

SCHEDA TECNICA N. 2/10

L'AMMINISTRATORE DI SISTEMA E LA PRIVACY



a cura di Gianantonio Poli

Commissione Consultiva Organizzazione dello Studio e informatica

Coordinatore: Gianantonio Poli. Delegato del Consiglio: Elisabetta Migliorati.
Membri: Aldo Bertana, Francesca Bertelli, Luca Calzolari, Claudio Cerutti, Davide Felappi,
Filippo Fornari, Stefano Guerrini, Biagio Notario, Alberto Odorici, Aldo Massimo Rossi,
Paolo Tebaldini, Carlo Valetti.

INDICE

1. Premessa
2. Il Provvedimento del Garante
3. L' Amministratore di Sistema
4. L' ambito di applicazione
5. Le misure da adottare
 - 5.1 Valutazione delle caratteristiche soggettive
 - 5.2 Designazioni individuali
 - 5.3 Elenco degli Amministratori di Sistema
 - 5.4 Verifica delle attività
 - 5.5 Registrazione degli accessi
6. Gli adempimenti del Titolare
7. Le sanzioni

1. Premessa

Il Garante per il trattamento dei dati personali, con un recente Provvedimento, ha definitivamente chiarito la figura ed il ruolo di un soggetto misterioso che era già ben noto a chi si è occupato di Privacy e a chi ha affrontato l'applicazione delle norme del Codice sulla Privacy presso le aziende, gli enti e gli studi professionali.

Questo soggetto, mai ben definito dal Codice, e sempre difficilmente collocabile all'interno dell'ordinamento normativo riguardante la privacy, è l'**Amministratore di Sistema (AdS)** (1).

Con tale Provvedimento l'Amministratore di Sistema d'ora in poi assume la stessa importanza delle altre figure previste dalla normativa della Privacy quali il **Titolare**, il **Responsabile**, al quale è equiparato, e l'**Incaricato**.

2. Il Provvedimento del Garante

Il Garante ha voluto richiamare tutti i titolari dei trattamenti dei dati mediante strumenti elettronici alla necessità di prestare massima attenzione ai rischi e alle criticità presenti nell'affidamento di incarichi agli Amministratori di Sistema.

Il Garante ha prescritto una serie di norme relative alla figura dell'Amministratore di Sistema che comportano interventi di carattere organizzativo e **che sono entrati in vigore a partire dal 15 dicembre 2009**.

Questo nuovo adempimento non si è esaurito nella mera predisposizione di una nuova lettera di incarico ma ha richiesto al Titolare del trattamento una serie di misure e di adempimenti riguardo all'esercizio dei doveri di controllo sulle attività dell'Amministratore di Sistema.

Allo scopo di facilitare il compito per quelle realtà nelle quali i servizi informatici sono svolti da ditte esterne, il Garante ha consentito ai Titolari del trattamento di poter nominare Responsabili esterni del trattamento che a loro volta provvedono a nominare gli Amministratori di Sistema con tutti gli adempimenti e le misure previste.

In caso di incarico a terzi in *outsourcing*, l'onere di tali operazioni ricadrà quindi sul Responsabile esterno del trattamento dei dati. Il Titolare del trattamento, cui spetta sempre e comunque il compito di controllo, sarà libero da onerosi adempimenti.

(1)

- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema del 27 novembre 2008.

- Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema del 12 febbraio 2009.

- Amministratori di sistema: avvio di una consultazione pubblica del 21 aprile 2009 (G.U. n. 105 dell'8 maggio 2009).

- 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 del 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009).

- Provvedimento del Garante del 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009).

3. L'Amministratore di sistema

Il Provvedimento definisce l'Amministratore di Sistema (AdS) come la figura professionale dedicata alla gestione e alla manutenzione degli impianti di elaborazione con cui vengono effettuati i trattamenti di dati personali. Può essere un ente, una società o anche una persona fisica.

L'Amministratore di Sistema può assumere vari ruoli e funzioni a seconda delle competenze assegnate che possono riunirsi anche in capo ad una sola persona :

- **Amministratore delle basi di dati** (Database Administrator), responsabile dell'integrità dei dati stessi, dell'efficienza e delle prestazioni del sistema-database, dei back-up e dei disaster recovery;
- **Amministratore della rete** (Network Administrator) che gestisce l'infrastruttura delle reti e cioè gli apparati fisici come macchine, cavi, sistemi wi-fi, hub, switch e router ed effettua le diagnosi dei vari computer o server presentano in rete ;
- **Amministratore della sicurezza** (Security Administrator), che si occupa della custodia delle credenziali, della gestione dei sistemi di autenticazione e di autorizzazione, dei privilegi di accesso nonché della gestione dei dispositivi di sicurezza firewall, antivirus e l'adozione di misure di sicurezza in generale;
- **Amministratore web** (Web Administrator), che si preoccupa della gestione dei servizi web, in internet e intranet, ovvero servizi che permettono ad utenti interni e/o esterni di accedere ai siti web e ai servizi di rete internet in upload e download e di navigazione in generale ;

