

# PRIVACY E AMMINISTRATORI DI SISTEMA

*Giuseppe Migliorini – Augusto Scatolini*

<i>Premessa.....</i>	<i>2</i>
<i>Scopo del provvedimento.....</i>	<i>2</i>
<i>Cosa si intende per Amministratore di sistema.....</i>	<i>3</i>
<i>A chi si rivolge il provvedimento e aree di esenzione .....</i>	<i>3</i>
<i>AdS interno e AdS esterno.....</i>	<i>4</i>
<i>Le misure e gli accorgimenti tecnici e organizzativi prescritti .....</i>	<i>5</i>
<i>Cosa deve fare il Titolare.....</i>	<i>7</i>
<i>Aspetto sanzionatorio.....</i>	<i>8</i>

## Premessa

Chi ha avuto modo di cimentarsi con l'applicazione della privacy ha, inevitabilmente, incontrato una figura chiave dell'Ente o dell'Azienda: l'Amministratore di Sistema (AdS). Questa figura, non ben definita dal Codice, è sempre stata difficilmente collocabile nel "Sistema Privacy".

Il Garante per il trattamento dei dati personali, con i recenti provvedimenti<sup>1</sup>, ha colmato la lacuna e chiarito il ruolo dell'AdS che da ora in poi assume il rango delle altre figure fondamentali della Privacy quali il Titolare, il Responsabile (al quale è equiparato) e l'Incaricato.

Pertanto il Garante prescrive una serie di norme relative alla figura dell'AdS che comportano per lo più interventi di carattere organizzativo e **che entrano in vigore a partire dal 15 dicembre 2009**.

## Scopo del provvedimento

L'Autorità intende 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.

Questo nuovo adempimento non si esaurisce nella mera predisposizione di una nuova lettera di incarico o nella modifica di quella già esistente ma richiede al titolare una serie di "misure e accorgimenti" e, non ultimi, di adempimenti in ordine all'esercizio dei doveri di controllo da parte del titolare sulle attività dell'amministratore.

Allo scopo di facilitare il compito per quelle realtà nelle quali taluni servizi informatici sono svolti da società esterne, il Garante ha consentito che non solo i titolari, ma anche i responsabili possano effettuare gli adempimenti connessi all'individuazione degli AdS ed alla tenuta dei relativi elenchi<sup>2</sup>. L'applicazione di questo criterio fa sì che, in caso di outsourcing, l'onere di tali operazioni ricada sul responsabile esterno del trattamento. Il titolare, cui spetta sempre il compito di controllare, sarà pertanto libero da adempimenti che altrimenti sarebbe difficile, se non impossibile, attuare.

---

<sup>1</sup> Atti del Garante riguardanti l'AdS:

- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema. 27 novembre 2008 [doc. web n. 1577499]
- Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema. 12 febbraio 2009 [doc. web n. 1591970]
- Amministratori di sistema: avvio di una consultazione pubblica (G.U. n. 105 dell'8 maggio 2009). 21 aprile 2009 [doc. web n. 1611986]
- Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento. 25 giugno 2009 [doc. web n. 1626595] (G.U. n. 149 del 30 giugno 2009)

<sup>2</sup> Provvedimento del Garante 25 giugno 2009 [doc. web n. 1626595] (G.U. n. 149 del 30 giugno 2009)

## **Cosa si intende per Amministratore di sistema**

Ai sensi del provvedimento l'AdS è la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali.

Può essere comunque solo una persona fisica.

L'Ads, oggi, può assumere vari ruoli:

- amministratore delle basi di dati (database administrator), responsabile dell'integrità dei dati stessi, dell'efficienza e delle prestazioni del sistema-database;
- amministratore della rete (network administrator) che gestisce l'infrastruttura di rete (apparati come hub, switch e router) ed effettua le diagnosi dei problemi che i vari personal computer o server hanno con questa
- amministratore della sicurezza (security administrator), compresa la gestione dei dispositivi tipo firewall e l'adozione di misure di sicurezza generale;
- amministratore web (web administrator), che si preoccupa della gestione dei servizi web, ovvero servizi che permettono ad utenti interni e/o esterni di accedere ai siti web;

E' evidente che, a seconda della complessità della struttura, questi ruoli potranno essere coperti da una o più persone.

