CIRCOLARE N. 12
11 MARZO 2011

La normativa sulla "Privacy": l'adozione delle misure minime di sicurezza, le semplificazioni, l'Amministratore di sistema

ASSOCIAZIONE PROFESSIONALE
I 36100 VICENZA, VIA NAPOLI 66 – TEL. 0444322866 - 0444322705 R.A. – FAX. 0444545075
Codice fiscale e partita I.V.A. 02380850244
Indirizzo E-Mail: info@studioacerbi.com - Web-site: www.studioacerbi.com

Uno degli ambiti di forte impatto organizzativo e amministrativo per imprese e professionisti è senz'altro quello relativo alle disposizioni in tema di sicurezza nel trattamento dei dati.
L'articolo 31 del D.Lgs. n. 196/2003 (cd. Codice della Privacy) stabilisce infatti che i dati personali devono essere "*custoditi e controllati … in modo da ridurre al minimo … i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta*".

1. L'adozione delle misure minime di sicurezza

Il Codice sulla *Privacy* (D.Lgs. n. 196/2003) impone a tutti coloro che trattano dati personali la predisposizione di adeguati controlli in materia di sicurezza, sulla base di uno specifico protocollo previsto dal *c.d. Disciplinare Tecnico della norma* (allegato B del citato D.Lgs. n. 196/2003).
La norma obbliga alla realizzazione di diversi adempimenti, tra cui:

- la nomina del ***titolare del trattamento dei dati***, che generalmente coincide con la Società, nella persona del suo Legale rappresentante;
- la nomina del/dei ***responsabile/i del trattamento dei dati;***
- la nomina dell'/degli ***incaricato/i al trattamento dei dati;***
- il rilascio di apposita informativa;
- la preventiva richiesta del consenso al trattamento dei dati;
- la notificazione al Garante della *Privacy*, quando corra l'obbligo;
- l'**adozione di idonee misure di sicurezza**, per garantire che i dati personali vengano custoditi e controllati in modo da ridurre ad un ragionevole margine, il rischio di:
  - sottrazione, alterazione, perdita degli stessi,
  - di accesso non autorizzato da parte di terzi,
  - trattamento di dati non consentito e non conforme a quanto normativamente previsto.

È quanto mai opportuno ricordare che chi non adempie ai citati obblighi si espone al rischio di vedersi condannato, oltre che a pesanti sanzioni anche di natura penale, all'eventuale risarcimento dei danni che i terzi potrebbero lamentare come conseguenza dell'inefficiente controllo dell'attività di trattamento dei dati personali.
Il Legislatore, in relazione all'obbligo generale di protezione dei dati personali, ha previsto un livello minimo di sicurezza cui corrispondono le c.d. "misure minime", tra le quali vi è anche la redazione del **DPS** (Documento Programmatico sulla Sicurezza) quando il trattamento dei dati viene effettuato con strumenti elettronici e riguarda dati "sensibili" (ossia idonei a rivelare l'origine etnica e razziale, le convinzioni religiose, politiche, filosofiche, l'appartenenza a partiti e sindacati, nonché quelli idonei a rivelare lo stato di salute e la vita sessuale), o "giudiziari".

Il DPS deve essere aggiornato e rivisto ogni anno entro il 31 marzo; periodicamente è necessario verificare il rispetto delle prescrizioni normative, e annualmente corre l'obbligo di effettuare un percorso formativo specifico da parte del titolare, dei responsabili e degli incaricati al trattamento dei dati.

