DR. ERIC FALZONE – PADOVA 12 DICEMBRE 2008

IL DPS UN OBBLIGO, UN DOVERE O UNA CORTESIA?

Regole per scegliere tra:
Documento Programmatico sulla Sicurezza
e Autocertificazione Privacy

INDICE

1. Introduzione 2
2. Il DPS come Misura Minima di Sicurezza 2
3. DPS o Autocertificazione Privacy? 3
4. DPS Integrale o Semplificato? 5
5. Conclusioni 6

FONTI NORMATIVE E BIBLIOGRAFICHE

Privacy in Azienda: Manuale di Formazione per Titolari, Responsabili e Incaricati (Autore Eric Falzone – Casa Editrice Hoepli Spa) – Codice Civile - Decreto Legislativo 30 giugno 2003, n. 196 e Allegato B) – Decreto Legge 25 giugno 2008, n. 112 coordinato con la Legge di conversione 6 agosto 2008, n. 133 "Disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitivita', la stabilizzazione della finanza pubblica e la perequazione tributaria" - Decreto del Presidente della Repubblica del 28/12/2000 n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" - D.M. 18 aprile 2005 "Adeguamento alla disciplina comunitaria dei criteri di individuazione di piccole e medie imprese" - Provvedimento a Carattere Generale del Garante Privacy del 27 novembre 2008 "Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali"

NOTE LEGALI

Via E. Forlanini 16 – 35136 Padova - Tel. 348-6916273 – Fax 049-9817345

*Web: **www.eucs.it** - E-mail: **eric.falzone@eucs.it***

1. Introduzione

Nel corso del 2008, il legislatore ha apportato significative innovazioni al Codice Privacy, che hanno modificato in maniera rilevante alcuni obblighi in materia di misure minime di sicurezza per determinate categorie di Titolari del trattamento.

In particolare in alcuni casi è stata introdotta, la possibilità di sostituire il Documento Programmatico sulla Sicurezza (DPS) con un documento di autocertificazione, mentre in altri di redigerlo in maniera semplificata rispetto ai requisiti minimi previsti per legge.

Queste novità, descritte purtroppo in maniera non molto chiara dal legislatore, hanno portato ad un radicale mutamento dell'assetto generale del Codice Privacy, con notevoli scompensi interpretativi ed applicativi per i Titolari del trattamento.

Scopo del presente saggio è, quindi, quello di delineare il nuovo quadro normativo di riferimento, al fine di dipanare le controverse questioni interpretative emerse in merito all'obbligatorietà o meno della redazione del Documento Programmatico di Sicurezza quale misura minima di sicurezza.

2. Il DPS come Misura Minima di Sicurezza

In tema di misure minime di sicurezza l'art. 33 del D.lg. 196/03 sancisce che*: "Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31 […] i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo […] volte ad assicurare un livello minimo di protezione dei dati personali."*

Il che significa che il primo e indefettibile obbligo di ogni Titolare è sempre il rispetto di quanto previsto dall'art. 31 del D.lg. 196/03 ovvero il dovere di custodire e controllare i dati personali trattati *"[…] in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita […] di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta."*

All'interno di questo ampio ed inderogabile obbligo generale, si inseriscono poi ulteriori adempimenti di sicurezza, che sono specificatamente definiti per legge e che sono definiti "minimi" in quanto in assenza del loro rispetto è inibito al Titolare un qualsiasi trattamento di dati personali ("*misure minime di sicurezza*").

Le misure minime di sicurezza sono in definitiva delle prescrizioni specifiche - per il trattamento di dati personali con strumenti elettronici (art. 34 del D.lg. 196/03) o senza l'ausilio di strumenti elettronici (art. 35 del D.lg. 196/03) - che devono essere obbligatoriamente adottate dal Titolare secondo particolari modalità tecniche definite per legge (*Disciplinare tecnico in materia di misure minime di sicurezza contenuto nell'allegato B*).

Tra le misure minime di sicurezza obbligatorie per il trattamento di dati personali con strumenti elettronici è compresa la *"tenuta di un aggiornato documento programmatico sulla sicurezza"* (art. 34.1.g del D.lg. 196/03).

Tralasciando le fantomatiche leggende che vogliono il "*Documento Programmatico sulla Sicurezza (DPS)*" a data certa e le problematiche dottrinali relative all'interpretazione sistematica dell'art. 34.1.g del D.lg. 196/03 con la regola 19 dell'Allegato B), la redazione di questo documento non è altro che la semplice descrizione e formalizzazione del "*Sistema di Gestione Privacy Aziendale*" ovvero l'illustrazione delle scelte in materia di protezione di dati personali stabilite in azienda.

Dr. Eric Falzone - Via Forlanini 16 – 35136 Padova - PI: 03928150287
Tel. 348-6916273 - Fax 049-9817345 – Web: www.eucs.it - E-mail eric.falzone@eucs.it

Purtroppo, però, la redazione del DPS invece di essere considerata uno strumento fondamentale per una sana e corretta gestione della politica di sicurezza dei dati personali - e più in generale della sicurezza delle informazioni aziendali – è stata recepita dalle aziende come un "folle e oneroso" obbligo di legge esacrato con manifestazioni degne della migliore tradizione della "commedia cinematografica all'italiana".

