

Le nuove prescrizioni privacy per i titolari del trattamento relativamente alle attribuzioni delle funzioni di Amministratore di Sistema

Avv. Andrea Lisi e Avv. Graziano Garrisi

Digital&Law Department Studio Legale Lisi – www.studiolegalelisi.it

Il tema legato all'implementazione di misure di sicurezza e del rispetto della normativa sulla privacy è stato da sempre al centro dell'attenzione di quanti si trovano a gestire grandi banche dati o ad essere titolari o responsabili del trattamento o della conservazione all'interno di importanti aziende.

Per quest'ultimi, infatti, sono state previste nuove cautele da rispettare nella scelta e nomina degli amministratori di sistema. L'individuazione precisa e responsabile di tali soggetti, infatti, riveste una notevole importanza, perché è una delle scelte fondamentali all'interno di un'azienda e contribuisce a incrementare la complessiva sicurezza dei trattamenti svolti. Basti pensare, infatti, che molto spesso l'amministratore di sistema è dotato di una particolare posizione a cui spetta anche la capacità di stabilire - in raccordo con il titolare e/o eventuali altri responsabili dei relativi trattamenti - chi può accedere in modo privilegiato alle risorse del sistema informativo e a tutti i dati personali aziendali (anche sensibili): per tale motivo gli amministratori di sistema devono essere scelti con particolare attenzione, poiché i rischi che possono correre le banche dati o le reti informatiche sono sempre più elevati.

Dopo le recenti e numerose modifiche normative o "di prassi" a cui abbiamo assistito negli ultimi tempi, ecco che viene pubblicato un ulteriore provvedimento del Garante Privacy che introduce un nuovo adempimento in materia di gestione e protezione dei dati personali trattati attraverso sistemi informatici e di garanzia della sicurezza degli stessi dati e sistemi.

Il Garante Privacy, infatti, con un provvedimento del 27 novembre 2008 ("*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*"), ha introdotto l'obbligo per gli amministratori di sistema (compresi coloro che svolgono la mansione di amministratore di rete, di data base o i manutentori), di **conservare gli "access log" per almeno sei mesi in archivi imm modificabili e inalterabili.**

Devono, cioè, essere adottati sistemi idonei alla registrazione degli accessi logici, ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema e, novità forse più importante, gli *access log* devono avere le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste; **ciò vuol dire che le registrazioni devono avere i riferimenti temporali certi e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo** (non inferiore a sei mesi). Come non pensare a processi di conservazione digitale in linea con le regole tecniche previste dall'art. 71 del Codice dell'amministrazione digitale e oggi contenute nella deliberazione CNIPA n. 11/2004 e nel DPCM 13 gennaio 2004?

I titolari dovranno altresì favorire una più agevole conoscenza, nell'ambito della propria organizzazione, dell'esistenza di eventuali amministratori di sistema: è importante garantire, in questo modo, la conoscibilità dell'esistenza di tali figure e di chi svolge ruoli analoghi all'interno di tutti gli enti e le organizzazioni; viene precisato, inoltre, che **gli amministratori di sistema, indipendentemente se nominati incaricati o responsabili del trattamento, devono essere**

sempre persone fisiche ben individuate all'interno del DPS e il loro nomi devono essere comunicati o resi conoscibili da tutti i soggetti interessati.

A parere di chi scrive, quindi, per evitare spiacevoli sanzioni, ogni titolare dovrà verificare che tale elencazione sia stata effettuata nell'ambito del prossimo aggiornamento annuale del DPS e, nei casi in cui il titolare non sia tenuto a redigerlo, si dovrà provvedere ad inserire il nominativo degli amministratori di sistema in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Se poi l'attività degli amministratori di sistema riguarda, anche indirettamente, servizi o sistemi che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati, in qualità di datori di lavoro, sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema all'interno delle proprie organizzazioni attraverso **apposita informativa ex art. 13 d.lgs. 196/2003** (in alternativa si possono utilizzare anche strumenti di comunicazione interna quali l'intranet aziendale, ordini di servizio a circolazione interna ect.). Sono fatti salvi, in ogni caso, i casi di esclusione per legge di tale forma di pubblicità o conoscibilità.