Le funzioni principali dell'Amministratore di Sistema sono richiamate all' allegato B del Codice sulla Privacy, in quanto la maggior parte dei compiti previsti spettano 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, all'assegnazione di privilegi di accesso. Tali operazioni possono comportare una capacità di azione su informazioni aventi caratteristiche di un trattamento di dati personali.

La particolare funzione dell'Amministratore di Sistema, può rappresentare una circostanza aggravante, se svolta da chi commette i seguenti reati :

- accesso abusivo a sistema informatico o telematico (art. 615-ter) e di frode informatica (art. 640-ter), - danneggiamento di informazioni, dati e programmi informatici (articoli 635-bis e ter) e - danneggiamento di sistemi informatici e telematici (articoli 635-quater e quinquies).

4. L'ambito di applicazione

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 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. (art. 29 D.L. 25 giugno 2008, n. 112, convertito con modificazioni Legge 6 agosto 2008, n. 133 - art. 34 del Codice sulla Privacy - Provvedimento del Garante 27 novembre 2008).

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, 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.

Il provvedimento prevede per il titolare un diverso comportamento nella nomina dell'Amministratore di Sistema, a seconda che questo operi o meno dentro l'azienda.

Si elencano qui di seguito alcune situazioni più frequenti:

- Il sistema informatico risiede in remoto e si accede alle applicazioni tramite interfaccia web (internet). In questo caso il titolare nomina il Responsabile del trattamento, quale anche Amministratore di Sistema, una ditta esterna ;
- Il sistema informatico è interno, una ditta esterna interviene “solo occasionalmente” mentre il Responsabile del trattamento gestisce l'intero apparato del sistema informatico. In questo caso l'Amministratore di Sistema fa la “manutenzione ordinaria”. Il Titolare del trattamento nomina l'Amministratore di Sistema interno che può coincidere con il Responsabile del trattamento ;
- Il sistema informatico è interno, una ditta esterna segue buona parte del sistema informatico (server, database etc.). In questo caso il Titolare del trattamento nomina l'Amministratore di Sistema interno e nomina Responsabile del trattamento la ditta esterna ;
- Il sistema informatico è interno, una ditta esterna fa la manutenzione sia ordinaria che straordinaria e gestisce l'intero sistema informatico . In questo caso molto frequente il titolare nomina Responsabile del trattamento la ditta esterna che a sua volta nomina gli Amministratori di Sistema all'interno del suo organico;
- Il sistema informatico è interno, non c'è nessuna ditta esterna che fa la manutenzione e che gestisce il sistema informatico. In questo caso il titolare nomina il Responsabile interno del trattamento che sarà anche Amministratore di Sistema.

5. Le misure da adottare

Il Garante per la *Privacy* al riguardo fissa i seguenti accorgimenti tecnici e organizzativi che il Titolare o il Responsabile del trattamento dei dati deve rispettare nei confronti dell'Amministratore di Sistema :

5.1 Valutazione delle caratteristiche soggettive

Il Titolare e il Responsabile del trattamento devono scegliere il soggetto che verrà nominato Amministratore di Sistema valutandone i requisiti di **esperienza, capacità e affidabilità**.

L'Amministratore di Sistema deve garantire a sua volta il rispetto delle disposizioni in materia di privacy e sicurezza e la trasparenza nell'operato.

Il provvedimento del Garante non stabilisce criteri o livelli di professionalità. I criteri di valutazione sono comunque almeno equivalenti a quelli richiesti per la designazione dei Responsabili del trattamento di cui all' art. 29 D.Lgs. 196/2003.

5.2 Designazioni individuali

Il Titolare o il Responsabile del trattamento dei dati designano individualmente l'AdS secondo un preciso profilo di autorizzazione. La lettera di incarico all'Amministratore di sistema dovrà contenere :

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

Nel caso molto frequente che aziende o studi professionali abbiano piccole strutture informatiche e che ditte esterne effettuino interventi sui sistemi e sui dati anche da remoto, il Responsabile del trattamento potrà essere esterno e provvederà alla nomina dell'Amministratore di sistema al proprio interno. E' opportuno in questo caso che il Titolare del trattamento notifichi al Responsabile del trattamento esterno questa incombenza e che, a sua volta, quest'ultimo confermi al Titolare del trattamento la nomina di uno o più Amministratori di Sistema.