Questo "furor di popolo" ha portato, quindi, il legislatore a modificare il Codice Privacy declassando il DPS da documento ufficiale del "Sistema di Gestione Privacy Aziendale" a documento tecnico specifico obbligatorio solo in caso di particolari trattamenti di dati personali.

Questa variazione è stata introdotta con l'art. 29 del D.L. 25 giugno 2008, n. 112 coordinato con la Legge di conversione 6 agosto 2008, n. 133 *"Disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitivita', la stabilizzazione della finanza pubblica e la perequazione tributaria"*, che ha modificato il Codice Privacy inserendo nell'articolo 34 il seguente comma 1-bis:

"Per i 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 ad 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 decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte. In relazione a tali trattamenti, nonché a trattamenti comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante, sentito il Ministro per la semplificazione normativa, individua con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico di cui all'Allegato B) in ordine all'adozione delle misure minime di cui al comma 1."

3. DPS o Autocertificazione Privacy?

A seguito dell'introduzione del comma 1-bis all'art. 34 del D.lg. 196/03, è sopraggiunto un ulteriore annoso e amletico problema per i Titolari: *"Fare il DPS o Non Fare il DPS"*?

Per rispondere a questa inquietante domanda è necessaria un'analisi esaustiva dell'art. 34 comma 1-bis.

In primis tale comma introduce il principio che: *"[…] la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazione […]"* solo per *"[…] i soggetti che trattano […] 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 ad organizzazioni sindacali o a carattere sindacale […]"*.

Per capire la portata di questa innovazione è, quindi, necessario soffermarsi sulla definizione di dato personale sensibile; ai sensi dell'art. 4.1.d del D.lg. 196/03 sono, infatti, sono considerati dati sensibili tutti 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"*.

Dr. Eric Falzone - Via Forlanini 16 – 35136 Padova - PI: 03928150287
Tel. 348-6916273 - Fax 049-9817345 – Web: www.eucs.it - E-mail eric.falzone@eucs.it

Coordinando la definizione di dato personale sensibile con il nuovo principio introdotto dall'art. 34 comma 1-bis, possiamo, quindi, affermare con certezza che sono sicuramente soggetti alla tenuta di un aggiornato DPS tutti quei Titolari che trattano le seguenti categorie di dati personali sensibili con strumenti elettronici:

- *Origine razziale ed etnica di clienti, fornitori e dipendenti*
- *Convinzioni religiose, filosofiche o di altro genere di clienti, fornitori e dipendenti*
- *Opinioni politiche, adesione a partiti, associazioni od organizzazioni a carattere religioso, filosofico e politico di clienti, fornitori e dipendenti*
- *Stato di salute di clienti e fornitori*
- *Stato di salute con indicazione della relativa diagnosi di dipendenti*
- *Vita sessuale di clienti, fornitori e dipendenti*

Sono altresì soggetti alla redazione del DPS tutti i titolari che trattano dati personali giudiziari con strumenti elettronici.

In definitiva, possiamo asserire che sono sottratti all'obbligo della tenuta di un aggiornato DPS, unicamente quei titolari che trattano le seguenti categorie di dati personali con strumenti elettronici:

- *dati personali comuni di clienti, fornitori e dipendenti*
- *dati personali sensibili di dipendenti relativi allo stato di salute o malattia (solo se senza indicazione della diagnosi)*
- *dati personali sensibili di carattere sindacale*

Considerato, però, che ai sensi dell'art. 4.1.a del D.lg. 196/03 per trattamento si intende: *"[…] compiere qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati"* permangono notevoli perplessità sulla reale possibilità di rientrare in una delle categorie per le quali si è esentati dalla redazione del DPS.

Infatti, quanti Titolari si sentono realmente in grado di affermare con certezza, che mai in nessun caso la propria struttura tratta dati personali per cui è prevista la redazione del DPS?
E quanti di questi Titolari sono poi disposti ad ufficializzare tale dichiarazione con la sottoscrizione di una "*Dichiarazione sostitutiva di atto di notorietà ex art. 47 del D.P.R. 445/00*" che in caso di "*dichiarazioni mendaci*" o di "*dati non più rispondenti a verità*" può portare a pesanti sanzioni penali ai sensi dell'art. 76 del D.P.R. 445/00?

La verità è che per poter affermare con certezza di rientrare in una delle categorie esentate dalla redazione del DPS, è necessaria una dettagliata classificazione dei dati personali trattati ed un'esaustiva analisi dei trattamenti effettuati con strumenti elettronici, il che significa in termini pratici svolgere buona parte del lavoro necessario per la redazione del DPS… a questo punto perché non completare l'opera?

