

La disciplina in tema di privacy: attesi chiarimenti sui soggetti interessati dalle nuove misure

Sì alla sicurezza, ma semplificata

Obiettivo è evitare le sanzioni, aumentate dal Milleproroghe

Misure a confronto

Allegato b al codice della privacy

A carico del professionista ci sono i seguenti adempimenti: autenticazione informatica nell'uso degli elaboratori, eventuale profilazione degli utenti, predisposizione di programmi anti-intrusione, obbligo di back up periodico dei dati e ripristino dei dati, redazione del Documento programmatico sulla sicurezza. Per quanto riguarda, invece, i trattamenti con uso di strumenti diversi dall'elaboratore il professionista deve fornire prescrizioni sulla custodia e gestione dei fascicoli e deve identificare personale di pulizia e di guardia e che comunque ha accesso ai locali dopo la chiusura degli uffici. Il documento programmatico sulla sicurezza va aggiornato entro il 31 marzo di ogni anno.

Formula semplificata

L'autenticazione informatica per l'uso degli elaboratori può coincidere con il log in del sistema operativo, il Documento programmatico sulla sicurezza contiene solo la descrizione delle misure adottate e non deve dare conto di attività formativa per gli incaricati del trattamento; si dilatano i termini entro cui aggiornare i programmi anti-intrusione ed entro cui effettuare la copia dei dati, la quale può limitarsi ai documenti (con esclusione dei dati statici, purché ne esista una copia di sicurezza da cui effettuare eventualmente il ripristino).



Pagina a cura
DI ANTONIO CICCIA

La sicurezza informatica dei dati, per i professionisti, è un obbligo normativo, che discende dalle disposizioni del Dlvo 196/2003.

Il professionista, nell'esercizio della sua attività, tratta i dati personali, anche sensibili, ed è quindi assoggettato alla disciplina che impone precauzioni idonee a evitare dispersione e perdite dei dati e anche accessi o manipolazioni abusive.

Anche il professionista, che si rivolge a un esperto dovrà preoccuparsi di designare l'amministratore di sistema, come previsto dal provvedimento del Garante del 27 novembre 2008, pubblicato sulla *Gazzetta Ufficiale* n. 300 del 24 dicembre 2008. L'adempimento deve essere realizzato entro il 23 aprile 2009, come previsto dallo stesso provvedimento.

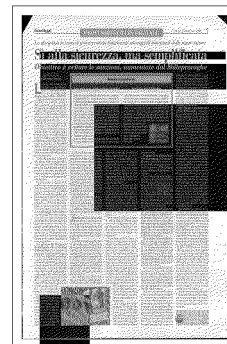
Tutto ciò per non incorrere nei rigori delle sanzioni previste dal decreto Milleproroghe, che ha innalzato sanzioni penali e sanzioni pecuniarie amministrative, in particolare per le violazioni alla sicurezza informatica.

Peraltro non è chiaro se il professionista possa avvalersi delle misure di semplificazioni previste, proprio per gli obblighi di sicurezza informatica, dal provvedimento del 27 novembre 2008 pubblicato in *Gazzetta*

Ufficiale n. 287 del 9 dicembre 2008, le quali sono riservate a chi tratta dati personali per le correnti finalità amministrative e contabili. Non sono, infatti, ancora intervenute indicazioni circa l'esatta interpretazione dell'espressione «correnti finalità amministrative e contabili» e quindi non è definito quale tipo di trattamenti o di dati rientri in una finalità tale da non poter essere qualificata come «corrente».

Le misure di sicurezza dell'allegato «B» al Codice della privacy. Le misure di sicurezza descritte all'allegato b del dlvo 196/2003 prevedono a carico del professionista i seguenti adempimenti: autenticazione informatica nell'uso degli elaboratori, eventuale profilazione degli utenti, predisposizione di programmi anti-intrusione, obbligo di back up periodico dei dati e ripristino dei dati; redazione del Documento programmatico sulla sicurezza.

Per quanto riguarda, invece, i trattamenti con uso di strumenti diversi dall'elaboratore il professionista deve fornire prescrizioni sulla custodia e gestione dei fascicoli e deve, altresì, identificare personale di pulizia e di guardia e che comunque ha accesso ai locali dopo la chiusura degli uffici.



Il documento programmatico sulla sicurezza va aggiornato entro il 31 marzo di ogni anno. Nel documento programmatico sulla sicurezza, per la cui redazione tutti gli ordini e collegi professionali hanno predisposto fac simile per i loro iscritti, deve essere inserita una fotografia della situazione esistente, con apposita analisi dei rischi di attentato agli elaboratori, e anche una parte programmatica, che individui gli obiettivi di sicurezza da raggiungere.

Quindi per il 2009 il professionista dovrà segnare in agenda la data di fine marzo ed entro allora verificare il proprio Dps e, meglio, la situazione della sicurezza informatica nel proprio studio.

Misure di sicurezza semplificate. Con il provvedimento del Garante del 27 novembre 2008 è stata approvata la semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'allegato B).

Il primo è rappresentato dalla individuazione della platea dei soggetti interessati. L'indicazione del provvedimento in esame è di riservare le misure semplificate ai soggetti che trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese.

