

ADEMPIMENTI PRIVACY

Il Garante per la protezione dei dati personali ha **imposto** che sia predisposto un "elenco degli amministratori di sistema e loro caratteristiche", **entro il 15 dicembre 2009**

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 (*due diligence*)" sulle attività dell'amministratore.

1 IL NUOVO ADEMPIMENTO IN SINTESI

Con il **provvedimento a carattere generale del 27 novembre 2008** dal titolo "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, il Garante per la protezione dei dati personali **impone ai titolari di trattamenti di dati personali** (anche solo in parte gestiti mediante strumenti elettronici) **di predisporre un "elenco degli amministratori di sistema e loro caratteristiche"**.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel Documento Programmatico sulla Sicurezza, oppure, nei casi in cui il titolare non sia tenuto a redigere il DPS, **annotati comunque in un documento interno** da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Nella pratica occorre:

- individuare coloro che ricadono nella categoria di "amministratore di sistema"
- valutare l'esperienza, la capacità e l'affidabilità dei soggetti designati quali "amministratore di sistema" che devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza
- designare tali "amministratore di sistema" in modo individuale con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato
- verificare l'operato degli amministratori di sistema, con cadenza almeno annuale, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti
- registrare gli accessi ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema, mediante l'adozione di sistemi idonei alla registrazione degli accessi logici (autenticazione informatica).

Sono esclusi dall'ambito applicativo del presente provvedimento 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; **Prov. Garante 6 novembre 2008**).

1.1 COSA SI INTENDE PER AMMINISTRATORE DI SISTEMA?

Il primo punto riguarda l'individuazione di coloro che ricadono nella categoria di "amministratore di sistema".

Tale figura, anche se non esplicitamente indicata nel "Codice in materia di protezione dei dati personali" era prevista, viceversa, dal d.P.R. 318/1999 (abrogato dal Codice) che definisce l'amministratore di sistema il

"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).

Nel [provvedimento del 27 novembre 2008](#) il Garante dice che con "amministratore di sistema" si individuano figure professionali *finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti* e che sono 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** e ciò anche quando l'amministratore non consulti "in chiaro" le informazioni relative ai trattamenti di dati personali.

1.2 COME SI VALUTANO LE CAPACITÀ DELL'AMMINISTRATORE DI SISTEMA?

Il titolare, prima di procedere alla nomina, deve valutare l'esperienza, la capacità e l'affidabilità dei soggetti designati quali "amministratore di sistema" che devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza. In che modo ciò può essere svolto (ed eventualmente dimostrato al Garante in caso di ispezione)? È ovvio che si parte dal presupposto che chi di fatto svolge già oggi la funzione di amministratore di sistema sia in grado di svolgere la propria funzione; è opportuno allora predisporre una sorta di **curriculum vitae di ciascun amministratore che indichi chiaramente titoli di studio, certificazioni professionali, esperienze professionali, corsi di formazione già svolti. Il CV deve essere datato e firmato sia dall'amministratore che dal titolare.** L'indicazione dei percorsi formativi svolti specie per gli ambiti non prettamente tecnologici ma relativi invece alle problematiche della privacy e della protezione dei dati personali assume un valore particolarmente importante per il "rispetto della garanzia delle vigenti disposizioni". L'amministratore di sistema non può essere solo un bravo tecnico ma deve conoscere la normativa sulla privacy.

1.3 DESIGNAZIONE DELL'AMMINISTRATORE DI SISTEMA.

Occorre predisporre una lettera di "incarico" specifica che contenga:

- 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.

1.4 FAC SIMILE: NOMINA AD AMMINISTRATORE DI SISTEMA

Egr. Sig.