Nel caso, poi, di servizi di amministrazione di sistema affidati in outsourcing il titolare avrà l'obbligo conservare gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

I titolari del trattamento avranno, altresì, un obbligo di verifica annuale sull'operato degli amministratori di sistema, per controllare la rispondenza o meno alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalla normativa vigente.

In tema di esclusioni, tale provvedimento non si applica ai titolari che rientrano nel beneficio delle esenzioni privacy oggetto delle recenti misure di semplificazione, previste per le piccole e medie imprese o per i professionisti che trattano dati personali per le sole finalità amministrative e contabili.

Proviamo ora ad esaminare i motivi per i quali il Garante ha ritenuto necessario introdurre tale ulteriore adempimento:

1 - In primo luogo, gli amministratori di sistema, o coloro che gestiscono l'accesso a banche dati, sono generalmente preposti a operazioni da cui discendono grandi responsabilità ed elevate criticità rispetto alla protezione dei dati personali a cui hanno accesso. Ricordiamo, infatti, che per sua natura l'amministratore di sistema è dotato di una capacità di azione propria e di un rapporto fiduciario che lo lega al titolare nello svolgimento delle relative mansioni (ruolo così importante per le aziende e per le grandi organizzazioni pubbliche e private, tanto da farlo nominare a volte anche quale responsabile del trattamento). Ma anche nelle piccole realtà tale figura riveste una certa importanza, perché dovrebbe essere preposto a compiti di vigilanza e controllo del corretto utilizzo del sistema informatico gestito e utilizzato;

2 - In secondo luogo, le attività di backup o disaster recovery (regolamentate anche nel Codice Privacy), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione o la semplice manutenzione hardware comportano la possibilità per tali soggetti di agire sulle informazioni critiche aziendali, attività tutte che ricadono nella definizione di "trattamento di dati personali", anche quando l'amministratore non consulti in chiaro tali informazioni;

3 - Le funzioni tipiche dell'amministrazione di un sistema sono specificatamente richiamate all'interno dell'allegato B del Codice Privacy, laddove si prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Si è voluto, quindi, assicurare un maggiore controllo su chi di fatto si occupa dell'assolvimento degli adempimenti previsti nello stesso allegato B, ovvero adempimenti che in genere sono affidati

all'amministratore di sistema: realizzazione di copie di sicurezza, custodia delle credenziali, gestione dei sistemi di autenticazione e di autorizzazione, ect.;

4 -Infine, vi sono alcuni reati previsti dal codice penale per i quali il rivestire la funzione di amministratore di sistema costituisce una circostanza aggravante (abuso della qualità di operatore di sistema nell'accesso abusivo a sistema informatico o telematico - art. 615 ter c.p. - o di frode informatica - art. 640 ter c.p. -, oppure per le fattispecie di danneggiamento di informazioni, dati e programmi informatici - artt. 635bis e ter c.p. - e di danneggiamento di sistemi informatici e telematici - artt. 635-quater e quinquies).

Con tale provvedimento il Garante ha, così, lanciato un ulteriore monito a tutti i titolari del trattamento, invitando ad affidare tale incarico, sia in qualità di responsabile sia di incaricato, a soggetti che siano affidabili, prima di tutto, oltre che capaci ed esperti, poiché devono fornire idonea garanzia del pieno rispetto delle disposizioni in materia di corretto trattamento, compreso il profilo relativo alla sicurezza informatica (in considerazione anche delle responsabilità, di natura penale e civile, che possono derivare in caso di incauta o inidonea designazione).

Infatti, il titolare può designare facoltativamente uno o più responsabili del trattamento, solo tra soggetti che "per esperienza, capacità e affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza" (art. 29, comma 2, del Codice). Si dovrà procedere, pertanto, con designazioni individuali, contenenti la descrizione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Tutto questo dovrà essere rispettato decorsi sei mesi dalla pubblicazione del provvedimento per tutti i trattamenti già in essere o che iniziano entro il 22.01.09, mentre per i trattamenti successivi, sarà obbligatorio sin da subito.