Circolare del Settore Amministrazione del 29 Ottobre 2004

OGGETTO: Decreto Legislativo 30 giugno 2003, n.196.

Si premette che il Decreto in oggetto sostituisce la legge 31 dicembre 1996, n.675 sulla "Tutela della persona e di altri soggetti rispetto al trattamento dei dati personali".

Il nuovo codice sulla Privacy impone ad Aziende, Società sportive e Professionisti di adottare le misure minime di sicurezza per il trattamento dei dati personali "sensibili" e l'archiviazione in forma cartacea e/o informatica.

Non c'è dubbio che sia l'Unione che gli affiliati dispongano di dati personali attraverso, ad esempio, l'iscrizione e il tesseramento e che tra questi dati ve ne siano di "sensibili", quali il certificato medico, i certificati dei carichi pendenti, ecc

In generale, tutti i depositari di dati personali sensibili, che li trattino mediante strumenti elettronici, devono adottare misure di sicurezza al fine di ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito dei dati.

Pertanto, possono essere assunte fin d'ora le seguenti precauzioni:
a) - i computers devono essere dotati di password all'accensione;
- sui computers va installato un buon antivirus;
- vanno installati programmi per la protezione delle reti informatiche firewall e programmi spybot anti spyware, particolarmente se collegati in internet;
- avere la licenza per ogni programma acquistato;
- far firmare al socio al momento dell'iscrizione apposita liberatoria;
- prevedere che agli sportelli delle segreterie altri soci non possano udire o vedere le informazioni del socio che in quel momento fornisce propri dati (ad es. separatori, ecc);
- conservare il cartaceo in armadi o cassetti muniti di chiusura o lucchetti, in modo che non possano essere consultati o manomessi.
b) Il personale addetto al trattamento dei dati personali, sensibili, deve essere responsabilizzato e deve garantire il "….buon trattamento dei dati".
c) Tutti i depositari di dati personali sensibili, che li trattino mediante strumenti elettronici, devono redigere, entro il 31 dicembre 2004, un Documento Programmatico di Sicurezza (DPS) da conservare presso la struttura titolare e da presentare in caso di verifica alla Guardia di Finanza (abilitata ad effettuare ispezioni ad hoc) e/o all'Ufficio del Garante della Privacy.
Il Documento deve contenere :
- l'elenco dei trattamenti di dati personali (dati sensibili e giudiziari);
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure adottate per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura titolare.
d) Il titolare dei rapporti nell'organigramma della privacy, deve riferire dell'avvenuta redazione o aggiornamento del DPS.
e) La scadenza del 31 dicembre 2004 deve intendersi come:
- termine ultimo per l'adozione di tutte le "misure minime" non previste dalla precedente disciplina;
- termine ultimo per la redazione o l'aggiornamento del DPS;
- termine ultimo per la predisposizione del documento a data certa per descrivere le obiettive ragioni tecniche che hanno impedito l'adozione immediata delle misure minime;
- termine ultimo per l'adozione, da parte dei soggetti legittimati di nuove misure minime su strumenti

elettronici, non previste dalla precedente disciplina.
f) Le sanzioni :
- il mancato o l'inidoneo invio dell'informativa all'interessato (soggetto cui si riferiscono i dati) sono puniti con la sanzione amministrativa del pagamento di una somma da 3000,00 a 18000,00 €, nei casi meno gravi;
- la mancata adozione delle misure minime di sicurezza è punita con una sanzione penale che va dal pagamento di una ammenda da 10000,00 a 50000,00 €, all'arresto fino a due anni;
- il trattamento dei dati senza il consenso scritto dell'interessato, è un illecito penale, punito con la reclusione da sei a diciotto mesi, nei casi meno gravi;
- la falsità delle dichiarazioni, comunicazioni, notificazioni ed in qualunque atto o documento destinato al Garante della Privacy è un illecito penale, punito con la reclusione da sei mesi a tre anni.
g) Il trattamento dei dati effettuato senza l'ausilio di strumenti elettronici è consentito solo se saranno adottate le seguenti misure minime:
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- previsione di procedure per una idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti (es. archivi chiusi a chiave);
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degliincaricati.

L'Unione resta a disposizione per eventuali ulteriori chiarimenti.