5.3 Elenco degli Amministratori di Sistema

I dati identificativi degli Amministratori di sistema, con la specifica delle funzioni e degli ambiti ad essi attribuiti, devono essere annotati 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 del trattamento devono garantire l'annotazione dei dati identificativi delle persone fisiche preposte quali Amministratori di sistema.

I Titolari del trattamento, qualora siano datori di lavoro, sono tenuti a rendere nota o conoscibile l'identità degli Amministratori di sistema nel caso che durante il trattamento dei dati o lo svolgimento di servizi di informazione venga a conoscenza indirettamente di dati di carattere personale dei lavoratori dipendenti.

5.4 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 o dei Responsabili del trattamento, in modo da monitorare la rispondenza alle funzioni ed ai compiti assegnati ed il rispetto delle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste.

5.5 Registrazione degli accessi

Il Titolare o il Responsabile del trattamento dovrà adottare 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 la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Gli *event records* generati dai sistemi di autenticazione contengono 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 con apposito *software*. Il requisito può essere ragionevolmente soddisfatto con l'esportazione periodica dei dati di *log* su supporti di memorizzazione non riscrivibili.

6. Gli adempimenti del Titolare

Di seguito si riporta un elenco degli adempimenti a carico del Titolare del trattamento dei dati :

- Provvedere alla nomina dell' Amministratore di Sistema dopo attenta valutazione di esperienza, capacità e affidabilità del soggetto designato;
- Prevedere, in fase di nomina, le funzioni e gli ambiti di operatività consentiti all'Amministratore di Sistema;
- Riportare sul DPS l'elenco degli Amministratori di Sistema e le funzioni e gli ambiti a loro attribuiti ;
- Verificare annualmente le attività svolte dall'Amministratore di Sistema in relazione al rispetto delle misure di sicurezza previste dal DPS;
- Prevedere la registrazione degli accessi dell'Amministratore di Sistema al sistema e agli archivi. Tali registrazioni devono comprendere riferimenti temporali, riferimento all'evento che le ha generate e devono essere conservate almeno per sei mesi .

7. Le sanzioni

Il Codice della privacy non prevede specifiche sanzioni in caso di mancata nomina dell'Amministratore di Sistema, 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, 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") art. 2043 del codice civile .

Sotto l'aspetto penale la violazione delle norme sulle misure minime di sicurezza è penalmente sanzionata con l'arresto sino a due anni ex art. 169 co 1 D.Lgs.196/2003.

NOMINA DI AMMINISTRATORE DI SISTEMA FAC SIMILE

Il sottoscritto _____ [*indicare il nominativo/denominazione del Titolare o del Responsabile del Trattamento dei dati*], con sede legale/residente in [_____], Via [_____] n.[___], in qualità di _____ [*Titolare/Responsabile*] del trattamento dei dati personali ai sensi del D.Lgs. 196/2003,

designa

il Sig. [_____] nato a [_____] il [_____] e residente a [_____] Via [_____] n.[___] per suo conto/in qualità di [_____] della società [_____] con sede in [_____] Via[_____] n.[___]

Amministratore di Sistema

ai sensi e per gli effetti di cui al provvedimento del Garante per la protezione dei dati personali datato 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) pubblicato sulla G.U. n. 300 del 24 dicembre 2008, con riferimento ai dati personali trattati nell'ambito della gestione e della manutenzione di un impianto di elaborazione o di sue componenti.

Data [_____]

Firma [_____]

Per accettazione

L'Amministratore di Sistema

[_____]

Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008
(G.U. n. 300 del 24 dicembre 2008)

(così modificato in base al provvedimento del [25 giugno 2009](#))

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196) e, in particolare, gli artt. 31 ss. e 154, comma 1, lett. c) e h), nonché il disciplinare tecnico in materia di misure minime di sicurezza di cui all'[allegato B](#) al medesimo Codice;

VISTI gli atti d'ufficio relativi alla protezione dei dati trattati con sistemi informatici e alla sicurezza dei medesimi dati e sistemi;

RILEVATA l'esigenza di intraprendere una specifica attività rispetto ai soggetti preposti ad attività riconducibili alle mansioni tipiche dei c.d. "amministratori di sistema", nonché di coloro che svolgono mansioni analoghe in rapporto a sistemi di elaborazione e banche di dati, evidenziandone la rilevanza rispetto ai trattamenti di dati personali anche allo scopo di promuovere presso i relativi titolari e nel pubblico la consapevolezza della delicatezza di tali peculiari mansioni nella "Società dell'informazione" e dei rischi a esse associati;