Non rientrano invece in questa 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 funzioni principali dell'AdS sono richiamate nell' allegato B al Codice<sup>3</sup>. Infatti, la maggior parte dei compiti previsti nel medesimo allegato spettano tipicamente all'AdS: 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. Tali operazioni possono comportare un'effettiva capacità di azione su informazioni da considerarsi a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

Da notare poi che, secondo il Codice penale, buona parte delle funzioni tecniche attribuite all'AdS, possono rappresentare una circostanza aggravante, se svolte da chi commette un reato. È il caso ad esempio dell' accesso abusivo a sistema informatico o telematico (art. 615-ter) e di frode informatica (art. 640-ter), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (articoli 635-bis e ter) e di danneggiamento di sistemi informatici e telematici (articoli 635-quater e quinquies).

## **A chi si rivolge il provvedimento e aree di esenzione**

Il provvedimento si rivolge a tutti i soggetti pubblici e privati che trattano dati personali con sistemi di elaborazione elettronica. Sono esclusi i trattamenti effettuati in ambito pubblico e

---

<sup>3</sup> Allegato B. Disciplinare tecnico in materia di misure minime di sicurezza

privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle misure di semplificazione introdotte nel corso del 2008 per legge<sup>4</sup>.

In sostanza, non debbono adeguarsi al provvedimento coloro che utilizzano dati personali non sensibili, oppure che trattano, come unici dati sensibili, quelli riferiti ai propri dipendenti e collaboratori (anche a progetto), quelli costituiti dallo stato di salute o malattia e dall'adesione ad organizzazioni sindacali o a carattere sindacale, oppure, ancora, quei soggetti che trattano dati personali unicamente per correnti finalità amministrative e contabili. Si tratta, generalmente, di piccole e medie imprese, sia pubbliche che private, di artigiani, di commercianti e di liberi professionisti.

## AdS interno e AdS esterno

Per prima cosa, e per non incorrere in facili equivoci, è importante ripetere ancora una volta che NON sono Amministratori di Sistema 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.

Il provvedimento prevede per il titolare un diverso comportamento nella nomina dell'AdS a seconda che questo operi o meno dentro l'azienda. Poiché la casistica è molto ampia, vediamo di ricorrere ad alcuni esempi fra i più frequenti:

1. Tutto il sistema informatico risiede in remoto e si accede alle applicazioni tramite interfaccia web (internet) [è un caso estremo ma possibile]  
*-in questo caso il titolare nomina responsabile la ditta esterna -*
2. Il sistema informatico è in casa, l'AdS interno fa la manutenzione ordinaria mentre la ditta esterna interviene "solo occasionalmente" [caso abbastanza frequente]  
*- il titolare nomina l'AdS interno e basta-*
3. Il sistema informatico è in casa, l'AdS interno governa parti del sistema informatico, mentre altre (server, database ...) sono seguite da ditta/e esterne [caso possibile]  
*-Il titolare nomina l'AdS interno e nomina responsabile la ditta esterna-*
4. Il sistema informatico è in casa, l'AdS interno NON c'è, la ditta esterna fa tutta la manutenzione, sia ordinaria che straordinaria [caso abbastanza frequente]  
*- il titolare nomina responsabile la ditta esterna che a sua volta nomina gli AdS-*
5. Il sistema informatico è in casa, l'AdS interno fa tutto quindi non c'è nessuna ditta esterna [caso estremo e contrario al primo ma possibile]  
*- il titolare nomina l'AdS interno e basta -*

---

<sup>4</sup> (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 27 novembre 2008).

