

2009

Privacy: amministratore di sistema

adempimenti per la nomina ad "amministratore di sistema"

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



Privacy: Il nuovo adempimento del garante 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).

Cosa si intende per amministratore di sistema?

Il primo punto di riflessione 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.

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**.

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.

A chi deve "rispondere" il titolare dei dati?

Il titolare può essere chiamato a rispondere (e quindi a dover documentare e dimostrare il suo operato) della sua responsabilità a:

Autorità:

- Garante Privacy
- Magistratura, Forze di polizia
- Organismi di vigilanza (ad esempio Banca d'Italia nel caso di intermediari finanziari)

Organismi di controllo interno:

- Consiglio di Amministrazione
- Collegio Sindacale
- Comitati vari di controllo, sicurezza, audit

Privacy: amministratore di sistema

adempimenti per la nomina ad "amministratore di sistema"

- Revisori dei Conti
- Certificatori (Iso9001 ed affini)

"Interessati" che intendono esercitare il loro "diritto di accesso":

- Dipendenti,
- clienti,
- fornitori

e chiunque voglia esercitare tale diritto.

Sanzioni per inadempienza

L'inadempienza alla normativa comporta sanzioni da 30.000 a 180.000 euro

archimedia



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Comunicato stampa - 14 gennaio 2009

Amministratori di sistema: occorre massima trasparenza sul loro operato. Il Garante fissa i criteri, quattro mesi per mettersi in regola

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. Ad essi viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione.

Per questo il Garante ha [deciso](#) di richiamare l'attenzione di enti, amministrazioni, società private sulla figura professionale dell' amministratore di sistema e ha prescritto l'adozione di specifiche misure tecniche ed organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici.

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. I gravi casi verificatisi negli ultimi anni hanno evidenziato una preoccupante sottovalutazione dei rischi che possono derivare quando l'attività di questi esperti sia svolta senza il necessario controllo.

Le misure e le cautele dovranno essere messe in atto entro quattro mesi da parte di tutte le aziende private e da tutti i soggetti pubblici, compresi gli uffici giudiziari, le forze di polizia, i servizi di sicurezza. Sono esclusi invece i trattamenti di dati, sia in ambito pubblico che privato, effettuati a fini amministrativo contabile, che pongono minori rischi per gli interessati.

Registrazione degli accessi

Adozione di sistemi di controllo che consentano la registrazione degli accessi effettuate dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici.

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.

Verifica della attività

Verifica almeno annuale da parte dei titolari del trattamento sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali.

Elenco degli amministratori di sistema e loro caratteristiche

Ciascuna azienda o soggetto pubblico dovrà inserire nel documento programmatico della sicurezza o in un documento interno (disponibile in caso di accertamenti da parte del Garante) gli estremi identificativi degli amministratori di sistema e l'elenco delle funzioni loro attribuite.

Dovranno infine essere valutate con attenzione esperienza, capacità, e affidabilità della persona chiamata a ricoprire il ruolo di amministratore di sistema, che deve essere in grado di garantire il pieno rispetto della normativa in materia di protezione dei dati personali, compreso il profilo della sicurezza.

Roma, 14 gennaio 2008

Comunicato del garante



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

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)

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; Prov. 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 annessa 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 inadeguata 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 sistema

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 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 deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

4.4 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 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; Provv. 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 sistema

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.

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). Ciò, salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con diverse previsioni dell'ordinamento che disciplinano uno specifico settore.

d. Servizi in outsourcing

Nel caso di servizi di amministrazione di sistema affidati in *outsourcing* il titolare deve conservare direttamente e

specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

e. Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, 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;

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

Allegato B



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

B. Disciplinare tecnico in materia di misure minime di sicurezza

(Artt. da 33 a 36 del Codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

- 19.1. l'elenco dei trattamenti di dati personali;
- 19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- 19.3. l'analisi dei rischi che incombono sui dati;
- 19.4. 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;
- 19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
- 19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti 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;
- 19.7. 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;
- 19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-*ter* del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati

esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

archimedia

Privacy: domande e risposte

D: Cosa si intende per amministratore di rete

R: La disciplina di protezione dei dati previgente al Codice del 2003 definiva l'amministratore di rete, 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, lettera c) decreto del Presidente della Repubblica n. 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 **nell' allegato B** della nuova normativa, 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.

D: In quali aziende è necessario la nomina dell'amministratore di rete

R: Secondo la normativa la nomina dell'amministratore di rete è obbligatoria in qualsiasi azienda che effettui il trattamento di basi dati con strumenti di elaborazione elettronica, a prescindere dalla dimensione. In particolare le aziende che mettono a disposizione l'accesso al proprio sistema ad operatori interni ed esterni per attività di manutenzione, aggiornamento, modifica, sviluppo con l'autorizzazione ad un accesso completo al sistema. Tuttavia anche i titolari che trattano dati in questo modo sono **esclusi** se le finalità del trattamento sono soltanto quelle **amministrativo-contabili** (oggetto dei recenti interventi di semplificazione).

