

COMUNICATO IMPORTANTE PRIVACY

Milano 10 dicembre 2009

Oggetto: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema

Provvedimento del 27 novembre 2008, con le integrazioni e le modificazioni apportate dal [COMUNICATO STAMPA del Garante del 26 giugno 2009](#)

Gent.mi associati,

richiamandoci alle nostre precedenti comunicazioni, Vi ricordiamo che il giorno:

15 dicembre 2009

scadrà il termine entro il quale i titolari dei trattamenti di dati personali, effettuati con strumenti elettronici dovranno provvedere alla designazione della figura **dell'Amministratore di sistema**.

Chi è l'amministratore di sistema.

Ai sensi del Provvedimento del Garante devono considerarsi come **amministratori di sistema**:

- *le figure professionali in ambito informatico finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti;*
- *altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.*

Queste figure svolgono attività tecniche quali *il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione (CD-R di backup, chiavi con memoria, ecc..) e la manutenzione hardware*, attività che comportano, in molti casi, un'effettiva capacità di azione su informazioni, che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

Il Garante sottolinea poi che le funzioni tipiche **dell'amministrazione di un sistema** sono richiamate nel menzionato [Allegato B](#), nella parte in cui prevede l'obbligo per i titolari di assicurare *la custodia delle componenti riservate delle credenziali di autenticazione*¹ e che gran parte dei compiti previsti nel medesimo [Allegato B](#) spettano tipicamente **all'amministratore di sistema**: dalla *realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati)* alla *custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione*.

Per ulteriori informazioni sui compiti dell'amministratore di sistema e sui contenuti dell'Allegato B, vi consigliamo di rivolgervi ai vs. consulenti informatici o ai fornitori di sistemi software e/o hardware.

Quali sono le misure e gli accorgimenti prescritti ai titolari dei trattamenti.

Le misure e gli accorgimenti prescritti sono i seguenti:

- Il titolare, prima di attribuire le funzioni di **amministratore di sistema**, deve valutare: l'esperienza, la capacità e l'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
- La designazione dell'**amministratore di sistema** deve essere individuale e devono essere indicati in modo analitico gli ambiti di trattamento consentiti;

¹ *Le credenziali di autenticazione* sono tipicamente il codice utente o user-id e la password che consentono l'accesso ad un sistema informatico

- Gli estremi identificativi delle persone fisiche, **amministratori di sistema**, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante;
- L'identità dell'**amministratore di sistema** deve essere resa nota o conoscibile ai dipendenti, da parte del titolare/datore di lavoro, qualora l'attività dello stesso amministratore di sistema riguardi anche indirettamente sistemi che trattano informazioni di carattere personale dei lavoratori;
- Il titolare, o il responsabile del trattamento nel caso di servizi di amministrazione di sistema affidati in *outsourcing*, devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali **amministratori di sistema**;
- I titolari o il responsabile del trattamento devono verificare, con cadenza almeno annuale, l'operato dell'**amministratore di sistema**, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;
- Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli **amministratori di sistema**. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità e 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.

Il Garante, a tal proposito, ha specificato che, nella maggior parte delle piccole realtà aziendali, tale obbligo è attuabile utilizzando le funzionalità disponibili nel sistema operativo Windows.

A tal proposito, Microsoft ha messo a disposizione dei propri utenti una guida reperibile in internet al seguente link: <http://download.microsoft.com/documents/italy/SBP/privacy/Log-accessi.pptx>

Per ulteriori informazioni su tale adempimento, vi consigliamo di rivolgervi ai vs. consulenti informatici o ai fornitori di sistemi software e/o hardware.

Titolari dei trattamenti esclusi dalle misure e dagli accorgimenti sopra prescritti

Le misure e gli accorgimenti sopra prescritti sono rivolti a tutti i titolari dei trattamenti di dati personali effettuati con strumenti elettronici esclusi, allo stato, i trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili, che pongono minori rischi per gli interessati.

Bozze di:

- lettera di incarico ad Amministratore di sistema;
- lettera di incarico alla custodia delle credenziali.

In calce alleghiamo, a mero titolo unicamente esemplificativo e ai fini di meglio chiarire le istruzioni date dal Garante, le seguenti 2 bozze di lettera di incarico.

ALLEGATI:

Ottica Pinco Pallo

Egregio Signor
Rossi Mario
C.F.

OGGETTO: Lettera di incarico ad *Amministratore di sistema*

Egregio Signor Rossi,

In ottemperanza alle disposizioni dell'Allegato B del Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) ed al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (G.U. n. 300 del 24/12/2008), Lei è nominato *Amministratore del sistema* informatico del centro ottico.