## **Le misure e gli accorgimenti tecnici e organizzativi prescritti**

Oltre agli adempimenti noti, il Garante fissa alcuni punti che il titolare del trattamento deve rispettare nei confronti dell'amministratore di sistema. E precisamente:

- a. Valutazione delle caratteristiche soggettive;
- b. Designazioni individuali;
- c. Elenco degli amministratori di sistema;
- d. Servizi in outsourcing;
- e. Verifica delle attività;
- f. Registrazione degli accessi.

### *a. Valutazione delle caratteristiche soggettive degli AdS*

Il titolare o il responsabile, all'atto dell'attribuzione delle funzioni di AdS, deve valutare preventivamente le caratteristiche personali del soggetto che deve possedere requisiti di esperienza, capacità e affidabilità. Altra garanzia importante è il rispetto (oltre la conoscenza) delle disposizioni in materia di trattamento, sicurezza compresa.

Questi requisiti richiedono valutazioni sia qualitative (fortemente soggettive) che quantitative (ad es. un riscontro oggettivo può essere dato da esperienze lavorative, studi, corsi, master..); tuttavia molto dipende dalla discrezionalità del titolare o del responsabile che dovranno misurare le proprie scelte secondo la realtà in cui opera l'azienda o l'ente. È evidente che in questo campo il provvedimento non può stabilire criteri rigorosi; è comunque richiesto che i criteri di valutazione siano almeno equivalenti a quelli richiesti per la designazione dei responsabili<sup>5</sup>.

### *b. Designazioni individuali*

Il titolare o il responsabile designano individualmente l'AdS secondo un preciso profilo di autorizzazione affidandogli specifici ambiti di operatività e facendo attenzione ad evitare ogni accesso ai dati eccedenti le necessità.

Quindi, il titolare o il responsabile dovranno predisporre una lettera di incarico per l'amministratore di sistema che conterrà:

- attestazione che l'incaricato ha le caratteristiche richieste dalla legge;
- elencazione analitica degli ambiti di operatività richiesti e consentiti in base al profilo di autorizzazione assegnato;
- indicazione delle "verifiche" almeno annuali che il titolare svolgerà sulle attività svolte dall'amministratore di sistema;
- indicazione che la nomina ed il relativo nominativo sarà comunicato al personale ed eventualmente a terzi nei modi richiesti dalla legge.

La lettera dovrà essere sottoscritta dall'AdS per accettazione.

E se l'amministratore è esterno? Accade spesso che strutture medio piccole ricorrano all'esterno per le funzioni di amministratore di sistema, oppure che ditte esterne effettuino interventi sui sistemi e sui dati anche da remoto e, quindi, possano accedere ai trattamenti

---

<sup>5</sup> Art. 29 D.Lgs. 196/2003

aziendali. Con l'aggiornamento apportato dal recente provvedimento del Garante<sup>6</sup>, sarà il responsabile esterno (e quindi la ditta che fornisce il servizio) a provvedere alla nomina dell'AdS al proprio interno. Sarà, quindi, opportuno che il titolare del trattamento notifichi al responsabile esterno questa incombenza e che, a sua volta, quest'ultimo confermi al titolare la nomina del/gli AdS.

#### *c. Elenco degli AdS*

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Nel caso di servizi di amministrazione di sistema affidati in *outsourcing* il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.<sup>7</sup>

Qualora l'attività degli AdS riguardi anche indirettamente servizi o sistemi che trattano informazioni di carattere personale di lavoratori, i titolari nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli AdS avvalendosi a seconda delle opportunità: dell'informativa<sup>8</sup>, della intranet aziendale, della pubblicazione all'albo pretorio, oppure della affissione presso le varie sedi di lavoro.

#### *d. Verifica delle attività*

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

Ci possiamo chiedere quanto queste verifiche possano essere fattibili ed eventualmente attendibili, considerato che per gran parte delle misure in esame l'unico esperto in materia è di solito l'AdS che finirebbe per rivestire la figura del "verificatore" e "verificato" allo stesso tempo.

Tuttavia è auspicabile che le attività da verificare, indicate nella lettera di incarico (v. il precedente punto b), siano scelte con sufficiente ocularità in modo da non ingenerare false interpretazioni e da essere facilmente "auditabili".

