



**le nuove frontiere dell'informatica
amministratori di sistema:
la versione definitiva**

Bologna, 22 ottobre 2009
Savoia Hotel Regency
Via del Pilastro, 2 - 40127 Bologna

il seminario è organizzato da



in collaborazione con:



orlandi&partners
studiolegale

**MISURE E ACCORGIMENTI PRESCRITTI AI TITOLARI
DEI TRATTAMENTI EFFETTUATI CON STRUMENTI
ELETTRONICI RELATIVAMENTE ALLE ATTRIBUZIONI
DELLE FUNZIONI DI AMMINISTRATORE DI SISTEMA
PROVVEDIMENTO 27 NOVEMBRE 2008**

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

e relative

FAQ

POST CONSULTAZIONE PUBBLICA AVVIATA 21 APRILE 2009

e successive

MODIFICHE

PROVVEDIMENTO 25 GIUGNO 2009

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

LA RATIO DEL PROVVEDIMENTO

“REFRESH”

RATIO FONDAMENTALE DEL PROVVEDIMENTO

Gli "amministratori di sistema" sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali (...)

Le ispezioni effettuate in questi anni dall'Autorità hanno permesso di mettere in luce in diversi casi **una scarsa consapevolezza da parte di organizzazioni grandi e piccole del ruolo svolto dagli amministratori di sistema (...)**

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 (...)

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

LA RATIO DEL PROVVEDIMENTO

“REFRESH”

il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di:

h) curare 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

Segnalazione ai titolari di trattamenti relativa alle funzioni di amministratore di sistema > si applica a tutti!

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**

LA RATIO DEL PROVVEDIMENTO

“REFRESH”

il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di:

c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143

MISURE E ACCORGIMENTI PRESCRITTI AI TITOLARI DEI TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI ai sensi dell'art. 154, comma 1, lett. c) del Codice 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

NB: UNICA ESCLUSIONE

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.

gestione di informazioni attinenti ad altre imprese, amministrazioni, clienti, fornitori e dipendenti utilizzate, anche in relazione a obblighi contrattuali e normativi, per correnti finalità amministrative e contabili

LE PRESCRIZIONI

DOPO LE MODIFICHE

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.**

2-Designazioni individuali con elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

3- Redazione, conservazione ed aggiornamento di un “elenco degli amministratori di sistema” (anche per i casi di outsourcing)

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 è tenuto a redigerlo, annotati comunque~~ in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti 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.

■ ■ ■ ■ ■ ■ ■ ■ ■ ■
■ **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** ■



LE PRESCRIZIONI

DOPO LE MODIFICHE

4- Informazione ai lavoratori

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, **il titolare deve rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni**, 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 **o tramite procedure formalizzate ad istanza del lavoratore** (ad es., intranet aziendale, ordini di servizio a circolazione interna o bollettini).

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

5- Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del titolare **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.

6- 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**.

I PRINCIPALI “CHIARIMENTI” DELLE FAQ

Sulla definizione di "amministratore di sistema"

figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti

ma anche

altre figure quali:

gli amministratori di basi di dati

gli amministratori di reti e di apparati di sicurezza

gli amministratori di sistemi software complessi.

FAQ n. 1

figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione **con cui vengono 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.**

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

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.

QUINDI: ads ≠ manutentore occasionale ≠ operatore di sistema ≠ utente

I PRINCIPALI “CHIARIMENTI” DELLE FAQ

Sui "LOG"

FAQ nn. 9, 10 e 11 CONTENUTO DEI LOG

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.**

NB: Il provvedimento **non chiede in alcun modo** che vengano registrati dati sull'attività interattiva (comandi impartiti, transazioni effettuate) degli amministratori di sistema.

Tipicamente **contiene:**

"username" utilizzato

data e all'ora dell'evento (timestamp)

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...)

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.

FAQ n. 12 REQUISITI DEI LOG

L' **inalterabilità** dei log può essere ragionevolmente soddisfatta 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".

NB: il Garante non ha 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

FAQ n. 4 LOGGARE I CLIENT!

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

I PRINCIPALI “CHIARIMENTI” DELLE FAQ

FAQ nn. 20 e 21 REQUISITI AdS

Le **caratteristiche degli AdS** da prendere in considerazione sono:

esperienza
capacità
affidabilità

Si tratta quindi di qualità tecniche, professionali e di condotta, non di requisiti morali.

Gli **estremi identificativi** degli AdS sono i 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.