Sono state previste dal Garante per la protezione dei dati personali alcune **semplificazioni** degli obblighi in materia di "misure minime di sicurezza" per determinate categorie di trattamento dei dati. In particolare:

con il provvedimento del Garante del 19/06/2008	piccole e medie imprese, professionisti e artigiani possono godere di semplificazioni su alcuni adempimenti previsti dal D.Lgs. n. 196/2003, quali informativa, esonero dal consenso, incaricati del trattamento dei dati personali,
con il D.L. n. 112/2008	sono state introdotte ulteriori semplificazioni in materia di DPS (si veda di seguito al paragrafo 2.3); in pratica è possibile **evitare** di redigere il documento programmatico sulla sicurezza **quando** i soggetti trattano soltanto dati non sensibili, ovvero, in presenza di dati sensibili, questi siano costituiti unicamente dallo stato di salute o malattia dei propri dipendenti e collaboratori a progetto, senza indicazione della relativa diagnosi o dall'adesione a organizzazioni sindacali o a carattere sindacale.

2. Le semplificazioni

Il D.L. n. 112/2008 (cd. "manovra estiva") ha introdotto delle significative semplificazioni al Codice della Privacy. Esse riguardano, oltre al DPS di cui si dirà appena di seguito, anche la notificazione al Garante della *Privacy* e il trattamento dei dati personali fuori dalla UE.
In particolare:

2.1 La notificazione al Garante

Relativamente alla notificazione, che costituisce un obbligo solo al verificarsi di determinate e specifiche condizioni, ora la norma contiene un'esplicita indicazione delle informazioni che il titolare deve fornire attraverso il sito del Garante, utilizzando l'apposito modello.
Di seguito si ricordano le informazioni richieste dalla notificazione:

Le informazioni richieste nella notificazione
a) le coordinate identificative del titolare del trattamento e, eventualmente, del suo rappresentante, nonché le modalità per individuare il responsabile del trattamento, se designato;
b) la/le finalità del trattamento;
c) una descrizione della/delle categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime;
d) i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;
e) i trasferimenti di dati previsti verso Paesi terzi;
f) una descrizione generale che permetta di valutare in via preliminare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento.

2.2 Il trasferimento dei dati personali fuori dalla UE

Altra modifica, probabilmente quella meno rilevante per la gran parte dei soggetti interessati, riguarda il trasferimento di dati personali oggetto di trattamento verso un Paese non appartenente all'Unione europea. Tale trasferimento era consentito in precedenza solo se autorizzato dal Garante, sulla base di adeguate garanzie per i diritti dell'interessato, individuate e avallate dalla Commissione Europea o individuate dal Garante stesso anche in relazione a garanzie prestate contrattualmente. Ora il Garante potrà autorizzare il trasferimento dopo aver appurato l'esistenza delle necessarie garanzie, oltre che su base contrattuale, anche mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo.

2.3 Semplificazioni relative al DPS

Il Documento Programmatico sulla Sicurezza (DPS), può essere sostituito da una "autocertificazione", e in altri casi è possibile che possa essere redatto in modo "semplificato" rispetto ai requisiti minimi.

2.3.1 Esonero dal DPS ed autocertificazione

In pratica è possibile **evitare** di redigere il documento programmatico sulla sicurezza **quando** i soggetti:

- trattano soltanto dati non sensibili
- ovvero, in presenza di dati sensibili, questi siano costituiti unicamente:
  - dallo stato di salute o malattia dei propri dipendenti e collaboratori a progetto, senza indicazione della relativa diagnosi;
  - dall'adesione a organizzazioni sindacali o a carattere sindacale.

Si tratta molto spesso degli unici dati sensibili trattati da molte piccole o medie aziende, che, prima delle modifiche, costringevano alla redazione del DPS.
Per evitare di dover redigere il DPS, sarà sufficiente che il titolare del trattamento dei dati renda un'autocertificazione (di cui all'art. 47 del D.P.R. n. 445/2000), in cui dichiari **di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte.**
In altri termini, vengono sottratti dall'obbligo di redazione del DPS tutte quelle situazioni che rientrano nella normale ed ordinaria gestione imprenditoriale (ad esempio quelle situazioni tipiche della gestione del personale per cui il datore di lavoro è tenuto a far uso di dati relativi alla salute del dipendente).
Si precisa peraltro che il D.L. n. 112/2008 non ha abolito l'obbligo dell'adozione di misure di sicurezza diverse dal DPS e che, per tutti i casi di trattamenti datoriali di dati sensibili dei lavoratori diversi da quelli sulla salute (ad esempio trattenute sindacali o eventuali sussidi per figli disabili) persiste l'obbligo di redazione del DPS.
Ancora, per l'acquisizione di dati sulla salute dei propri dipendenti per fini discrezionali, come quello di gestire programmi convenzionati, liberamente riconosciuti a beneficio dei dipendenti stessi (per esempio una polizza collettiva per il rimborso di spese mediche), permane l'obbligo di redazione del DPS.