CONSIDERATA l'esigenza di consentire più agevolmente, nei dovuti casi, la conoscibilità dell'esistenza di tali figure o di ruoli analoghi svolti in relazione a talune fasi del trattamento all'interno di enti e organizzazioni;

RITENUTA la necessità di promuovere l'adozione di specifiche cautele nello svolgimento delle mansioni svolte dagli amministratori di sistema, unitamente ad accorgimenti e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del titolare (*due diligence*);

CONSTATATO che lo svolgimento delle mansioni di un amministratore di sistema, anche a seguito di una sua formale designazione quale responsabile o incaricato del trattamento, comporta di regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti;

RILEVATA la necessità di richiamare l'attenzione su tale rischio del pubblico, nonché di persone giuridiche, pubbliche amministrazioni e di altri enti (di seguito sinteticamente individuati con l'espressione "titolari del trattamento": art. 4, comma 1, lett. f) del Codice) che impiegano, in riferimento alla gestione di banche dati o reti informatiche, sistemi di elaborazione utilizzati da una molteplicità di incaricati con diverse funzioni, applicative o sistemiche;

RILEVATO che i titolari sono tenuti, ai sensi dell'art. 31 del Codice, ad adottare misure di sicurezza "idonee e preventive" in relazione ai trattamenti svolti, dalla cui mancata o non idonea predisposizione possono derivare responsabilità anche di ordine penale e civile (artt. 15 e 169 del Codice);

CONSTATATO che l'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti;

CONSIDERATO inoltre che, qualora ritenga facoltativamente di designare uno o più responsabili del trattamento, il titolare è tenuto a individuare solo soggetti che "*per esperienza, capacità ed 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);

RITENUTO che i titolari di alcuni trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili, i quali pongono minori rischi per gli interessati e sono stati pertanto oggetto di recenti misure di semplificazione (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 6 novembre 2008](#)), debbano essere allo stato esclusi dall'ambito applicativo del presente provvedimento;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Francesco Pizzetti;

PREMESSO:

1. Considerazioni preliminari

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche 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.

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (*backup/recovery*), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione *hardware* comportano infatti, 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.

La rilevanza, la specificità e la particolare criticità del ruolo dell'amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante. Ci si riferisce, in particolare, all'abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di 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 (artt. 635 *bis* e *ter*) e di danneggiamento di sistemi informatici e telematici (artt. 635 *quater* e *quinques*) di recente modifica¹.

La disciplina di protezione dei dati previgente al Codice del 2003 definiva l'amministratore di sistema, individuandolo quale "soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione" (art. 1, comma 1, lett. c) d.P.R. 318/1999).

Il Codice non ha invece incluso questa figura tra le proprie definizioni normative. Tuttavia 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. 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.

Nel loro complesso, le norme predette mettono in rilievo la particolare capacità di azione propria degli amministratori di sistema e la natura fiduciaria delle relative mansioni, analoga a quella che, in un contesto del tutto differente, caratterizza determinati incarichi di custodia e altre attività per il cui svolgimento è previsto il possesso di particolari requisiti tecnico-organizzativi, di onorabilità, professionali, morali o di condotta, a oggi non contemplati per lo svolgimento di uno dei ruoli più delicati della "Società dell'informazione"².

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.

L'Autorità ravvisa inoltre l'esigenza di individuare in questa sede alcune prime misure di carattere organizzativo che favoriscano una più agevole conoscenza, nell'ambito di organizzazioni ed enti pubblici e privati, dell'esistenza di determinati ruoli tecnici, delle responsabilità connesse a tali mansioni e, in taluni casi, dell'identità dei soggetti che operano quali amministratori di sistema in relazione ai diversi servizi e banche di dati.

2. Quadro di riferimento normativo

Nell'ambito del Codice il presente provvedimento si richiama, in particolare, all'art. 154, comma 1, lett. h), rientrando tra i compiti dell'Autorità quello di promuovere la "conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati".

La lett. c) del medesimo comma 1 prevede poi la possibilità, da parte del Garante, di prescrivere misure e

accorgimenti, specifici o di carattere generale, che i titolari di trattamento sono tenuti ad adottare.

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 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 idonea designazione.

4. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici

Di seguito sono indicati gli accorgimenti e le misure che vengono prescritti ai sensi dell'art. 154, comma 1, lett. c) del Codice, a tutti i titolari dei trattamenti di dati personali effettuati con strumenti elettronici, esclusi, allo stato, quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle recenti misure di semplificazione (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; [Prov. Garante 6 novembre 2008](#)).

I seguenti accorgimenti e misure lasciano impregiudicata l'adozione di altre specifiche cautele imposte da discipline di settore per particolari trattamenti o che verranno eventualmente prescritte dal Garante ai sensi dell'art. 17 del Codice.