Su DESIGNAZIONE E VERIFICA DEGLI ADS

FAQ n. 16 SCOPO DEI LOG E DELLA VERIFICA ANNUALE

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.**

FAQ nn. 7 e 8 CONTENUTO DELLA DESIGNAZIONE AdS

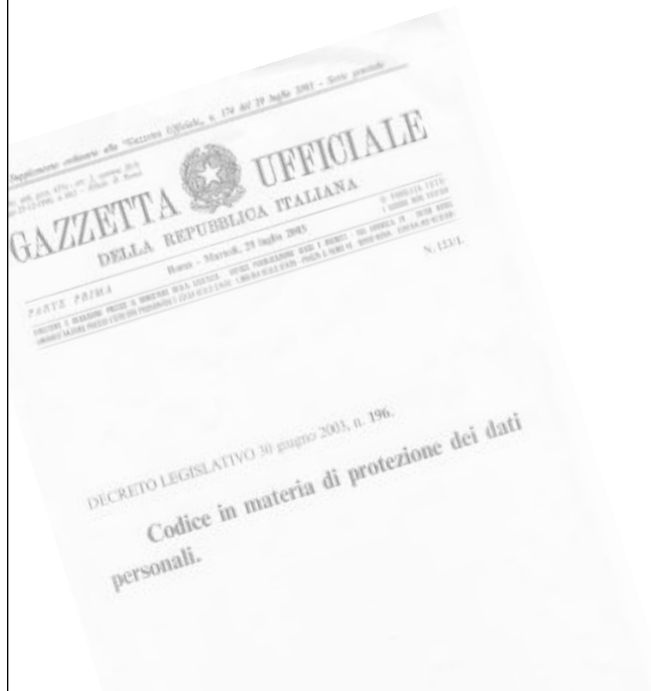
Occorre una **"elencazione analitica"** degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, ovvero la descrizione puntuale degli stessi, evitando l'attribuzione di ambiti insufficientemente definiti, analogamente a quanto previsto al comma 4 dell'art. 29 del Codice riguardante i responsabili del trattamento. E' tuttavia sufficiente specificare **l'ambito di operatività in termini 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.

SANZIONI

responsabilità civile
aggravata ex art. 2050

responsabilità penale

sanzioni amministrative



sanzioni amministrative

L. 27 febbraio 2009, n. 14

Conversione in legge, con modificazioni, del *decreto-legge 30 dicembre 2008, n. 207*, recante proroga di termini previsti da disposizioni legislative e disposizioni finanziarie urgenti.

Publicata nella Gazz. Uff. 28 febbraio 2009, n. 49, S.O.

1

Aumento sanzioni pecuniarie preesistenti

2

Riduzione dei min. e max. per violazioni di minore gravità

3

Introduzione nuove sanzioni pecuniarie

4

Maggiore “scalabilità” (!) delle sanzioni

5

Valorizzazione ruolo “normativo” del Garante



1 Aumento sanzioni pecuniarie preesistenti

Omessa o inidonea informativa (art. 161)



PRIMA

PAGAMENTO DI UNA SOMMA DA TREMILA EURO A DICIOTTOMILA EURO O, NEI CASI DI DATI SENSIBILI O GIUDIZIARI O DI TRATTAMENTI CHE PRESENTANO RISCHI SPECIFICI AI SENSI DELL'ARTICOLO 17 O, COMUNQUE, DI MAGGIORE RILEVANZA DEL PREGIUDIZIO PER UNO O PIÙ INTERESSATI, DA CINQUEMILA EURO A TRENTAMILA EURO. LA SOMMA PUÒ ESSERE AUMENTATA SINO AL TRIPLO QUANDO RISULTA INEFFICACE IN RAGIONE DELLE CONDIZIONI ECONOMICHE DEL CONTRAVVENTORE

DOPO

PAGAMENTO DI UNA SOMMA DA SEIMILA EURO A TRENTASEMILA EURO



DECRETO LEGISLATIVO 30 giugno 2003, n. 196.
Codice in materia di protezione dei dati personali.

2 Riduzione dei min. e max. per violazioni di minore gravità



Se taluna delle violazioni di cui agli articoli 161, 162, 163 e 164 è di **minore gravità**, avuto altresì riguardo alla natura anche economica o sociale dell'attività svolta, i **limiti minimi e massimi stabiliti dai medesimi articoli sono applicati in misura pari a due quinti.**

Esempio per l'omessa informativa

<u>MIN ORD</u>	<u>MAX ORD</u>	<u>MIN RID</u>	<u>MAX RID</u>
6000	36000	1200	7200



DECRETO LEGISLATIVO 30 giugno 2003, n. 196.
Codice in materia di protezione dei dati
personali.

3 Introduzione nuove sanzioni pecuniarie



Omissione misure minime di sicurezza ex art. 33

sanzione del pagamento di una somma **da ventimila euro a centoventimila euro**, con esclusione del pagamento in misura ridotta

>>> correlativamente, scompare dal reato ex art. 169 *“l’ammenda da diecimila euro a cinquantamila euro”*>> **si applica la sanzione suddetta**

Violazione delle disposizioni indicate nell'articolo 167

sanzione del pagamento di una somma **da ventimila euro a centoventimila euro**, con possibilità del pagamento in misura ridotta



DECRETO LEGISLATIVO 30 giugno 2003, n. 196.
Codice in materia di protezione dei dati personali.