#### *e. Registrazione degli accessi*

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 adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e

---

<sup>6</sup> Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento. 25 giugno 2009 [doc. web n. 1626595] (G.U. n. 149 del 30 giugno 2009)

<sup>7</sup> 2 d) del dispositivo del provvedimento del Garante del 27 novembre 2008 [doc. web n. 1577499]

<sup>8</sup> art. 13 del Codice della Privacy

la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Questa misura ha suscitato molte perplessità sul piano anche operativo. I chiarimenti successivi venuti dal Garante<sup>9</sup> hanno ridimensionato il problema e semplificato la sua attuazione, anche se non vengono fissate regole rigorose, in quanto il corretto comportamento deve essere commisurato al contesto del "Sistema Privacy" che abbiamo di fronte.

Per quanto riguarda le registrazioni, di norma i requisiti richiesti possono essere soddisfatti da funzionalità già disponibili nei più diffusi sistemi operativi, senza richiedere necessariamente l'uso di strumenti *software* o *hardware* aggiuntivi. Gli *event records* generati dai sistemi di autenticazione contengono usualmente i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento, una descrizione dell'evento (sistema di elaborazione o *software* utilizzato, se si tratti di un evento di *log-in*, di *log-out*, o di una condizione di errore, quale linea di comunicazione o dispositivo terminale sia stato utilizzato...).

Le caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di *log* sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con apposito *software*. Il requisito può essere ragionevolmente soddisfatto con la strumentazione *software* in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di *log* su supporti di memorizzazione non riscrivibili.

## Cosa deve fare il Titolare

Sulla base di quanto detto, quali passi deve compiere il titolare nei confronti dell'AdS?

- a. Adozione di specifiche cautele, accorgimenti e misure (organizzative e tecniche) idonee a consentire un agevole controllo, da parte del titolare, sull'attività dell'AdS;
- b. Individuazione e nomina dell'AdS;
- c. Individuazione, nel provvedimento di nomina, degli ambiti di operatività consentiti all'AdS in base al profilo di autorizzazione assegnato ;
- d. Predisposizione di un elenco con gli estremi identificativi degli AdS e con le funzioni agli stessi attribuite;
- e. Inclusione del suddetto elenco in un documento interno all'azienda che deve essere sempre aggiornato e sempre reso disponibile per eventuali controlli da parte del Garante;
- f. Qualora gli amministratori di sistema operino anche su dati ed informazioni personali relativi ai lavoratori, l'elenco deve essere reso noto a questi ultimi secondo le più diverse modalità;
- g. Predisposizione dl piano operativo dell'amministratore di sistema (attività di cui all'allegato B del Codice).

---

<sup>9</sup> V. anche le FAQ allegato al provvedimento del 27 novembre 2008 [doc. web n. 1577499]

## Aspetto sanzionatorio

Quali responsabilità si assume il titolare qualora non adotti le misure previste nel provvedimento?

Il Codice della privacy non prevede specifiche sanzioni in caso di mancata nomina dell'AdS, ma prevede sanzioni sia amministrative che penali per la mancata adozione delle misure di sicurezza.

Per quanto riguarda le sanzioni amministrative, il non affidare un tale compito di responsabilità ad un soggetto professionalmente affidabile ed esperto, espone il titolare ad un maggior rischio di violazione delle norme sulle misure di sicurezza.

Per quanto riguarda le conseguenze sanzionatorie di natura civilistica, è bene ricordare che il titolare è sempre soggetto a responsabilità civile e condannabile al risarcimento del danno qualora l'omissione o la non perfetta adozione di misure di sicurezza abbia cagionato a terzi un danno ingiusto ("Risarcimento per fatto illecito")<sup>10</sup>.

Sotto l'aspetto penale, infine, va ricordato che la violazione delle norme sulle misure minime di sicurezza è penalmente sanzionata con l'arresto sino a due anni<sup>11</sup>.

---

<sup>10</sup> art. 2043 del codice civile

<sup>11</sup> art. 169 co 1 D.Lgs.196/2003