D: E' necessario nominare l'amministratore di rete anche nel caso in cui sul sistema non siano presenti dati sensibili.

R: E' necessario nominare l'amministratore di rete in tutti quei casi in cui all'interno del sistema siano conservati dati personali o sensibili esposti ad accessi da personale interno od esterno all'azienda operanti con la qualifica ed i diritti di amministratore.

D: Cosa si intende per dati personali o riservati

R: Per dati personali (non sensibili) si intendono quei dati non di pubblico dominio come ad esempio, i numeri di telefono cellulari.

D: Chi deve nominare l'amministratore di rete?

R: La nomina spetta al Responsabile aziendale per la privacy o al titolare del trattamento dei dati. Il titolare del trattamento deve accertare la capacità effettiva della persona che svolgerà il ruolo di amministratore del sistema mediante acquisizione di curriculum che ne comprovi l'esperienza, compresa la conoscenza della legge sulla privacy.

D. Quali figure rientrano nel concetto di amministratore di sistema ?

Quelle in possesso di competenze tali da poter essere incaricate della gestione e manutenzione dei sistemi informatici o delle loro componenti (hardware e software). Nella stessa definizione rientrano anche le figure equiparate che svolgono una attività di gestione e manutenzione che presenta dei rischi relativi alla protezione dei dati personali (amministratori di database, di rete, di sicurezza, di software, ecc...).

D: L'amministratore può essere anche una figura esterna all'azienda?

R: Sì, l'amministratore può essere anche una figura esterna e possono essere anche più persone che svolgono questo ruolo a seconda delle attività e delle specializzazioni richieste. Per ogni amministratore dovrà essere rilasciata una User ed una password diversa in modo da facilitare la tracciatura delle attività svolte sul sistema.

D. Con quali modalità deve avvenire la nomina ?

E' opportuno che sia documentata e che contenga una indicazione precisa delle funzioni e dei compiti attribuiti all'amministratore (così come avviene per il responsabile del trattamento). In questo modo si fa chiarezza sull'ambito di esigibilità della prestazione professionale richiesta all'amministratore di sistema.

D. Che cosa si intende per verifica dell'operato degli amministratori ?

Significa che gli amministratori devono rispettare, nello svolgimento delle attività, le misure tecniche, organizzative e di sicurezza previste dalla legge in materia di protezione dei dati personali e che le eventuali violazioni od anomalie nel loro operato devono essere prontamente identificate e sanate dal titolare. Questo garantisce che il titolare possa considerarsi diligente nell'effettuazione dei controlli e spiega il perché venga richiesto agli amministratori, all'atto della nomina, di fornire idonea garanzia di rispetto delle disposizioni di legge vigenti.

D. Quando deve essere effettuata la verifica ?

Quando si reputa opportuna, anche in relazione alle dimensioni ed alla complessità dell'organizzazione di riferimento e, comunque, con cadenza almeno **annuale**.

D. L'attività degli amministratori di sistema deve essere registrata ?

Soltanto quella che comporta un **accesso**, inteso come superamento di una procedura di autenticazione informatica, ai sistemi ed agli archivi elettronici. In assenza di contrarie indicazioni sembra che la registrazione debba comprendere tanto gli eventi positivi (success) che negativi (failure) di accesso.

D. Con quali modalità e garanzie deve essere effettuata la registrazione ?

Le registrazioni (record) devono contenere l'indicazione della data (*timestamp*) e la descrizione dell'evento che le genera. Devono inoltre essere complete, non modificabili e consentire la verifica della loro integrità, tenendo conto delle finalità di controllo cui sono preordinate. A seconda della dimensione e della complessità della infrastruttura IT questa misura può richiedere uno sforzo organizzativo e tecnologico non indifferente, anche dal punto di vista dell'analisi della situazione di partenza.

Le registrazioni vanno conservate per un periodo minimo di **6 mesi**.

D: Quale è lo scopo della raccolta delle attività nel file di registrazione del sistema informativo.

R: Il file di log dovrà documentare le attività svolte dall'amministratore di rete sul sistema informativo nella sua interezza. Dovrà essere non alterabile o modificabile, consultabile in qualsiasi momento dal titolare dei dati, mantenuto per almeno sei mesi.

D: L'amministratore di rete è responsabile dell'attivazione del sistema di Log.

R: E' il titolare del trattamento dei dati che **risponde** nel caso in cui il sistema di rilevamento delle attività dell'amministratore di rete non venisse attivato. L'amministratore di rete risponde in merito alla sicurezza del sistema e dei dati ed al rispetto delle misure minime od opportune nel trattamento degli stessi. La responsabilità dell'amministratore di rete rimane inalterata e deve rispettare le normali regole deontologiche della figura professionale. Il log sarà uno strumento a disposizione del responsabile privacy per monitorare che l'attività svolta dagli amministratori di rete sia conforme a queste regole ed al codice della privacy.

