11 dicembre 2009 7:05

Amministratore di sistema di rete: dati personali e privacy. Regole da adottare entro il 15 dicembre 2009

di Deborah Bianchi*

A seguito delle indicazioni formulate nel corso di una consultazione pubblica indetta il 21 aprile 2009, il Garante Privacy ha emanato nuove disposizioni (Provvedimento 25 giugno 2009) per modificare il precedente Provvedimento 27 novembre 2008 concernente le misure di sicurezza applicabili agli amministratori di sistema (http://stefanobendandi.blogspot.com/2009/01/privacy-ed-amministratori-di-sistema.html).

Le modifiche si giustificano con l'intento di facilitare l'adozione delle misure, anche per quelle realtà aziendali nelle quali determinati servizi informatici sono forniti da società esterne.

In tal senso l'autorità ha consentito che gli adempimenti connessi all'**individuazione** degli amministratori di sistema ed alla **tenuta** dei relativi elenchi possano essere soddisfatti, oltre che dal titolare anche dai responsabili del trattamento.

Inoltre i termini per l'adozione delle misure tecniche ed organizzative sono stati prorogati al **15 dicembre 2009.**

E' bene sottolineare che le realtà più complesse sia private che pubbliche hanno provveduto alla designazione dei propri amministratori di sistema ancor prima del Provvedimento del Garante indicandoli direttamente nei loro DPS (Documento Programmatico sulla Sicurezza). Pensiamo alle grandi aziende, alle unità sanitarie locali, ai grandi comuni, alle province, alle regioni.

Lo **spirito della disposizione dell'Authority** si coglie ponendo attenzione ai casi in cui l'amministratore di sistema già esistente e nominato dal titolare abusava della propria posizione di onnipotenza informatica per sbirciare i dati personali degli interessati (clienti o utenti) trattati dalla struttura presso le cui dipendenze l'amministratore svolgeva servizio o presso cui prestava la propria opera.

Proprio la registrazione di molte di queste ipotesi sul suolo nazionale spinge il Garante a indicare le avvertenze necessarie per evitare gli abusi introducendo, se del caso, anche la conservazione dei file di log inerenti l'attività degli amministratori di sistema.

Posto dunque che il Provvedimento si rivolge maggiormente a strutture di significative dimensioni, dobbiamo chiederci quali riflessi abbia questa disposizione sulle realtà piccole e medie.

CONSIGLI PRATICI PER LE PICCOLE IMPRESE E PER I PROFESSIONISTI

La nomina dell'amministratore di sistema non è obbligatoria ma è a discrezione del titolare del trattamento.

L'Authority suggerisce di considerare a fondo lo stato della propria struttura e dedurre la necessità o meno di nominare un amministratore di sistema.

"*Nel corso delle attività ispettive disposte negli ultimi anni dal Garante è stato possibile rilevare quale importanza annettano ai ruoli di system administrator (e di network administrator o database administrator) la gran parte di aziende e di grandi organizzazioni pubbliche e private, al di là delle definizioni giuridiche, individuando tali figure nell'ambito di piani di sicurezza o di documenti programmatici e designandoli a volte quali responsabili.*

In altri casi, non soltanto in organizzazioni di piccole dimensioni, si è invece riscontrata, anche a elevati livelli di responsabilità, una carente consapevolezza delle criticità insite nello svolgimento delle predette mansioni, con preoccupante sottovalutazione dei rischi derivanti dall'azione incontrollata di chi dovrebbe essere preposto anche a compiti di vigilanza e controllo del corretto utilizzo di un sistema informatico.

Con il presente provvedimento il Garante intende pertanto richiamare tutti i titolari di trattamenti effettuati, anche in parte, mediante strumenti elettronici alla necessità di prestare massima attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema".

(Garante Privacy, Provvedimento 27 novembre 2008, Considerazioni preliminari).

"*3. Segnalazione ai titolari di trattamenti relativa alle funzioni di amministratore di sistema*
Ai sensi del menzionato art. 154, comma 1, lett. h) il Garante, nel segnalare a tutti i titolari di trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici la particolare criticità del ruolo degli amministratori di sistema, richiama l'attenzione dei medesimi titolari sulla necessità di adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di amministratore di sistema; richiama inoltre l'attenzione sull'esigenza di valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. ***Ciò, tenendo in considerazione l'opportunità o meno di tale attribuzione (discrezionalità e non obbligatorietà della nomina di amministratore di sistema)****e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilità, specie di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare in caso di incauta o inidonea designazione*."

(Garante Privacy, Provvedimento 27 novembre 2008, Premessa).

All'esito di questa analisi possiamo concludere che il titolare del trattamento può anche decidere di non fare alcuna nomina.

Per di più **a conforto di questa tesi** si pone il **Comunicato del Garante del 10 dicembre 2009** in cui espressamente l'Authority precisa che, onde evitare inutili aggravi per le piccole aziende, **i titolari che non hanno mai fruito di una figura professionale attinente al ruolo di ADS non dovranno procedere alla relativa nomina.**

Tuttavia se il titolare di una piccola o media struttura vuole comunque procedere alla nomina per sentirsi maggiormente in regola deve attenersi di massima alle linee di seguito esposte stigmatizzate per tipologia di realtà lavorativa.

STRUTTURA PICCOLA

Poniamo il caso della presenza di un unico personal computer ad uso esclusivo del titolare.

