORMATIVA SULLA PRIVACY**

  - Bisogna sempre informare gli interessati prima di trattarne i dati personali.
  - L'informativa deve essere semplice e non burocratica.
  - L' informativa può essere orale o scritta.

IL CONSENSO

Per trattare i dati personali di chiunque bisogna per prima cosa chiederne il **consenso**.

NON SEMPRE

- quando i dati derivano da un rapporto contrattuale come per i clienti, fornitori, collaboratori, ecc.;
- quando i dati sono trattati solo per ordinarie finalità amministrativo-contabili;
- quando derivano da pubblici registri come l'elenco del telefono, siti Internet o simili;
- quando vanno trattati per un obbligo di legge.

SEMPRE

- Per iscritto quando i dati trattati sono sensibili;
- quando si vogliono comunicare i dati a terzi;
- quando si vogliono inviare comunicazioni commerciali.

ACTA Area Software
www.actaareasoftware.com

L'INFORMATIVA E IL CONSENSO

- L’unica prova di essere stati autorizzati al trattamento dati in caso di contenzioso è:

l’informativa con il consenso firmato dall’interessato

- Un’informativa breve può essere riportata nella prima comunicazione con l’interessato, o nel preventivo, nelle fattura, nelle email:

“Utilizziamo - anche tramite collaboratori esterni - i dati che la riguardano esclusivamente per nostre finalità amministrative e contabili, anche quando li comunichiamo a terzi. Informazioni dettagliate, anche in ordine al suo diritto di accesso e agli altri suoi diritti, sono riportate su…”

LA CANCELLAZIONE E IL BLOCCO DEI DATI

Chiunque può chiedere, dei propri dati personali, ed in ogni momento:

- la rettifica;
- l'aggiornamento;
- il blocco;
- la cancellazione.

- La legge prevede che sia utilizzato un software per una veloce ricerca e cancellazione.
- E' **obbligatorio** rilasciare un **attestato** agli interessati.

I SOGGETTI TERZI

I dati personali raccolti nel proprio trattamento dati possono essere affidati a soggetti terzi ma rimangono sempre sotto la propria tutela e responsabilità.

- Alcuni esempi di soggetti terzi:
  - consulenti del lavoro
  - commercialisti
  - medici competenti
  - gestori di siti web dinamici e newsletter

IL COMMERCIALISTA

- Se si trattano solo dati amministrativo-contabili e/o si è autorizzate a comunicare i dati a terzi, questi possono affidati al commercialista che deve essere nominato responsabile del trattamento e deve rilasciare una garanzia scritta sull'applicazione della normativa sulla privacy e un obbligo di riservatezza sui dati stessi.

LA COPISTERIA

- Se affidate i vostri documenti ad una copisteria qualcuno potrebbe venire a scoprire del progetto riservato di un vostro cliente, ne siete in ogni caso responsabile voi.
- La copisteria deve rilasciare una garanzia scritta sul non trattamento dei dati che possono anche casualmente essere letti, sull'applicazione della normativa sulla privacy e un obbligo di riservatezza sui dati stessi.

L'IMPRESA DI PULIZIE

- L'impresa deve rilasciare al titolare una garanzia scritta sul non trattamento dei dati che possono anche casualmente essere letti, sull'applicazione della normativa sulla privacy e un obbligo di riservatezza sui dati stessi.
- È necessario identificare il personale dell'impresa di pulizia che accede al vostro studio.

I DOCUMENTI

LE NOMINE

Effettuare in forma scritta le nomine di:

- Responsabili dei trattamenti
- Incaricati
- Amministratori di sistema
- Responsabili "esterni" dei trattamenti

Le nomine devono contenere istruzioni e procedure

IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

- Nel 2012 il DPS è stato **abrogato.**

- In ogni caso tutte le misure di sicurezza e le procedure previste dalla normativa, e che erano riportate anche nel DPS, devono continuare ad essere rispettate.

IL DISCIPLINARE

Consegnare ad ogni collaboratore, consulente, dipendente un disciplinare su:

- linee guida sulla privacy
- uso dei computer
- navigazione in Internet
- uso della posta elettronica
- uso personale di computer, posta e attrezzature
- procedure di archiviazione non informatizzata
- controlli per la privacy

ESPORRE IL DISCIPLINARE

I DOCUMENTI DA CONSERVARE

- Non deve essere presentato o consegnato alcun documento a nessun ente o autorità.
- È utile avere un faldone dove inserire, conservare ed aggiornare periodicamente tutti i documenti prodotti sulla privacy.
- In caso di controllo è opportuno aver predisposto un **Documento sulla Privacy** riassuntivo sulle misure minime di sicurezza adottate per dimostrare l'adeguamento alla normativa.

LA NOTIFICAZIONE AL GARANTE

Deve essere fatta solo per casi specifici

Ad esempio per chi tratta:

- dati genetici e biometrici
- dati GPS o altra localizzazione geografica
- profili degli interessati (personalità)
- dati sensibili per indagini per conto terzi
- rischi di solvibilità economica, frodi, illeciti, situazione patrimoniali, inadempimenti generale di obbligazioni trattati con banche dati elettroniche

LE SCADENZE

- Non c'è ne sono più !
- Bisognava essere a norma già dal 31.3.2006

LE SANZIONI PRINCIPALI

- Varie sanzioni amministrative da €1.000 fino a €180.000.
- Per la mancata adozione delle misure minime di sicurezza: da €4.000 a €45.000 e fino a 2 anni di reclusione.
- Omessa o inidonea informativa: da €2.400 a €36.000.
- Trattamento illecito: fino a 3 anni di reclusione.

ATTENZIONE A:

- i computer lasciati accesi senza salvaschermo e password;
- i documenti consegnati a terzi;
- le nomine e gli obblighi di riservatezza non firmati;
- i documenti sensibili o giudiziari accessibili a chiunque o appallottolati nel cestino;
- la fattura del consulente informatico senza l'attestato di conformità;
- il ciclo di backup disattivato;
- il server e le copie di backup non sufficientemente protetti;
- il disciplinare non esposto nel luogo di lavoro;
- l'utilizzo della videosorveglianza.

LA NOSTRA SOLUZIONE

ACTAPRIVACY

Trattamento informatizzato dei dati conforme alla normativa sulla privacy

Soluzione per la gestione dei nominativi e delle risorse coinvolte nei propri progetti, pratiche e commesse, e di tutti gli aspetti della privacy della propria organizzazione e degli altri trattamenti dati oltre ACTAPRIVACY.

ACTA
Area Software

www.actaareasoftware.com