Dr. Eric Falzone - Via Forlanini 16 – 35136 Padova - PI: 03928150287
Tel. 348-6916273 - Fax 049-9817345 – Web: www.eucs.it - E-mail eric.falzone@eucs.it

4. DPS Integrale o Semplificato?

Per alcune categorie di Titolari, l'art. 34 comma 1-bis ha previsto la possibilità per *"[…] il Garante, sentito il Ministro per la semplificazione normativa […]" di individuare "[…] con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico di cui all'Allegato B) in ordine all'adozione delle misure minime […]"*.

In ossequio alla disposizione di legge, il Garante Privacy, il 27 novembre 2008, ha provveduto ad emanare il Provvedimento a Carattere Generale denominato *"Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali"* (pubblicato nella G.U. n. 287 del 9 dicembre 2008), con il quale ha definito modalità semplificate per l'applicazione delle misure minime di sicurezza.

Tra le agevolazioni previste dal suddetto provvedimento è compresa anche la possibilità di redigere di un DPS semplificato; Tale facoltà è, però, riservata esclusivamente a quelle categorie di Titolari che rientrino nei seguenti parametri:

1. *siano soggetti alla tenuta di un aggiornato DPS ai sensi dell'art. 34.1-bis*

2. *trattino dati personali "unicamente per correnti finalità amministrative e contabili"*

In particolare tale agevolazione è rivolta alle seguenti categorie di Titolari:

- *piccoli imprenditori ai sensi dell'art. 2083 del Codice Civile ovvero: "[…] i coltivatori diretti del fondo, gli artigiani, i piccoli commercianti e coloro che esercitano un'attività professionale organizzata prevalentemente con il lavoro proprio e dei componenti della famiglia."*

- *piccola e media impresa (PMI) ai sensi dell'art. 2.1 del D.M. 18 aprile 2005 "Adeguamento alla disciplina comunitaria dei criteri di individuazione di piccole e medie imprese" ovvero imprese che "[…] hanno meno di 250 occupati e […] un fatturato annuo non superiore a 50 milioni di euro, oppure un totale di bilancio annuo non superiore a 43 milioni di euro."*

In tutti gli altri casi è, invece, prevista la redazione del DPS in forma integrale secondo le modalità specificate nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali.

Dr. Eric Falzone - Via Forlanini 16 – 35136 Padova - PI: 03928150287
Tel. 348-6916273 - Fax 049-9817345 – Web: www.eucs.it - E-mail eric.falzone@eucs.it

5. Conclusioni

Alla luce di quanto è emerso dall'analisi dell'art. 34 comma 1-bis del D.lg. 196/03 e del Provvedimento a Carattere Generale del Garante Privacy del 27 novembre 2008, si evince che le categorie di Titolari esentate della tenuta di un aggiornato Documento Programmatico sulla Sicurezza sono realmente poche.

Infatti, a seguito della globalizzazione dei mercati e della consistente immigrazione dell'ultimo decennio, appare alquanto improbabile che un'azienda, nel corso del regolare svolgimento della propria attività istituzionale, non incorra in un trattamento di dati personali con strumenti elettronici che possa essere idoneo a rivelare l'origine razziale ed etnica o le convinzioni religiose e politiche o lo stato di salute di qualche interessato.

Bisogna, inoltre, tener conto che per poter affermare con certezza di rientrare in una delle categorie esentate dalla redazione del DPS, è necessaria una dettagliata classificazione dei dati personali trattati ed un'esaustiva analisi dei trattamenti effettuati con strumenti elettronici.

Infine, non bisogna mai dimenticare che in capo al Titolare incombono sempre gli obblighi generali di sicurezza di cui all'articolo 31 del D.lg. 196/03 e gli obblighi relativi alle misure minime di sicurezza di cui all'art. 33 del D.lg. 196/03 per quanto semplificate dal provvedimento del 27 novembre 2008 del Garante Privacy.

Quindi, anche qualora si rientrasse in una delle categorie di Titolari esentate dalla tenuta di un aggiornato DPS, bisognerebbe comunque produrre un documento descrittivo dei dati personali raccolti, dei trattamenti effettuati, delle misure di sicurezza e delle misure minime di sicurezza adottate in azienda, al fine di poter dimostrare in caso di trattamenti illeciti *"[…] di avere adottato tutte le misure idonee a evitare il danno […]"* (ai sensi dell'art. 2050 del Codice Civile) ed evitare in questo modo di incorrere in eventuali richieste di risarcimento.

Per tali motivazioni, appare alquanto privo di senso, ostinarsi a non voler redigere un documento programmatico sulla sicurezza, che se correttamente redatto permette di:

- *monitorare e revisionare periodicamente i processi aziendali di trattamento*
- *aumentare la governance dei sistemi informativi*
- *migliorare la sicurezza delle informazioni aziendali*
- *rendere più efficiente la struttura organizzativa*
- *allocare in maniera ottimale le risorse aziendali*
- *pianificare preventivamente l'impatto privacy delle scelte aziendali*
- *diminuire il rischio di eventuali richieste di risarcimento danni*

Dr. Eric Falzone - Via Forlanini 16 – 35136 Padova - PI: 03928150287
Tel. 348-6916273 - Fax 049-9817345 – Web: www.eucs.it - E-mail eric.falzone@eucs.it