Sintesi del nuovo contesto normativo per la redazione del Documento Programmatico di Sicurezza per i trattamenti di dati personali

GLORY.IT/G.Marcoccio
Roma, 8 Gennaio 2009

Introduzione

Nel secondo semestre del 2008 in Italia il Legislatore ed il Garante per la privacy sono entrambi intervenuti sulla disciplina relativa alla misure minime di sicurezza, e tra queste hanno posto specifica attenzione al documento programmatico per la sicurezza (DPS), allo scopo di semplificare e ridurre il peso dei relativi adempimenti in determinati contesti applicativi (tipi di trattamenti e finalità, tipologia di enti/organizzazioni).
Questa nota ne analizza brevemente le conseguenze per la redazione del DPS nel caso di società soggette alla legge italiana in materia di protezione dati personali e privacy.

Analisi del nuovo contesto

Il nuovo contesto relativo al DPS è originato da:

(1) l'articolo 29 del decreto legge 25 giugno 2008 n.112, come modificato dalla legge di conversione 6 agosto 2008 n. 133, e dal
(2) punto 2.5 del prospetto di cui alla prescrizione a) del provvedimento a carattere generale del Garante privacy italiano del 27 novembre 2008

Previgente contesto normativo per il DPS

Precedentemente a tali interventi normativi, la redazione del DPS era regolamentata dalla lettera g) del comma 1 dell'art. 34 "Trattamenti con strumenti elettronici" del Codice Privacy (D.Lgs 106/03): in sostanza la tenuta di un aggiornato documento programmatico sulla sicurezza rappresentava una delle misure minime di sicurezza per poter lecitamente effettuare trattamento dati personali con strumenti elettronici. I modi di trattamento erano quelli previsti dall'Allegato B del Codice Privacy, nel quale l'istruzione 19 richiedeva al titolare di un trattamento di dati sensibili o di dati giudiziari di redigere anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni, specificate nei punti 19.1 – 19.8.

Attuale contesto per il DPS

Con gli interventi normativi (1) e (2), la redazione del DPS è ora disciplinata in funzione di determinati trattamenti di alcuni tipi di dati sensibili, e/o trattamenti di dati personali per talune finalità effettuati da soggetti individuati anche in funzione della fascia dimensionale (piccole e medie imprese, …). Pertanto l'obiettivo di semplificazione posto dal legislatore e dal Garante Privacy ha ora determinato questo articolato contesto per la redazione del DPS:

Chi	Cosa in relazione al DPS	Fonti normative
a) Soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione a organizzazioni sindacali o a carattere sindacale	la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell'articolo 47 del Testo unico di cui al del decreto del presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte. (le altre misure sono quelle riferite, come minimo, nell'art.34 comma 1 del Codice Privacy)	(1)
b) Soggetti che svolgono unicamente trattamenti di dati personali per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani	possono redigere un documento programmatico sulla sicurezza semplificato sulla base delle indicazioni di seguito riportate.[1]	(2)
c) Rispetto alla totalità di coloro che svolgono trattamenti dati personali: i soggetti complementari a quelli sopra individuati in a) e b).	La regolamentazione per la redazione del DPS rimane inalterata, come stabilito precedentemente agli interventi (1) e (2)	(1), (2), Codice Privacy e relativo allegato B

Impatti per le società

Si considera, in estrema sintesi, il caso di società soggette alla applicazione del Codice Privacy che trattano dati personali in relazione al business ed ai servizi erogati ai Clienti, oltrechè per correnti finalità amministrative e contabili e per la gestione del rapporto di lavoro con i propri dipendenti e collaboratori. Le società in oggetto solo in pochi casi risultano rientrare nel novero dei liberi professionisti, artigiani e/o piccole/medie imprese. Da notare inoltre che la tipologia del business e dei servizi resi ai Clienti può richiedere un ampio e complesso insieme di trattamenti, distribuito su più realtà organizzative, supportato da una pluralità di sistemi informativi e possono inoltre comportare anche l'elaborazione di dati sensibili, ulteriori a quelli menzionati per il caso a) della tabella. Pertanto è considerato critico, da un punto di vista costi e di esposizione a rischi, procedere all'identificazione di eventuali sottocasi per i quali una organizzazione della società possa, per determinati trattamenti effettuati, rientrare nelle casistiche a) o b) della precedente tabella.

Da notare poi che le semplificazioni o esenzioni relative al DPS vanno commensurate all'effettiva esposizione al rischio che ne può derivare per una azienda nel caso in cui desideri adottarli e ne manchino in realtà i presupposti, ed inoltre devono essere considerate anche in relazione a quanto

[1] "Il documento deve avere i seguenti contenuti:

a) le coordinate identificative del titolare del trattamento, nonché, se designati, gli eventuali responsabili. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento;

b) una descrizione generale del trattamento o dei trattamenti realizzati, che permetta di valutare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento. In tale descrizione vanno precisate le finalità del trattamento, le categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime, nonché i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;

c) l'elenco, anche per categorie, degli incaricati del trattamento e delle relative responsabilità. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento con le relative responsabilità;

d) una descrizione delle altre misure di sicurezza adottate per prevenire i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta."

già predisposto e reso operativo in termini di misure minime implementate. A puro titolo di esempio, la cosiddetta semplificazione della redazione del DPS per il caso b), ha ampi margini di discrezione interpretativa se si confrontano realmente i termini semplificati di (2) con quelli generali e sempre validi di cui al Previgente contesto normativo per il DPS.

Un'ultima considerazione deve poi essere spesa sulle semplificazioni per le misure minime di sicurezza portate, per i casi a) e b) della precedente tabella, dal citato provvedimento generale del Garante. Tali semplificazioni non potrebbero in alcun modo essere realmente applicate agli attuali sistemi informativi in quanto da una parte prospettano un serio passo indietro per la sicurezza minima, oggettivamente assai poco accettabile in una qualunque realtà di impresa che utilizza sistemi informatici/telematici (sistemi antivirus aggiornabili, in alcuni casi, anche ogni 2 anni), dall'altra le misure sono già in essere, anche in conformità ad altri requisiti normativi e standard internazionali, e sarebbe ben più costoso rimuoverle per sostituirle con altre che portano, inoltre, ad un esposizione di rischio maggiore.