AUTOCERTIFICAZIONE SOSTITUTIVA DPS
Obbligo di cui alla lett. g) del comma 1 e al punto 19 dell'Allegato B
Ai sensi degli artt. 34 comma 1-*bis* D.Lgs. n. 196/2003 e 47 D.P.R. n. 445/2000

Il sottoscritto ……., nato a ……., in data ……., C.F. ……,
in qualità di Legale rappresentante società ……. con sede in ……., C.F. ……. P. Iva ……,
consapevole che il rilascio di false dichiarazioni ad un pubblico ufficiale o la presentazione di false documentazioni sono punibili a termine degli artt. 495 e 496 del Codice penale,

DICHIARA

Ai sensi dell'art. 34, comma 1-*bis* del D.Lgs. n. 196/2003

- ☐ di effettuare il trattamento di dati personali non sensibili;
- ☐ che gli unici dati sensibili trattati sono 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;
- ☐ che i dati di cui sopra sono trattati in osservanza delle misure di sicurezza prescritte dal D.Lgs. n. 196/2003 e dall'Allegato B) allo stesso.

……, lì…… Il Titolare del trattamento ……

2.3.2 DPS semplificato

Inoltre, secondo il testo del nuovo comma 1-*bis* dell'art. 34 del D.Lgs. n. 196/2003, in relazione ai trattamenti di cui sopra, nonché a quelli comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante ha individuato **modalità semplificate** di applicazione del disciplinare tecnico di cui all'allegato B), in ordine all'adozione delle **misure minime di sicurezza**.
In buona sostanza, si tratta di un'ulteriore semplificazione, legata più specificatamente alle misure minime di sicurezza, in ordine al trattamento di quei dati che possiamo definire "ordinari", come la tenuta di una contabilità piuttosto che la gestione di dati e documenti previsti per i datori di lavoro.

I soggetti interessati sono i titolari che:

- siano soggetti alla tenuta di un aggiornato DPS (quindi non nei casi di esonero);
- trattino dati personali "unicamente per correnti finalità amministrative e contabili" (il provvedimento parla, a titolo di esempio, di "gestione di ordinativi" e di "ordinaria corrispondenza con clienti, fornitori e dipendenti").

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

piccoli imprenditori ai sensi dell'art. 2083 c.c.	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 comma 1 del D.M. 18/04/2005	"*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*".

DOCUMENTO PROGRAMMATICO "SEMPLIFICATO"

Imprese e professionisti ammessi al DPS semplificato:

- possono **impartire agli incaricati** le istruzioni in materia di **misure minime anche oralmente;**
- possono utilizzare per l'accesso ai sistemi informatici un qualsiasi sistema di **autenticazione basato su un *username* e una *password***; lo *username* deve essere disattivato quando viene meno il diritto di accesso ai dati (es. non si opera più all'interno dell'organizzazione);
- in caso di assenze prolungate o di impedimenti del dipendente possono mettere in atto procedure o modalità che consentano comunque l'operatività e la sicurezza del sistema (ad es. l'invio automatico delle mail ad un altro recapito accessibile);
- devono **aggiornare** i programmi di sicurezza (**antivirus) almeno una volta l'anno;**
- devono effettuare ***backup* dei dati almeno una volta al mese.**

A differenza del DPS ordinario, l'aggiornamento di quello semplificato è richiesto solo in presenza di modifiche.

