Privacy: le misure minime di sicurezza nel nuovo contesto normativo (DL n. 112/2008)

Introduzione

Il Legislatore con DL n. 112/2008, convertito con modificazioni dalla legge n. 133/2008, 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 (di seguito DPS) con un documento di autocertificazione, mentre in altri di redigerlo in maniera semplificata rispetto ai requisiti minimi previsti per legge.
Queste novità hanno portato a un radicale mutamento dell'assetto generale del Codice Privacy, con notevoli difficoltà interpretative e applicative per i Titolari del trattamento.
Scopo del presente lavoro è, quindi, quello di tracciare il nuovo quadro normativo di riferimento, al fine di chiarire le controverse questioni interpretative emerse in merito all'obbligatorietà o meno della redazione del Documento Programmatico di Sicurezza quale misura minima di sicurezza.

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". Dunque ogni Titolare, nel rispetto di quanto citato dall'art. 31, ha in primo luogo 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 si concretizza la fattispecie penale di omissione delle misure minime e la conseguente responsabilità.
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. 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).
Sorvolando sulle problematiche dottrinali relative all'interpretazione dell'art. 34.1.g del D.lg. 196/03 con la regola 19 dell'Allegato B)[1], 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.
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 oneroso obbligo di legge.
Questo "scontento generale" 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 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

1 Una delle questioni dibattute in dottrina riguarda proprio l'adozione del DPS nell'ambito specifico del trattamento dei dati per via elettronica. In merito si riscontrano due orientamenti: da una parte si sostiene che deve essere adottato solo nel caso di trattamento di dati sensibili e giudiziari e dall'altra che deve essere adottato in ogni caso stante l'obbligo generale sancito dal Codice per il trattamento dei dati personali. Dalla lettura del Decreto appare chiaro come il Legislatore abbia predisposto una tutela più stringente per i dati sensibili e giudiziari rispetto ai dati personali. Sarebbe però incongruente interpretare quanto scritto sul Disciplinare tecnico solo nel senso dell'adozione del DPS in caso di trattamento di dati sensibili e giudiziari. In primo luogo perché si verificherebbe un contrasto tra obbligo generale (sancito dall'art. 34 dove si parla di «dati personali») e obbligo specifico sancito dall'Allegato B (c.d. Disciplinare tecnico) all'art. 19 (in cui si parla di «dati sensibili» e «giudiziari»).
L'art. 34 precisa che la redazione del DPS deve avvenire «nei modi» previsti dal Disciplinare tecnico ma non specifica "in conformità" ossia nei limiti da esso previsti. A mio avviso, dunque, l'art.19 stabilisce semplicemente una indicazione temporale sull'aggiornamento del DPS in caso di trattamento di dati sensibili e giudiziari fermo restando l'obbligo generale di aggiornamento (magari annuale o comunque nel momento in cui si siano verificati cambiamenti) sancito dall'art. 34.

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, può 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 di cui al comma 1".

Autocertificazione Privacy

A seguito dell'introduzione del comma 1-bis all'art. 34 del D.lg. 196/03, è sopraggiunto un ulteriore problema per i Titolari: "Redigere o no il DPS?" Per rispondere a questa 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".
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 dati personali sensibili con strumenti elettronici riferiti a 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 affermare 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, l'ampio significato normativo attribuito all'operazione di trattamento dati[2], 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?

Semplificazione del DPS: Beneficiari

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.

2 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".

Tra le agevolazioni previste dal suddetto provvedimento è compresa anche la possibilità di redigere un DPS semplificato; Tale facoltà è, però, riservata esclusivamente a quelle categorie di Titolari che rientrino nei seguenti parametri siano soggetti alla tenuta di un aggiornato DPS ai sensi dell'art. 34.1-bis e 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.

Trattamento dati con strumenti elettronici

Le principali novità per i trattamenti effettuati con strumenti elettronici sono elencate di seguito:
Le istruzioni agli incaricati del trattamento (dipendenti e collaboratori) possono essere impartite anche oralmente (non c'è bisogno di istruzioni scritte), con indicazioni di semplice e chiara formulazione.
Per l'accesso ai sistemi informatici si può utilizzare un qualsiasi sistema di autenticazione basato su un codice per identificare chi accede ai dati (di seguito, «username»), associato a una parola chiave (di seguito: «password»). Lo username deve individuare una sola persona, evitando che soggetti diversi utilizzino codici identici e la password deve essere conosciuta solo dalla persona che accede ai dati.
L'username deve essere disattivato quando l'incaricato non ha più titolo per accedere ai dati (trasferimento, cessazione dal servizio). Non è prevista espressamente la scadenza automatica per non uso semestrale.
È valida anche la procedura di login disponibile sul sistema operativo delle postazioni di lavoro connesse a una rete. Non si prevede espressamente l'obbligo di almeno otto

caratteri per la password e non se ne prevede l'obbligo di modifica con cadenza trimestrale (per i dati sensibili) o semestrale (per i dati comuni).
Se manca il titolare della password, il titolare può assicurare la disponibilità di dati o strumenti elettronici con procedure o modalità predefinite: Dunque al titolare deve essere data una informativa preventiva su come accedere ai dati in assenza del dipendente (ad esempio con l'opzione di inoltro peri messaggi di posta elettronica).
Non si prevede espressamente il meccanismo della nomina del custode delle credenziali (è ammesso qualsiasi procedura purché predefinita e conosciuta dagli incaricati del trattamento).
Le autorizzazioni, necessarie per diversificare l'ambito del trattamento consentito, possono essere assegnate agli incaricati anche tramite un sistema di autorizzazione o funzioni di autorizzazione incorporate nelle applicazioni software o nei sistemi operativi. Non si prevede espressamente un obbligo di verifica annuale delle condizioni legittimanti la sussistenza della autorizzazione. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici (ad esempio, antivirus), anche con riferimento ai programmi anti intrusione (articolo 615-quinquies del codice penale), e a correggerne difetti, sono effettuati almeno annualmente (e non più semestralmente). Se il computer non è connesso a reti di comunicazione elettronica accessibili al pubblico (linee Adsl, accesso a Internet tramite rete aziendale, posta elettronica), l'aggiornamento deve essere almeno biennale.
I dati possono essere salvaguardati anche attraverso il loro salvataggio con frequenza almeno mensile (e non più settimanale). Il salvataggio periodico può non riguardare i dati non modificati dal momento dell'ultimo salvataggio effettuato (dati statici), purché ne esista una copia di sicurezza da cui effettuare eventualmente il ripristino.

Trattamenti dati con strumenti cartacei

Anche in questo caso sono previste istruzioni, anche orali, agli incaricati finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
Inoltre è specificato un obbligo di custodia in capo all'incaricato del trattamento che deve controllare atti e documenti contenenti dati sensibili fino alla restituzione, in modo che a essi non accedano persone prive di autorizzazione. Non è espressamente previsto l'obbligo di identificazione del personale che accede agli uffici dopo la chiusura (ad esempio addetti di guardia e alle pulizie).

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, 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 non soltanto rappresenta la "fotografia" degli adempimenti aziendali, ma in caso di un controllo da parte delle Autorità competenti, risulta essere un efficace strumento di tutela dalle sanzioni penali e dalle richieste di risarcimento danni per violazione della privacy.