Il titolare si indica nel DPS quale amministratore di sistema e ovviamente non resta sottoposto all'obbligo di verifica delle attività dell'amministratore né alla tenuta del log degli accessi informatici.

Tale posizione trova conforto nelle faq (punto 3)accluse al Provvedimento del Garante 27 novembre 2008:

"3) Il caso di uso esclusivo di un personal computer da parte di un solo amministratore di sistema rientra nell'ambito applicativo del provvedimento?
Non è possibile rispondere in generale. In diversi casi, anche con un personal computer possono essere effettuati delicati trattamenti rispetto ai quali il titolare ha il dovere di prevedere e mettere in atto anche le misure e gli accorgimenti previsti nel provvedimento. Nel caso-limite di un titolare che svolga funzioni di unico amministratore di

sistema, come può accadere in piccolissime realtà d'impresa, non si applicheranno le previsione relative alla verifica delle attività dell'amministratore né la tenuta del log degli accessi informatici".

L'indicazione dell'assunta qualità di amministratore di sistema da parte del titolare potrà essere attestata su documento cartaceo a cui si conferirà data certa mediante, ad esempio, il servizio postale e che verrà accluso al DPS come allegato A.

STRUTTURA MEDIA

Poniamo il caso di più personal computer stand alone ovvero non raccolti in una rete interna all'azienda o allo studio professionale.

In tal caso si può ripetere lo stesso consiglio dato per la struttura piccola. In definitiva ciascun lavoratore o professionista usa il proprio pc in modo esclusivo e così si qualificherà quale amministratore di sistema del proprio spazio informatico.

Poniamo il caso invece di più computer collegati in rete secondo la logica server-client. Qui ciascun lavoratore o professionista fa capo a una base dati comune appartenente alla struttura.

In questa ipotesi la nomina dell'amministratore di sistema è sicuramente consigliata.

Tuttavia occorre tenere presente che in virtù del carattere estremamente fiduciario del rapporto che intercorre tra amministratore di sistema e azienda **è auspicabile che l'incarico ricada su una persona dell'organico interno** che si distingua per le capacità organizzative e le competenze informatiche.

La figura di amministratore di sistema tratteggiata dall'Authority si distingue nettamente dalla vecchia figura prevista dal decreto del Presidente della Repubblica 28 luglio 1999, n. 318, all'art. 1, che, da un punto di vista tecnico, sostanzialmente non era adeguato anche perché interpretava l'amministratore di sistema come soggetto al quale era affidato il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione.

La figura attuale di ADS non è limitata all'utilizzazione di un pc o di una banca dati ma abbraccia tutte le competenze necessarie per gestire gli adempimenti previsti dall'allegato B) del Codice Privacy..

Riportiamo, adesso, il punto 19, dell'allegato B):

«***Documento programmatico sulla sicurezza. 19.*** *Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:*

1. *l'elenco dei trattamenti di dati personali;*

2. *la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;*

3. *l'analisi dei rischi che incombono sui dati;*

4. *le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;*

5. *la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;*

6. *la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.*

7. *la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;*

8. *per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.»*

L'amministratore di sistema deve attendere a tutti i compiti sopra riportati come la distribuzione dei compiti nell'ambito delle strutture preposte al trattamento dei dati personali, l'analisi dei rischi, le misure da adottare per garantire la protezione dei dati, la protezione degli ambiti locali, la custodia e l'accessibilità.

L'amministratore di sistema allo stesso modo del responsabile, deve essere nominato per iscritto e nell'atto di nomina devono essere indicati quali sono i suoi compiti. Occorre evidenziare che sull'atto di nomina va apposta la firma a cura del soggetto designato.

Molto spesso quindi la figura dell'amministratore di sistema si troverà in capo al soggetto che è già stato nominato responsabile del trattamento (nelle strutture medie più grandi) o in capo al titolare (nelle strutture medie più piccole).

Si ribadisce la preferenza per un soggetto interno alla struttura che eventualmente per la parte più squisitamente tecnica potrà avvalersi di ditte di assistenza informatica che risulteranno nel DPS unicamente come incaricati.

Quanto al caso della riparazione sporadica o della manutenzione occorre rilevare con il Garante che queste non sono ipotesi di amministrazione del sistema e dunque non rimangono sottoposte alle disposizioni in materia.

Così l'Authority nel Provvedimento 27 novembre 2008, Faq, punto 1:

"1) Cosa deve intendersi per "amministratore di sistema"?
In assenza di definizioni normative e tecniche condivise, nell'ambito del provvedimento del Garante l'amministratore di sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati. i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati i personali.
Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software*".*

Le attività sottoposte a controllo da parte del titolare attengono alle funzioni attribuite con l'atto di nomina.

Quanto alla cadenza annuale del controllo è consigliabile assumere un criterio più elastico e considerare l'opportunità di procedere a una verifica ogni qual volta sia necessaria.

In effetti tale verifica può essere fatta più volte in un anno in maniera tale da controllare la rispondenza alle misure organizzative e tecniche e di sicurezza rispetto al trattamento dei dati personali previste dalle norme vigenti.

La registrazione dei file di log si consiglia nei casi in cui sia stato nominato ADS un soggetto esterno alla struttura. Nei casi in cui tale qualifica sia rivestita da una persona dell'organico interno il controllo avviene sulle proprie credenziali di accesso al sistema.

**** Deborah Bianchi,*** *avvocato specializzato in diritto applicato alle nuove tecnologie, esercita nel Foro di Pistoia e Firenze in materia civile e amministrativa.*