3. L'Amministratore di sistema

In attuazione degli originari provvedimenti del Garante della Privacy del 27 novembre 2008, Vi ricordiamo la disposizione relativa all'obbligo di **individuare** e, di conseguenza, di **nominare** per iscritto l' "**amministratore di sistema**", sia esso un soggetto interno sia esso un soggetto esterno.

Gli "**amministratori di sistema**" sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche.

Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione.
Le ispezioni effettuate in questi anni dall'Autorità hanno permesso di mettere in luce in diversi casi una scarsa consapevolezza da parte di organizzazioni grandi e piccole del ruolo svolto dagli amministratori di sistema. I gravi casi verificatisi negli ultimi anni hanno evidenziato una preoccupante sottovalutazione dei rischi che possono derivare quando l'attività di questi esperti sia svolta senza il necessario controllo.
Le misure e le cautele da mettere in atto, tenendo presente che sono esclusi i trattamenti di dati, sia in ambito pubblico che privato, effettuati a fini amministrativo contabile, che pongono minori rischi per gli interessati, sono le seguenti:

Registrazione degli accessi	Adozione di sistemi di controllo che consentano la registrazione degli accessi effettuate dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.
Verifica della attività	Verifica almeno annuale da parte dei titolari del trattamento sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali.
Elenco degli amministratori di sistema e loro caratteristiche	Ciascuna azienda o soggetto pubblico dovrà inserire nel documento programmatico della sicurezza o in un documento interno (disponibile in caso di accertamenti da parte del Garante) gli estremi identificativi degli amministratori di sistema e l'elenco delle funzioni loro attribuite. Dovranno, infine, essere valutate con attenzione, esperienza, capacità, e affidabilità della persona chiamata a ricoprire il ruolo di amministratore di sistema, che deve essere in grado di garantire il pieno rispetto della normativa in materia di protezione dei dati personali, compreso il profilo della sicurezza.

Nel rilevare il generale impegno da parte delle imprese ad adempiere alle prescrizioni impartite con il provvedimento del 27 novembre 2008, il Garante ha constatato che azioni promozionali da parte di consulenti rischiano di disorientare alcune aziende, soprattutto quelle di piccole dimensioni, esponendole a immotivati aggravi economici. L'Autorità ha inteso, dunque, ribadire quanto segue:

- le prescrizioni riguardano solo quei soggetti che, nel trattare i dati personali con strumenti informatici, devono ricorrere o abbiano fatto ricorso alla figura professionale dell'amministratore di sistema o a una figura equivalente.
- le prescrizioni non si applicano, invece, a quei soggetti anche di natura associativa che, generalmente dotati di sistemi informatici di modesta e limitata entità e comunque non particolarmente complessi, possano fare a meno di una figura professionale specificamente dedicata alla amministrazione dei sistemi o comunque abbiano ritenuto di non farvi ricorso.

In materia di "amministratore di sistema",

sono previsti i seguenti obblighi:	- individuare coloro che ricadono nella categoria di "amministratore di sistema"; - valutare l'esperienza, la capacità e l'affidabilità dei soggetti designati quali "amministratore di sistema" che devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza; - designare tali "amministratore di sistema" in modo individuale con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato; - verificare l'operato degli amministratori di sistema, con cadenza almeno annuale, in modo da controllare la sua rispondenza alle misure

organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;

- registrare gli accessi ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema, mediante l'adozione di sistemi idonei alla registrazione degli accessi logici (autenticazione informatica).

Possono essere considerati amministratori di sistema:

- gli amministratori di "basi di dati";
- gli "amministratori di reti" (es: titolare di Studio o dell'impresa che accede con la qualifica o le prerogative di "*administrator*" della rete) e di apparati di sicurezza;
- e gli "amministratori di sistemi *software* complessi" (es.: tecnico informatico nominato *ad hoc*), e ciò anche quando l'amministratore non consulti "in chiaro" le informazioni relative ai trattamenti di dati personali.