Per effetto del presente provvedimento:

4.1 Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'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.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

4.2 Designazioni individuali

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

4.3 Elenco degli amministratori di sistema³

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.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal [provvedimento](#) del Garante n. 13 del 1° marzo 2007 (in *G.U.* 10 marzo 2007, n. 58); in alternativa si possono anche utilizzare strumenti di comunicazione interna (a es., *intranet* aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

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

4.4 Verifica delle attività³

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

4.5 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 di verifica per cui sono richieste.

Le registrazioni 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.

5. Tempi di adozione delle misure e degli accorgimenti

Per tutti i titolari dei trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del presente provvedimento, le misure e gli accorgimenti di cui al punto 4 dovranno essere introdotti al più presto e comunque entro, e non oltre, il termine che è congruo stabilire, in centoventi giorni dalla medesima data.

Per tutti gli altri trattamenti che avranno inizio dopo il predetto termine di trenta giorni dalla pubblicazione, gli accorgimenti e le misure dovranno essere introdotti anteriormente all'inizio del trattamento dei dati.

TUTTO CIÒ PREMESSO IL GARANTE:

1. ai sensi dell'art. 154, comma 1, lett. h) del Codice, 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 sull'esigenza di valutare con particolare attenzione l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema (*system administrator*), amministratore di base di dati (*database administrator*) o amministratore di rete (*network administrator*), laddove tali funzioni 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 e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato;

2. ai sensi dell'art. 154, comma 1, lett. c) del Codice prescrive l'adozione delle seguenti misure ai titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici, anche in ambito giudiziario e di forze di polizia (artt. 46 e 53 del Codice), salvo per quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che pongono minori rischi per gli interessati e sono stati oggetto delle misure di semplificazione introdotte di recente per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; *Prov. Garante* 6 novembre 2008):

a. Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e 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.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

b. Designazioni individuali

La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

c. Elenco degli amministratori di sistema³

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 da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i titolari pubblici e privati sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico di cui al [provvedimento](#) del Garante n. 13 del 1° marzo 2007 (in *G.U.* 10 marzo 2007, n. 58) o, in alternativa, mediante altri strumenti di comunicazione interna (*ad es.*, *intranet* aziendale, ordini di servizio a circolazione interna o bollettini) o tramite procedure formalizzate a istanza del lavoratore. Ciò, salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con diverse previsioni dell'ordinamento che disciplinino uno specifico settore.

d. Servizi in outsourcing³

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.

e. Verifica delle attività³

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.

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

3. dispone che le misure e gli accorgimenti di cui al punto 2 del presente dispositivo siano introdotti, per tutti i trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella *Gazzetta Ufficiale* del presente provvedimento, al più presto e comunque entro, e non oltre, il termine che è congruo stabilire in centoventi giorni dalla medesima data: per tutti gli altri trattamenti che avranno inizio dopo il predetto termine di trenta giorni dalla pubblicazione, gli accorgimenti e le misure dovranno essere introdotti anteriormente all'inizio del trattamento dei dati ([vedi proroga al punto c\) del pmvv 25 giugno 2009](#));

3 bis. dispone che l'eventuale attribuzione al responsabile del compito di dare attuazione alle prescrizioni di cui al punto 2, lett. d) ed e), avvenga nell'ambito della designazione del responsabile da parte del titolare del trattamento, ai sensi dell'art. 29 del Codice, o anche tramite opportune clausole contrattuali;⁴

4. dispone che copia del presente provvedimento sia trasmesso al Ministero della giustizia–Ufficio pubblicazione leggi e decreti per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica Italiana.

Roma, 27 novembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

(1) V., ad es., l'art. 5 l. 18 marzo 2008, n. 48 che prevede, oltre a una maggiore pena, la procedibilità d'ufficio nel caso in cui il reato sia commesso con "abuso della qualità di operatore del sistema".

(2) Per altro verso il legislatore, nell'intervenire in tema di "Società dell'informazione", ha previsto che i certificatori di firma elettronica, i quali sono preposti al trattamento dei dati connessi al rilascio del certificato di firma, debbano possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche, oltre ai requisiti tecnici necessari per lo svolgimento della loro attività (artt. 26, 27 e 29 del d.lg. 7 marzo 2005 n. 82).

