PRIVACY E VOLONTARIATO - MISURE DI SICUREZZA

Premessa.

L'art. 15 della legge n. 675/96 (nota come "legge sulla privacy") ha stabilito che tutti i soggetti che operano un trattamento di dati personali devono attuare particolari procedure di sicurezza per ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Con il DPR n. 318/1999 erano state definite le misure minime di sicurezza, da attuare entro il 29/3/2000. Il loro mancato recepimento può comportare l'applicazione di sanzioni penali ai sensi dell'art. 36 della legge sulla privacy (reclusione fino a due anni !).
Il termine del 29/3/2000 per molti operatori è risultato troppo "stretto" e pertanto prima della scadenza del termine si è cominciato a parlare di una proroga, che dopo un iter alquanto travagliato è stata accordata con una legge approvata il 10/10/2000 e non ancora pubblicata sulla Gazzetta Ufficiale e con la quale il termine per l'applicazione delle misure minime di sicurezza è stato spostato al 31/12/2000, previo compimento di un particolare atto.
In funzione di ciò, riepiloghiamo gli adempimenti da effettuare per regolarizzare la propria situazione in materia.

Oggetto del provvedimento.

Le misure di sicurezza da adottare riguardano gli archivi che contengano dati personali (quali ad esempio i nostri schedari dei donatori), sia che vengano gestiti in modo cartaceo che attraverso procedure automatizzate (a mezzo computer).
Ricordiamo che per dato personale la legge indica qualunque informazione relativa a persona fisica, giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Tra i dati personali una particolare attenzione è rivolta ai cosiddetti "dati sensibili", che sono quelli idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni ed organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute, la vita sessuale.

Adempimenti per la sicurezza dei dati.

In tutti i casi è necessario che venga nominato un amministratore di sistema, cioè un soggetto cui viene conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore elettronico o di un sistema di base dati e di consentirne l'elaborazione.
Le misure di sicurezza minime previste sono diverse in base alle singole situazioni. Vediamole separatamente.

Trattamento dei dati personali con strumenti elettronici o comunque automatizzati (a mezzo computer).

Se si utilizzano elaboratori non accessibili da altri elaboratori o terminali (cioè se non c'è una "rete") è previsto che:
1) venga inserita una parola chiave per l'accesso ai dati da parte delle singole persone incaricate del trattamento; ove tecnicamente possibile, tale parola chiave deve essere autonomamente modificabile.
2) In caso di più soggetti incaricati del trattamento e di più parole chiave in uso, deve essere individuato per iscritto un soggetto preposto alla custodia di tali parole chiave.

Se invece gli elaboratori sono "in rete", cioè sono accessibili da altri elaboratori o terminali (ad esempio in caso di collegamento dei nostri schedari con quelli degli ospedali

convenzionati o degli schedari di sezione con quelli delle sedi centrali associative), oltre a quanto previsto ai punti 1 e 2 sopra riportati occorre:
3) assegnare un codice identificativo personale a tutti gli operatori, non riutilizzabile;
4) disattivare tali codici identificativi se si perde la qualifica di operatore o in caso di mancato utilizzo per oltre sei mesi;
(questi due adempimenti non sono richiesti in caso di trattamento di dati sensibili, per i quali vedi oltre).
5) predisporre sistemi di protezione contro le intrusioni esterne (antivirus, ecc.) la cui validità è da
verificare ed aggiornare almeno ogni sei mesi.
In caso di trattamento di dati sensibili occorre autorizzare in maniera specifica gli operatori, individuando altresì gli elaboratori utilizzabili, nel caso gli stessi siano accessibili tramite rete di telecomunicazione disponibile al pubblico (internet, canali telefonici non dedicati). In tale caso è necessario inoltre redigere un documento programmatico per la sicurezza.

Trattamento dei dati personali con strumenti non automatizzati (archivi cartacei)

a) Occorre designare per iscritto gli incaricati del trattamento, prescrivendo che l'accesso ai dati personali sia limitato a quelli strettamente necessari per l'adempimento dei loro compiti;
b) Gli atti e i documenti contenenti i dati personali devono essere conservati in archivi ad accesso selezionato (sale riservate e non stanze aperte al pubblico indistinto) e, se affidate agli incaricati, devono essere conservati e restituiti al termine delle procedure.
Se vengono trattati dati sensibili, oltre ai precedenti punti :
c) i dati affidati ai singoli incaricati, fino alla loro restituzione, devono essere conservati in contenitori con serratura;
d) l'accesso agli archivi deve essere controllato e dopo gli orari di chiusura eventuali soggetti ammessi a consultarli devono essere identificati e registrati.

Termini e modalità della proroga.

I soggetti che non fossero in regola con gli adempimenti sopra riportati alla data del 29/3/2000 hanno l'onere di redigere un documento in cui dichiarino di avere avuto particolari esigenze tecniche ed organizzative che hanno reso necessario avvalersi di un termine più ampio di quello previsto dall'art. 41 comma 3 della legge 675/96 (ricordiamo che si trattava del 29/3/2000), spiegando anche quali sono state tali esigenze (ad esempio la necessità di adeguamenti informatici complessi, la predisposizione di locali adatti alla conservazione in sicurezza di archivi cartacei, ecc.).
Tale documento deve essere redatto entro un mese dall'entrata in vigore della legge di proroga e cioè ex art. 2 della stessa legge approvata il 10/10/2000 entro un mese dalla sua pubblicazione sulla Gazzetta Ufficiale (che ad oggi non è ancora avvenuta).
Il documento deve avere data certa (si può utilizzare il sistema dell'apposizione del timbro datario della Posta sopra il foglio su cui è redatto il documento stesso, previa apposizione di francobollo di posta prioritaria da lire 1200 e la dicitura "AUTOPRESTAZIONE").
I contenuti del documento sono:
- una esposizione sintetica degli accorgimenti già adottati e da adottare, in funzione dei trattamenti di dati svolti sia in forma cartacea che informatizzata, nonché le linee guida che si seguiranno per dare piena attuazione al programma di sicurezza nella gestione dei dati.
Il documento così redatto e con la data certa deve essere conservato presso la sede dell'associazione, a disposizione in caso di controlli dell'Autorità garante per la protezione dei dati personali.
La sua mancata o tardiva predisposizione rende inapplicabile la proroga al 31/12/2000, con conseguente possibile sanzione penale.