Si è dell'opinione che il riferimento ai liberi professionisti debba indirizzare l'individuazione dei possibili beneficiari della agevolazione in commento. Si ritiene, quindi, che l'espressione «correnti finalità amministrative e contabili» debba essere letta nel senso che permetta a tutti i liberi professionisti, dotati di una organizzazione di dimensioni ridotte, di usufruire delle misure semplificate.

Se, invece, si ritenesse che l'espressione «correnti finalità amministrative» ammetta interpretazioni solo letterali, magari escludenti il trattamento di dati sensibili, è evidente la pratica inutilizzabilità della semplificazione. L'interpretazione restrittiva risulterebbe anche con effetti auto abroganti.

Una interpretazione coerente salva l'applicabilità delle norme di semplificazione della sicurezza informatica per il professionista, che ha una organizzazione di ridotte dimensioni.

Seguendo questa linea di lettura ne derivano i seguenti effetti. L'autenticazione infor-

matica per l'uso degli elaboratori può coincidere con il log in del sistema operativo, il Documento programmatico sulla sicurezza contiene solo la descrizione delle misure adottate e non deve dare conto di attività formativa per gli incaricati del trattamento, si dilatano i termini entro cui aggiornare i programmi antiintrusione ed entro cui effettuare la copia dei dati, la quale può limitarsi ai documenti (con esclusione dei dati statici, purché ne esista una copia di sicurezza da cui effettuare eventualmente il ripristino).

C'è comunque ancora un po' di tempo (fino al 31 marzo 2009) per avere un quadro definito della situazione e quindi per poter salire sul treno delle semplificazioni senza problemi interpretativi.

Nomina di un amministratore di sistema. Dalle semplificazioni (probabili) si torna al piano degli adempimenti passando a parlare della designazione dell'amministratore di sistema.

Qui si tratta di nuovi adempimenti o meglio del richiamo ad adempimenti, già previsti in generale dal codice della privacy per la sicurezza informatica, ma che vengono dettagliati dal provvedimento sopra richiamato. Il richiamo è stato motivato da una valutazione di un certo diffuso lassismo, cui il Garante intende porre un argine.

Il novero degli adempimenti prevede innanzi tutto la designazione individuale dell'amministratore di sistema. Il professionista, che si affida a un esperto informatico per la gestione della sicurezza degli elaboratori, deve quindi fare un atto espresso di incarico, in cui sono elencati gli ambiti di operatività.

La nomina dell'amministratore di sistema presuppone la valutazione della professionalità. Se ci sono più amministratori di sistema (magari per sedi territoriali diverse dello studio o dell'azienda) il professionista titolare del trattamento deve conservare l'elenco degli amministratori nominati.

Se ci sono dipendenti il professionista deve fornire loro un'informazione in cui comunica il nominativo dell'amministratore: ciò risponde a un'esigenza di tutela dei diritti del lavoratore subordinato in ossequio alle norme dello Statuto dei lavoratori.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve

conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema. Il lavoro dell'amministratore di sistema deve essere controllabile e il provvedimento prescrive la registrazione degli accessi ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Per tutti i titolari dei trattamenti già iniziati le misure e gli accorgimenti dovranno essere introdotti al più presto e comunque entro, e non oltre, il termine del 23 aprile 2009. Anche se già si parla di una proroga per l'adempimento al 15/7/2009.

Riciclaggio e smaltimento rifiuti informatici. Con altro provvedimento (del 13 ottobre 2008, pubblicato sulla *Gazzetta Ufficiale* n. 287 del 9 dicembre 2008) il garante si è occupato di rifiuti di apparecchiature elettriche ed elettroniche (Raee). Anche i professionisti devono adottare le misure tecniche riportate nell'allegato al provvedimento. Con riferimento alla dismissione di componenti elettrici ed elettronici suscettibili di memorizzare dati personali le precauzioni devono consistere nell'effettiva cancellazione o trasformazione in forma non intelligibile dei dati personali negli stessi contenute, così da impedire a soggetti non autorizzati che abbiano a vario titolo la disponibilità materiale dei supporti di venire a conoscenza non avendone diritto. Inoltre chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti deve comunque assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili;

Sanzioni. In materia di sicurezza informatica non si può non tenere conto del dl 207/2008: si assiste, quanto alle sanzioni penali per violazioni delle misure minime di sicurezza, a un maggiore rigore derivante dall'eliminazione della sanzione pecuniaria alternativa alla sanzione detentiva e all'incremento della somma da pagare per ottenere la derubricazione in illecito amministrativo (da 12.500 a 30.000 euro). Inoltre alla sanzione penale si aggiunge sempre una pesante sanzione amministrativa (fino a 120 mila euro, aumentabile fino a 480 mila euro in casi di maggiore gravità), non estinguibile con pagamento in misura ridotta. La sanzione amministrativa-



va prevede incrementi per casi di maggiore gravità, per l'ipotesi di livelli non congrui con le condizioni economiche del contravventore e per il caso di concorso di violazioni.

Anche per questa fattispecie è stata introdotta la diminuzione di sanzione per l'ipotesi di minore gravità, di cui potranno fruire in particolare i professionisti.