(3) Così modificato in base al provvedimento del [25 giugno 2009](#)

(4) Aggiunto in base al provvedimento del [25 giugno 2009](#)

Provvedimento "Amministratori di sistema" del 27 novembre 2008

(G.U. n. 300 del 24 dicembre 2008)

Risposte alle domande più frequenti (FAQ) *

- 1 Cosa deve intendersi per "amministratore di sistema"?
- 2 Cosa vuol dire la locuzione "Qualora l'attività degli ADS riguardi anche indirettamente servizi o sistemi che..."
- 3 Il caso di uso esclusivo di un *personal computer* da parte di un solo amministratore di sistema rientra nell'ambito applicativo del [provvedimento](#)?
- 4 Relativamente all'obbligo di registrazione degli accessi logici degli AdS, sono compresi anche i sistemi *client* oltre che quelli *server*?
- 5 Cosa si intende per operato dell'amministratore di sistema soggetto a controllo almeno annuale?
- 6 Chiarire i casi di esclusione dall'obbligo di adempiere al [provvedimento](#).
- 7 Cosa si intende per descrizione analitica degli ambiti di operatività consentiti all'ADS?
- 8 Oltre alla *job description* si deve andare più in dettaglio? Si devono indicare i singoli sistemi e le singole operazioni affidate?
- 9 Cosa si intende per *access log* (*log-in*, *log-out*, tentativi falliti di accesso, altro?...)
- 10 Laddove il *file* di *log* contenga informazioni più ampie, va preso tutto il *log* o solo la riga relativa all'*access log*?
- 11 Come va interpretata la caratteristica di completezza del *log*? Si intende che ci devono essere tutte le righe? L'adeguatezza rispetto allo scopo della verifica deve prevedere un'analisi dei rischi?
- 12 Come va interpretata la caratteristica di inalterabilità dei *log*?
- 13 Si individuano livelli di robustezza specifici per la garanzia della integrità dei *log*?
- 14 Quali potrebbero essere gli scopi di verifica rispetto ai quali valutare l'adeguatezza?
- 15 Cosa dobbiamo intendere per evento che deve essere registrato nel *log*? Solo l'accesso o anche le attività eseguite?
- 16 Quali sono le finalità di *audit* che ci dobbiamo porre con la registrazione e raccolta di questi *log*?
- 17 Cosa si intende per "consultazione in chiaro"?
- 18 Il regime di conoscibilità degli amministratori di sistema è da intendersi per i soli trattamenti inerenti i dati del personale e dei lavoratori?
- 19 La registrazione degli accessi è relativa al sistema operativo o anche ai DBMS?
- 20 Nella designazione degli amministratori di sistema occorre valutare i requisiti morali?
- 21 Cosa si intende per "estremi identificativi" degli amministratori di sistema?
- 22 E' corretto affermare che l'accesso a livello applicativo non rientri nel perimetro degli adeguamenti, in quanto l'accesso a una applicazione informatica è regolato tramite profili autorizzativi che disciplinano per tutti gli utenti i trattamenti consentiti sui dati?
- 23 Si chiede se sia necessario conformarsi al [provvedimento](#) nel caso della fornitura di servizi di gestione sistemistica a clienti esteri (*housing*, *hosting*, gestione applicativa, archiviazione remota...) da parte di una società italiana non titolare dei dati gestiti.
- 24 Si possono ritenere esclusi i trattamenti relativi all'ordinaria attività di supporto delle manutenzione degli immobili sociali ecc...). Ci si riferisce ai trattamenti con strumenti elettronici finalizzati, ad esempio, alla gestione dell'autoparco, alle procedure di acquisto dei materiali di consumo, alla aziende, che non riguardino dati sensibili, giudiziari o di traffico telefonico/telematico?



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 personali.

Il Garante non ha inteso equiparare gli "operatori di sistema" di cui agli articoli del Codice penale relativi ai delitti informatici, con gli "amministratori di sistema": questi ultimi sono dei particolari operatori di sistema, dotati di specifici privilegi.

Anche il riferimento al d.P.R. 318/1999 nella premessa del [provvedimento](#) è puramente descrittivo poiché la figura definita in quell'atto normativo (ormai a brogato) è di minore portata rispetto a quella cui si fa riferimento nel provvedimento.

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*.



2) Cosa vuol dire la locuzione "Qualora l'attività degli ADS riguardi anche indirettamente servizi o sistemi

che..."

I titolari sono tenuti a instaurare un regime di conoscibilità dell'identità degli amministratori di sistema, quale forma di trasparenza interna all'organizzazione a tutela dei lavoratori, nel caso in cui un amministratore di sistema, oltre a intervenire sotto il profilo tecnico in generici trattamenti di dati personali in un'organizzazione, tratti anche dati personali riferiti ai lavoratori operanti nell'ambito dell'organizzazione medesima o sia nelle condizioni di acquisire conoscenza di dati a essi riferiti (in questo senso il riferimento nel testo del [provvedimento](#) all'"anche indirettamente...").



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 previsioni relative alla verifica delle attività dell'amministratore né la tenuta del *log* degli accessi informatici.



