

Il 15 dicembre scade il termine per l'attuazione degli adempimenti introdotti dal Garante

Privacy, tracciabilità di log al via

Gli amministratori di sistema devono adeguarsi agli obblighi

DI STEFANIA ALGERIO

Il 15 dicembre scade il termine per l'attuazione degli obblighi introdotti dal garante per la protezione dei dati personali previsti dal Provvedimento del 27 novembre 2008 «Misure e accorgimenti prescritti ai titolari di trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratori di sistema», come modificato, con ulteriore Provvedimento del 25 giugno 2009 emanato a seguito di una consultazione pubblica alla quale hanno preso parte le associazioni rappresentative delle categorie coinvolte negli adempimenti.

L'attuazione del Provvedimento ha messo in difficoltà moltissimi «titolari» i quali, forse per la prima volta, hanno sentito parlare di log. Ma proprio i log sono oggetto di uno dei più importanti e impegnativi adempimenti introdotti dal provvedimento. I log sono file nei quali vengono registrate le operazioni che un utente compie su un sistema di elaborazione durante una sessione di lavoro.

Il Provvedimento fa riferimento a tutti quei log in cui siano registrati gli accessi ed i tentativi di accesso ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema (o figure ad essi assimilate), nonché le disconnessioni ed eventuali messaggi di errore.

Gli accessi al sistema da parte degli amministratori di sistema (effettuati dal server o anche direttamente dai client) devono essere infatti registrati negli access log, garantendo la completezza, l'inalterabilità e la possibilità di verificare l'integrità della registrazione stessa.

Il log, per essere completo, deve comprendere tutti gli eventi sopra descritti che interessino l'amministratore di sistema su tutti i sistemi di elaborazione su cui vengono trattati dati personali. Per quanto riguarda, invece, la caratteristica dell'inalterabilità, essa può, ad esempio, essere garantita con l'esportazione periodica dei dati di log su supporti di memorizzazione non riscrivibili, ricorrendo, ove ritenuto opportuno, anche all'apposizione della firma digitale. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate, e devono essere conservate per un periodo congruo, comunque non inferiore a sei mesi.

Nel caso il sistema di raccolta dei log adottato generi una raccolta di informazioni più ampia rispetto a quanto richiesto dal garante (in ordine agli eventi tracciati e/o ai soggetti che li hanno genera-

ti), è necessario verificare che la stessa non sia in contrasto con le disposizioni del codice. E responsabilità del titolare effettuare le verifiche necessarie, tenuto conto dei dati trattati, dell'organizzazione aziendale, delle procedure adottate e delle mansioni concretamente attribuite all'amministratore di sistema, per garantire le caratteristiche dei log richieste dal garante, valutando l'opportunità di un'implementazione dei propri sistemi software e hardware.

Dal punto di vista soggettivo, l'ambito applicativo del Provvedimento esclude i titolari recentemente interessati da misure di semplificazione, vale a dire:

I soggetti che trattano dati comuni 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 all'adesione di organizzazioni sindacali o a carattere sindacale (art. 29, legge 6 agosto 2008 n.133).

I soggetti che trattano dati personali unicamente per correnti finalità amministrative e contabili (Provvedimento del garante del 27 novembre 2008). Tutti i titolari che non rientrano nelle due categorie indicate devono attuare le misure di sicurezza individuate dal Garante relative agli amministratori di sistema. Particolarmente delicata, e strettamente legata alla questione dell'effettiva portata degli interventi del garante in materia di semplificazioni, la valutazione che ogni titolare deve effettuare in ordine alla propria sottoposizione al dettato del provvedimento. Mentre può essere relativamente semplice

verificare, tramite una seria mappatura dei propri trattamenti, se gli unici dati sensibili trattati siano quelli di cui all'art. 29 della legge 133/2008, molto più complesso è valutare se i dati trattati, quando anche fossero dati sensibili ulteriori rispetto a quelli di cui all'art. 29 della legge 133, siano trattati solo per «correnti finalità amministrative e contabili».

In assenza di specifici chiarimenti, è certamente prudentiale dare all'espressione di «correnti finalità amministrative e contabili» un'accezione sufficientemente restrittiva, tale da comprendere nella portata del Provvedimento qualunque attività che comporti per i dati rischi che non siano «minimi».

In tale ottica, rientrano certamente nel Provvedimento i titolari che trattano qualsiasi dato sensibile eccedente quelli riferiti esclusivamente allo stato di salute e malattia (senza diagnosi) dei propri dipendenti e alla loro eventuale adesione ad organizzazioni sindacali o a carattere sindacale, nonché i titolari di trattamenti eccedenti le esclusive correnti finalità amministrative e contabili.

Commercialisti, avvocati, consulenti del lavoro, qualsiasi titolare che tratti tali dati per finalità di marketing, un call center che effettui prenotazioni di visite mediche ci sembrano, a titolo puramente esemplificativo, sicuramente esclusi dalle semplificazioni e, pertanto, coinvolti dagli adempimenti sull'amministratore di sistema.

Chi è l'amministratore di sistema? O meglio, cosa comprende il garante nella locuzione «amministratore di sistema»? In base al Codice per la protezione dei dati persona-

li e al disciplinare Tecnico all. B), l'amministratore di sistema è il soggetto che attua alcune delle misure indicate dall'art. 34, quali ad esempio la creazione di profili di autorizzazione, l'aggiornamento degli antivirus ecc.