3 Introduzione nuove sanzioni pecuniarie

5 Valorizzazione ruolo “normativo” del Garante



Inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto ex art. 154, comma 1, lettere c) e d)

in ogni caso, pagamento di una somma **da trentamila euro a centottantamila euro**



Art. 154 Il Garante ha il compito di:

c) **prescrivere** anche d'ufficio ai titolari del trattamento **le misure necessarie o opportune** al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143;

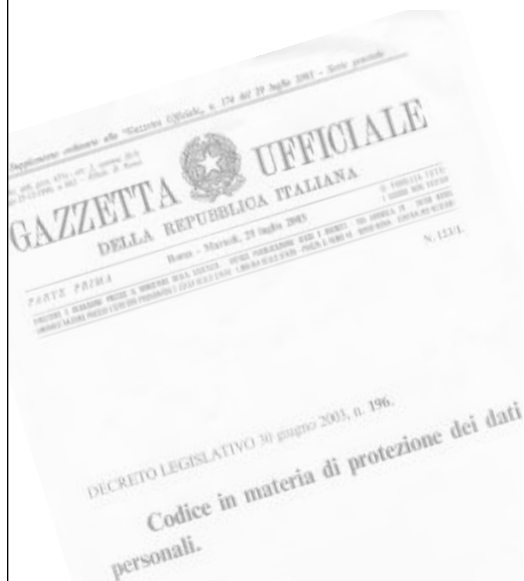
d) **vietare** anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o **disporre il blocco** ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali

ESEMPI DI PROVVEDIMENTI DEL GARANTE SANZIONABILI

- Provv. 27/11/2008 Amministratori di sistema
- Provv. 19/6/2008 Semplificazioni tratt. amministrativi e contabili
- Provv. 1/3/2007 Controlli su internet ed e-mail (in parte: “prescrive ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. c), del Codice, di adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (punto 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli”)
- Provv. 23/11/2006 Linee Guida Privacy e rapporto di lavoro (in parte)
- Provv. 29/4/2004 Videosorveglianza

ESEMPI DI PROVVEDIMENTI DEL GARANTE NON SANZIONABILI

- Provv. 13/10/2008 Rottamazione HD
- Provv. 26/06/2008 Linee Guida per consulenti e periti



4 Maggiore scalabilità (!) delle sanzioni

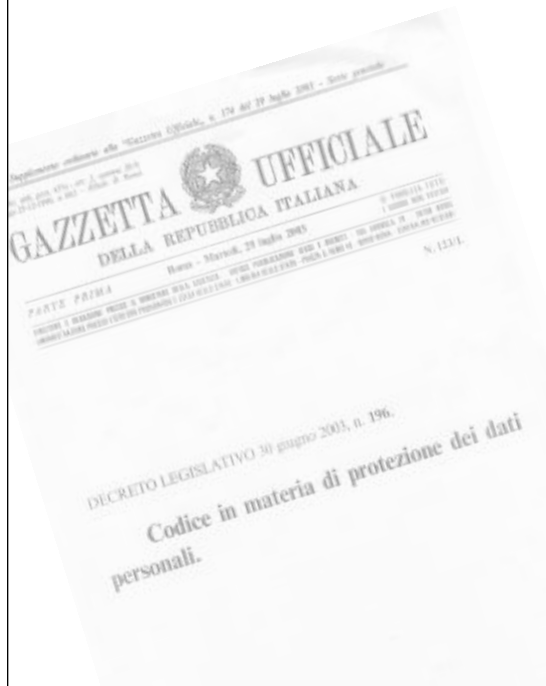


In caso di più violazioni di un'unica o di più disposizioni di cui al presente Capo, **a eccezione di quelle previste dagli articoli 162, comma 2, 162-bis e 164**, commesse anche in tempi diversi in relazione a **banche di dati di particolare rilevanza o dimensioni**, si applica la sanzione amministrativa del pagamento di una **somma da cinquantamila euro a trecentomila euro**.

Non è ammesso il pagamento in misura ridotta.

In **altri** casi di **maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati**, ovvero **quando la violazione coinvolge numerosi interessati**, i limiti minimo e massimo delle sanzioni di cui al presente Capo sono applicati in misura pari al **doppio**.

Le sanzioni di cui al presente Capo possono essere **aumentate fino al quadruplo** quando possono risultare **inefficaci in ragione delle condizioni economiche** del contravventore



Grazie!

orlandi@orlandi.mobi

skype: orlandi.mobi

mobile 335-1815598

www.orlandi.mobi