4) Relativamente all'obbligo di registrazione degli accessi logici degli AdS, sono compresi anche i sistemi *client* oltre che quelli *server*?

Sì, anche i *client*, intesi come "postazioni di lavoro informatizzate", sono compresi tra i sistemi per cui devono essere registrati gli accessi degli AdS.

Nei casi più semplici tale requisito può essere soddisfatto tramite funzionalità già disponibili nei più diffusi sistemi operativi, senza richiedere necessariamente l'uso di strumenti *software* o *hardware* aggiuntivi. Per esempio, la registrazione locale dei dati di accesso su una postazione, in determinati contesti, può essere ritenuta idonea al corretto adempimento qualora goda di sufficienti garanzie di integrità.

Sarà comunque con valutazione del titolare che dovrà essere considerata l'idoneità degli strumenti disponibili oppure l'adozione di strumenti più sofisticati, quali la raccolta dei *log* centralizzata e l'utilizzo di dispositivi non riscrivibili o di tecniche crittografiche per la verifica dell'integrità delle registrazioni.



5) Cosa si intende per operato dell'amministratore di sistema soggetto a controllo almeno annuale?

È da sottoporre a verifica l'attività svolta dall'amministratore di sistema nell'esercizio delle sue funzioni. Va verificato che le attività svolte dall'amministratore di sistema siano conformi alle mansioni attribuite, ivi compreso il profilo relativo alla sicurezza.



6) Chiarire i casi di esclusione dall'obbligo di adempiere al [provvedimento](#).

Sono esclusi i trattamenti effettuati in ambito pubblico e 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 (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del [Codice](#); Prov. Garante [27 novembre 2008](#)).



7) Cosa si intende per descrizione analitica degli ambiti di operatività consentiti all'ADS? [Rif. comma 2, lettera d]

Il [provvedimento](#) prevede che all'atto della designazione di un amministratore di sistema, venga fatta "elencazione analitica" degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, ovvero la descrizione puntuale degli stessi, evitando l'attribuzione di ambiti insufficientemente definiti, analogamente a quanto previsto al

comma 4 dell'art. 29 del [Codice](#) riguardante i responsabili del trattamento.



8) Oltre alla *job description* si deve andare più in dettaglio? Si devono indicare i singoli sistemi e le singole operazioni affidate?

No, è sufficiente specificare l'ambito di operatività in termini più generali, per settori o per aree applicative, senza obbligo di specificarlo rispetto a singoli sistemi, a meno che non sia ritenuto necessario in casi specifici.



9) Cosa si intende per *access log* (*log-in*, *log-out*, tentativi falliti di accesso, altro?...) [Rif. comma 2, lettera f]

Per *access log* si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi *software*.

Gli *event records* generati dai sistemi di autenticazione contengono usualmente i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento (*timestamp*), 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...).



10) Laddove il *file* di *log* contenga informazioni più ampie, va preso tutto il *log* o solo la riga relativa all'*access log*? [Rif. comma 2, lettera f]

Qualora il sistema di *log* adottato generi una raccolta dati più ampia, comunque non in contrasto con le disposizioni del [Codice](#) e con i principi della protezione dei dati personali, il requisito del [provvedimento](#) è certamente soddisfatto. Comunque è sempre possibile effettuare un'estrazione o un filtraggio dei *logfiles* al fine di selezionare i soli dati pertinenti agli AdS.



11) Come va interpretata la caratteristica di completezza del *log*? Si intende che ci devono essere tutte le righe? L'adeguatezza rispetto allo scopo della verifica deve prevedere un'analisi dei rischi?

La caratteristica di completezza è riferita all'insieme degli eventi censiti nel sistema di *log*, che deve comprendere tutti gli eventi di accesso interattivo che interessino gli amministratori di sistema su tutti i sistemi di elaborazione con cui vengono trattati, anche indirettamente, dati personali. L'analisi dei rischi aiuta a valutare l'adeguatezza delle misure di sicurezza in genere, e anche delle misure tecniche per garantire attendibilità ai *log* qui richiesti.



12) Come va interpretata la caratteristica di inalterabilità dei *log*?

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. In casi più complessi i titolari potranno ritenere di adottare sistemi più sofisticati, quali i *log server* centralizzati e "certificati".

È ben noto che il problema dell'attendibilità dei dati di *audit*, in genere, riguarda in primo luogo la effettiva generazione degli *auditable events* e, successivamente, la loro corretta registrazione e manutenzione. Tuttavia il [provvedimento](#) del Garante non affronta questi aspetti, prevedendo soltanto, come forma minima di documentazione dell'uso di un sistema informativo, la generazione del *log* degli "accessi" (*login*) e la loro archiviazione per almeno sei mesi in condizioni di ragionevole sicurezza e con strumenti adatti, in base al contesto in cui avviene il trattamento, senza alcuna pretesa di instaurare in modo generalizzato, e solo con le prescrizioni del

provvedimento, un regime rigoroso di registrazione degli *usage data* dei sistemi informativi.