La Sua designazione avviene in ragione del possesso dei requisiti di *esperienza, capacità ed affidabilità* richiesti dall'art. 29, comma 2 del DLgs. 196/2003 e richiamati dal sopracitato Provvedimento del Garante.

In qualità di *Amministratore del sistema*, Lei provvederà alla gestione e manutenzione dei sistemi di elaborazione dati presenti nel centro ottico.

In particolare, Lei dovrà svolgere i seguenti compiti:

- Redigere l'elenco dei sistemi di elaborazione e mantenerlo costantemente aggiornato.
- Gestire le connessioni di rete del centro ottico, garantendone la funzionalità e la sicurezza.
- In collaborazione con il *Custode delle credenziali*, configurare ed attivare le credenziali di autenticazione per gli Incaricati autorizzati al trattamento di dati con strumenti elettronici.
- Adottare le misure necessarie per proteggere gli elaboratori dal rischio di infezione da parte di virus e dalle intrusioni di soggetti non autorizzati.
- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere ad effettuare copie di back-up secondo le procedure definite nel Documento programmatico sulla Sicurezza.
- Assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro.
- Effettuare le prove di ripristino dei sistemi e dei dati nei modi e nei tempi indicati nel Documento programmatico sulla Sicurezza.
- Installare prontamente gli aggiornamenti periodici del sistema operativo e dei programmi applicativi resi disponibili dai fornitori tramite le relative funzioni automatiche.
- Provvedere alla distruzione dei supporti removibili obsoleti sui quali sono memorizzati dati sensibili. Se i supporti sono riutilizzabili, provvedere alla loro formattazione e consegnarli solo ad Incaricati autorizzati al trattamento dei dati.
- Adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte Sua (nella sua qualità di *Amministratore di sistema*); tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le ricordiamo, che il provvedimento del Garante già citato, obbliga l'azienda alla verifica almeno annuale delle attività svolte dall'amministratore di sistema in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti che si allegano alla presente.

Sulla base di quanto previsto al punto 2.c del citato Provvedimento del Garante, la informiamo che i suoi estremi identificativi saranno comunicati secondo quanto stabilito al comma 4.3

Con la sottoscrizione della presente Lei dichiara di comprendere ed accettarne integralmente il contenuto e di conoscere i contenuti del DLgs. 196/2003 e del *Documento programmatico sulla Sicurezza*.

Cogliamo l'occasione per porgerLe distinti saluti.

..... lì

Il Titolare del trattamento

Per ricevuta e integrale accettazione

.....

Firma dell'amministratore di sistema

Ottica Pinco Pallo

Egregio Signor
Rossi Mario
C.F.

OGGETTO: Lettera di incarico alla custodia delle credenziali

Egregio Signor Rossi,

In ottemperanza alle disposizioni contenute nell'Allegato B del Decreto legislativo 30 giugno 2003, n. 196, punto 10, La nominiamo *Custode delle credenziali* che consentono l'accesso agli strumenti elettronici (elaboratori e relative applicazioni).

In qualità di *Custode delle credenziali*, Lei dovrà svolgere i seguenti compiti:

- In collaborazione con l'*Amministratore di sistema*, attribuire a ciascun incaricato un codice identificativo personale (USER ID) per l'accesso agli elaboratori;
- Verificare che le USER-ID già utilizzate non vengano assegnate ad altri incaricati, nemmeno in tempi diversi;
- In occasione della prima definizione/cambio delle password, consegnare a ciascun incaricato una busta all'interno della quale ogni incaricato deve inserire un foglio contenente le credenziali riservate in uso. Ciascun incaricato deve chiudere la busta, contrassegnarla con il proprio nome, controfirmarla e consegnarla al Custode delle password.
- Custodire le buste chiuse consegnate dagli incaricati in un luogo sicuro;
- In caso di prolungata assenza o impedimento di un incaricato, consegnare al Titolare/Responsabile del trattamento la busta chiusa contenente le sue credenziali di autenticazione e comunicare tempestivamente all'incaricato l'avvenuta apertura della busta;
- Cancellare le credenziali di autenticazione non utilizzate da più di sei mesi, ad eccezione di quelle abilitate per soli scopi di gestione tecnica;
- Cancellare tempestivamente le credenziali di autenticazione assegnate agli incaricati in caso di revoca delle autorizzazioni di accesso ai dati.

Con la sottoscrizione della presente Lei dichiara di accettare integralmente il suo contenuto e di conoscere i contenuti del *Documento programmatico sulla Sicurezza*.

Cogliamo l'occasione per porgerLe distinti saluti.

..... lì

Firma del titolare o del Responsabile

Per ricevuta e integrale accettazione

.....

Firma del custode delle credenziali