005-2011 Circolare del 24 marzo 2011

Documento programmatico sulla sicurezza: scadenza al 31 marzo

Scade il prossimo **31 marzo** il termine annuale per la redazione e l'aggiornamento del **documento programmatico sulla sicurezza** (DPS), la misura minima di sicurezza prevista, in relazione all'obbligo generale di protezione dei dati personali, dall'art. 34 comma 1 lett. g) e dal punto 19 dell'allegato B) del DLgs. 196/2003, meglio noto come Codice della privacy.

Ai sensi dell'art. 31 del Codice della privacy, i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
Innanzitutto, in merito, si ricorda che l'obbligo di redazione del DPS ricorre in caso di trattamento di dati personali, "**sensibili**" o **giudiziari**, **con strumenti elettronici** (ad esempio, mediante computer).
Per dati "sensibili" si intendono quei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Per quanto riguarda il **contenuto**, il DPS deve contenere idonee informazioni riguardo:

- all'elenco dei trattamenti di dati personali;
- alla distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- all'analisi dei rischi che incombono sui dati;
- alle misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché alla protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- alla descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- alla 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;

- alla 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 della privacy, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, all'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Con l'art. 29 comma 1 del DL 112/2008, che ha aggiunto il comma 1-*bis* all'art. 34 del Codice della privacy, sono state introdotte alcune **semplificazioni** con riguardo ai trattamenti effettuati con strumenti elettronici.

Secondo tale norma, per i soggetti che trattano con strumenti elettronici soltanto dati personali "**non sensibili**" e **come unici dati "sensibili"** quelli costituiti dallo stato di salute o di malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale, l'obbligo di redigere e aggiornare il DPS è sostituito da un'**autocertificazione** in cui si attesta di trattare solo tali dati in osservanza delle altre misure di sicurezza prescritte.

Modalità semplificate sono previste anche per i soggetti pubblici e privati che trattano dati personali unicamente per **correnti finalità amministrative e contabili**, in particolare presso liberi professionisti, artigiani e piccole e medie imprese (sul punto si veda il Provv. del Garante per la protezione dei dati personali datato 27 novembre 2008).

Per la mancata redazione o il mancato aggiornamento del DPS, il Codice prescrive l'applicazione di **sanzioni amministrative e penali**.

Si ricorda ancora che, **nella relazione accompagnatoria del bilancio d'esercizio**, se dovuta, devono essere indicate l'avvenuta redazione o aggiornamento del DPS.

Si resta a disposizione per ogni ulteriore chiarimento.

Cordiali saluti.

dott. Giulio Gastaldello