Oggetto: **Nomina ad "amministratore del sistema"**

Ai sensi del "provvedimento" del Garante per la protezione dei dati personali del 27 novembre 2008 recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008 ed ad integrazione della eventuale nomina ad incaricato già consegnataLe e da Lei sottoscritta,

- dato il rapporto di lavoro con Lei in essere, la sua qualifica di assegnazione e la documentata preposizione alla unità operativa di appartenenza,

- considerando che le prestazioni da lei effettuate in via ordinaria forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza

con la presente La nominiamo incaricato con mansioni di **"Amministratore del sistema"** per i trattamenti svolti internamente in azienda o da essa operati le cui specifiche sono allegate (*in alternativa: richiamate nella versione corrente del Documento Programmatico sulla Sicurezza del quale può prendere visione*).

Specificatamente e limitatamente a tale contesto i suoi compiti consistono in:

- assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in azienda;
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni;
- predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e 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

La preghiamo di restituirci copia della presente, firmata per accettazione e per ricevuta della documentazione di cui sopra.

Distinti saluti.

Data, _____

Firma della Società/Titolare del trattamento

Per ricevuta ed accettazione:

(data e firma) -----

Si allega:

- curriculum dell'amministratore di sistema
- attestazioni formazione specifica

2

3 PRIVACY: GLI ADEMPIMENTI PER LE AZIENDE ENTRO IL 31 MARZO

Il decreto legislativo 30 giugno 2003, n. 196, meglio noto come "[Codice in materia di protezione dei dati personali](#)" prevede una serie di adempimenti che **ogni azienda deve rispettare entro il 31 marzo di ogni anno.**

Ecco una rapida sintesi di tutte le scadenze.

3.1 DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Annualmente, e **non oltre il 31 marzo** di ogni anno, l'azienda deve aggiornare il proprio "Documento Programmatico sulla Sicurezza" (DPS) che deve contenere, al minimo (regola 19 dell'[allegato B](#), "Disciplinare tecnico in materia di misure minime di sicurezza", del D. Lgs. n.196)

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento (...);
- la previsione di interventi formativi degli incaricati del trattamento (...);
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare.

Tali elementi "obbligatori" del DPS devono ovviamente contenere informazioni "aggiornate" alla data di redazione del Documento Programmatico per cui occorre pianificare con cura le attività da svolgere e le funzioni aziendali (ad esempio: l'ufficio Risorse Umane per i piani formativi e l'ufficio Sicurezza per le misure di sicurezza) da coinvolgere.

3.2 NOTA AL CONSIGLIO D'AMMINISTRAZIONE SUL DPS

Ogni anno occorre riportare ([allegato B](#), punto 26) **nella relazione accompagnatoria del bilancio d'esercizio dell'avvenuta redazione o aggiornamento del Documento Programmatico sulla Sicurezza.**

3.3 NOTIFICAZIONE DEI TRATTAMENTI

Solo nei casi previsti dal Codice (art. 37 del Codice) occorre notificare al Garante per la protezione dei dati personali i trattamenti di dati che si intende effettuare. Tale notifica (ripeto: necessaria solo nei casi individuati dalla legge) va fatta PRIMA dell'inizio dei trattamenti stessi. È buona prassi indicare nel DPS se vi sono stati nuove notifiche di tali trattamenti rispetto all'anno precedente.

3.4 ACQUISIZIONE DEI DPS DEI "RESPONSABILI" ESTERNI

Nel caso l'azienda abbia nominato "responsabili" del trattamento esterni (ad esempio: società terze a cui sono affidati in outsourcing alcuni trattamenti di dati) **è necessario richiedere a tali "responsabili"**

copia (anche in formato ridotto) **del loro Documento Programmatico** (da allegare o citare nel proprio aggiornamento).

3.5 PIANI DI FORMAZIONE

È necessario ogni anno **predisporre un piano di formazione in ambito privacy per tutti coloro che trattano** (in maniera informatizzata o cartacea) **dati personali**. La formazione in ambito privacy è un **obbligo di legge**: occorre "rendere edotti gli incaricati del trattamento dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali" (punto 19.6 dell'[allegato B](#))

4 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 i 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 abrogato) 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?

E' 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".

E' 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" (log-in) 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) 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?

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](#)