13) Si individuano livelli di robustezza specifici per la garanzia della integrità?

No. La valutazione è lasciata al titolare, in base al contesto operativo (cfr. [faq n. 14](#)).



14) Quali potrebbero essere gli scopi di verifica rispetto ai quali valutare l'adeguatezza?

Quelli descritti al paragrafo 4.4 del [provvedimento](#) e ribaditi al punto 2, lettera e), del dispositivo. L'adeguatezza è da valutare in rapporto alle condizioni organizzative e operative dell'organizzazione.



15) Cosa dobbiamo intendere per evento che deve essere registrato nel log? Solo l'accesso o anche le attività eseguite?

Il [provvedimento](#) non chiede in alcun modo che vengano registrati dati sull'attività interattiva (comandi impartiti, transazioni effettuate) degli amministratori di sistema. Si veda la risposta alla [faq n. 11](#).



16) Quali sono le finalità di audit che ci dobbiamo porre con la registrazione e raccolta di questi log?

La raccolta dei *log* serve per verificare anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso...). L'analisi dei *log* può essere compresa tra i criteri di valutazione dell'operato degli amministratori di sistema.



17) Cosa si intende per "consultazione in chiaro"?

Il riferimento in premessa (par. 1 "Considerazioni preliminari") è alla criticità di mansioni che comportino la potenzialità di violazione del dato personale anche in condizioni in cui ne sia esclusa la conoscibilità, come può avvenire, per esempio, nel caso della cifratura dei dati.



18) Il regime di conoscibilità degli amministratori di sistema è da intendersi per i soli trattamenti inerenti i dati del personale e dei lavoratori?

Sì.



19) La registrazione degli accessi è relativa al sistema operativo o anche ai DBMS?

Tra gli accessi logici a sistemi e archivi elettronici sono comprese le autenticazioni nei confronti dei *data base management systems* (DBMS), che vanno registrate.



20) Nella designazione degli amministratori di sistema occorre valutare i requisiti morali? [Rif. comma 2, lettera a]

No. Il riferimento alle caratteristiche da prendere in considerazione, al comma 2, lettera a), del dispositivo, è all'esperienza, alla capacità e all'affidabilità del soggetto *designato*. Si tratta quindi di qualità tecniche, professionali e di condotta, non di requisiti morali.



21) Cosa si intende per "estremi identificativi" degli amministratori di sistema?

Si tratta del minimo insieme di dati identificativi utili a individuare il soggetto nell'ambito dell'organizzazione di appartenenza. In molti casi possono coincidere con nome, cognome, funzione o area organizzativa di appartenenza.



22) È corretto affermare che l'accesso a livello applicativo non rientri nel perimetro degli adeguamenti, in quanto l'accesso a una applicazione informatica è regolato tramite profili autorizzativi che disciplinano per tutti gli utenti i trattamenti consentiti sui dati?

Sì. L'accesso applicativo non è compreso tra le caratteristiche tipiche dell'amministratore di sistema e quindi non è necessario, in forza del [provvedimento](#) del Garante, sottoporlo a registrazione.



23) Si chiede se sia necessario conformarsi al [provvedimento](#) nel caso della fornitura di servizi di gestione sistemistica a clienti esteri (*housing, hosting, gestione applicativa, archiviazione remota...*) da parte di una società italiana non titolare dei dati gestiti.

Il [provvedimento](#) si rivolge solo ai titolari di trattamento. I casi esemplificati prefigurano al più una responsabilità di trattamento (secondo il Codice italiano), e sono quindi esclusi dall'ambito applicativo del provvedimento.



24) Si possono ritenere esclusi i trattamenti relativi all'ordinaria attività di supporto delle aziende, che non riguardino dati sensibili, giudiziari o di traffico telefonico/telematico? Ci si riferisce ai trattamenti con strumenti elettronici finalizzati, ad esempio, alla gestione dell'autoparco, alle procedure di acquisto dei materiali di consumo, alla manutenzione degli immobili sociali ecc...).

Tali trattamenti possono considerarsi compresi tra quelli svolti per ordinarie finalità amministrativo-contabili e, come tali, esclusi dall'ambito applicativo del [provvedimento](#).

* Così richiamate dal provvedimento "Amministratori di sistema: avvio di una consultazione pubblica" - 21 aprile 2009 [doc. web n. [1611986](#)]