Il garante riconduce gli adempimenti alle figure professionali addette alla gestione e manutenzione di un impianto di elaborazione e delle sue componenti, ma anche a tutti quei soggetti equiparabili all'amministratore di sistema dal punto di vista dei rischi relativi alla protezione dei dati (amministratori di base dati, amministratori di reti, di apparati di sicurezza ecc.).

Una volta analizzata la propria struttura e focalizzati i soggetti a cui attribuire le funzioni di amministratore di sistema, il titolare deve attuare le disposizioni del Provvedimento:

Valutazione delle caratteristiche soggettive: anche quando l'attribuzione delle funzioni di amministratore di sistema avviene nell'ambito della designazione quale incaricato del trattamento (art. 29 dlgs 196/2003) il titolare deve effettuare le valutazioni previste per la nomina dei responsabili del trattamento (art. 29 dlgs 196/2003). Deve quindi valutare l'esperienza, la capacità e l'affidabilità del soggetto designato, non solo relativamente alle conoscenze e competenze tecniche possedute, ma anche riguardo alla conoscenza delle disposizioni che regolano il trattamento dei dati personali.

Designazioni: la designazione degli amministratori di sistema o delle figure equiparate deve essere nominativa e deve indicare analiticamente l'am-

bito di operatività consentito, in base al profilo di autorizzazione assegnato. Quando le funzioni di amministratore di sistema sono affidate a soggetti esterni (outsourcing) questi devono fornire al Titolare l'elenco nominativo dei soggetti a cui, al proprio interno, hanno attribuito le funzioni di amministratore di sistema.

Elenco nominativo degli amministratori designati: il titolare deve mantenere presso la propria sede un elenco aggiornato dei nominativi degli amministratori di sistema nominati, siano essi interni o esterni. L'elenco degli amministratori deve essere esibito in caso di verifica.

Conoscibilità degli amministratori di sistema: qualora l'attività degli amministratori di sistema riguardi, anche indirettamente, servizi o sistemi che trattano i dati di carattere personali dei lavoratori, i Titolari sono tenuti a rendere nota o conoscibile l'identità degli amministratori. Per assolvere all'obbligo di conoscibilità il titolare può avvalersi della rete intranet aziendale, può indicare nell'informativa ex art. 13 dlgs 196/2003 resa ai dipendenti l'identità degli amministratori o inserire questa informazione nel regolamento per l'uso dei sistemi informativi aziendali (Provvedimento del Garante del 1° marzo 2007 n. 13). Verifica dell'attività: il titolare (o, ove nominato, il responsabile) del trattamento è tenuto, almeno annualmente, a verificare l'operato dell'amministratore di sistema, in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali, previste dalle norme vigenti.

—© Riproduzione riservata—

VISTO DA...

Registri, semplificazione in tempi stretti

La completa dematerializzazione dei registri obbligatori e dei documenti amministrativi attraverso la loro conservazione sostitutiva è pienamente e, direi finalmente, attuabile in tempi brevissimi.

Il risparmio generato presso tutti i professionisti contabili e le imprese italiane assume ora una rilevanza economica importante.

Imprese e professionisti devono ringraziare il lavoro di squadra e la collaborazione fra i ministri Brunetta e Calderoli che hanno recepito le istanze di quel mondo imprenditoriale per il quale innovazione e semplificazione sono da sempre un punto di partenza per migliorare il tessuto economico italiano.

Il disegno di legge predisposto dai due ministri, approvato dal consiglio dei ministri, fa giustizia di una discrepanza dovuta probabilmente al mancato dialogo con gli attori coinvolti e contenuta nell'articolo 2215-bis del codice civile, introdotto nel 2008.

Esso prevedeva la marcatura temporale trimestrale dei libri contabili obbligatori in caso di loro dematerializzazione e conseguente conser-

vazione sostitutiva, mentre per quelli cartacei era sufficiente la bollatura annuale.

E facile comprendere che la tenuta informatica dei registri diveniva una complicazione per le imprese rispetto alla stampa e archiviazione cartacea. Ora sarà sufficiente «stampare» i registri su file ed apporre marcatura temporale e firma digitale alla scadenza naturale dei 12 mesi, procedendo con la Conservazione sostitutiva, come dispone il decreto dell'Economia del 2004.

E forse un esempio limitato, ma è ciò che serve alle imprese, è quello che si attende tutto quel mondo formato da 8 milioni di partite Iva e dai lavoratori dipendenti che gravitano attorno ad esse. Noi non abbiamo bisogno di conflittualità sui massimi sistemi, noi vogliamo collaborazione e stabilità all'interno della compagine che governa questo Paese, noi, caro presidente Fini, non sentiamo il bisogno di un altro Casini. Solo così usciremo dall'emergenza e potremo creare nuovi posti di lavoro e miglioreremo le condizioni economiche di quelli che già ci sono.

Bonfiglio Mariotti,
presidente Assosoftware

Brevi

Da ottobre 2009 01Sistemi Srl di Pisa e DB Servizi Srl di Sansepolcro sono entrate a far parte di Assosoftware.

Questa pagina è realizzata in collaborazione con



ASSOSOFTWARE

Associazione nazionale
professionisti di software
gestionale e fiscalità



www.assosoftware.it - info@assosoftware.it