D: Esistono software già predisposti per la gestione dei file di registrazione secondo le nuove norme del garante.

R: Sì, esistono strumenti in grado di gestire differenti file di registrazione, archiviandoli e mettendoli a disposizione del responsabile privacy. Archimedia ha individuato alcune soluzioni adatte a garantire il rispetto della normativa sia per le piccole medi imprese che per gli studi professionali.

D: Chi controlla che le misure minime e gli altri adempimenti previsti dalla legge sono messi in pratica?

R: La Polizia Postale (con le sue 76 Sezioni sul territorio) e la Guardia di Finanza in forza di un protocollo di intesa con il Garante.

D: Se esiste una autorizzazione generale al trattamento dei dati, è possibile trattare i dati senza il consenso dell'interessato?

R: No, è solo possibile omettere la notifica al Garante e si può procedere con il trattamento dei dati, osservando tutte le prescrizioni.

D: E' vero che è obbligatorio per tutte le organizzazioni avere un DPS (Documento Programmatico della Sicurezza)?

R: No! Il D.P.S. è obbligatorio (Art. 34 del Testo Unico) solo per quelle organizzazioni che trattano dati personali (anche non sensibili) con l'impiego di elaboratori elettronici. Chi tratta i dati solo manualmente su supporto cartaceo, non è tenuto ad avere il DPS.

D: E' obbligatorio preparare un D.P.S. (Documento Programmatico sulla Sicurezza) che contenga una analisi dei rischi?

R: Sì, è esplicitamente richiesto dal comma 19.6 dell'Allegato B del D.Lgs. 196/03 per tutte le organizzazioni che trattano dati sensibili con l'ausilio di elaboratori elettronici.

D: A cosa serve il Documento Programmatico della Sicurezza (DPS)?

R: Il Documento Programmatico per la Sicurezza identifica gli aspetti dell'infrastruttura tecnologica aziendale coinvolti nella gestione di dati personali e sensibili, verificandone l'aderenza a quanto disposto dalle più recenti normative (Dlgs. N.196 del 30 Giugno 2003). Inoltre, il DPS definisce e descrive le misure necessarie per una vera "messa in sicurezza" del sistema informativo aziendale.

D: Il documento è solo un adempimento legale?

R: Il documento rappresenta non solo un adempimento legale ma un vero e proprio strumento di riferimento per l'azienda in materia di trattamento dei dati personali, e in generale di definizione delle

strategie di sicurezza, e delle conseguenti policy che tutti i dipendenti, collaboratori, partner e fornitori devono adottare.

D: Quali sono i risultati per il Cliente di un progetto DPS ?

R: Il DPS evidenzia i punti di forza e di debolezza dell'infrastruttura esistente, evidenziando anche i rischi normativi (legati ad eventuali inadempimenti richiesti dalla legge) e funzionali (legati al proprio modello di business derivanti da una gestione della sicurezza non ottimale). Formalizza inoltre le policy di lavoro, costituendo un valido riferimento per l'utilizzo dell'infrastruttura informativa, e formalizza le procedure di intervento in caso di problemi o guasti.

D: Non siamo collegati ad internet, non siamo già sicuri?

R: No. Il collegamento ad internet è solo una delle minacce e neanche la più importante. Secondo le statistiche di istituti di ricerca e polizie, circa tre quarti degli incidenti sono generati all'interno delle organizzazioni. Di questi, oltre la metà sono involontari, perchè... "errare è umano".

D: Possiamo scegliere di ignorare questo dispositivo di legge e correre il rischio?

R: No. La sensibilità dell'opinione pubblica sul tema della privacy è molto alta. Se le probabilità di ricevere un'ispezione da parte degli ispettori del Garante della Privacy sono basse, in caso di incidenti anche banali (p.e. il furto di un disco o di un computer contenente dati personali nella vostra azienda) potreste non essere in grado di dimostrare che trattavate i dati in conformità alla legge. In questo caso vi esponete al rischio di sanzioni anche penali (e la responsabilità penale è personale).

D: I dati personali che abbiamo li facciamo elaborare da uno studio esterno, non è lui il titolare?

R: No. Anche se tutti i trattamenti (per esempio di paghe e contributi o contabili) sono effettuati all'esterno, i titolari di quei trattamenti siete voi e quindi voi ne risponderete in merito alla loro privacy e sicurezza.

D: La nostra rete è protetta dal "firewall", non siamo già sicuri?

R: No. Il firewall è un dispositivo utile, ma che, quando ben gestito, svolge solo una funzione ben precisa: proteggere la vostra rete informatica aziendale da specifici tipi di incidenti di origine esterna. Questo ha poco a che vedere con la Privacy ed il Dlgs.196/2003, che in particolare mira anche a proteggere i dati personali (informatici e non) e la vostra azienda sia da incidenti interni che esterni, deliberati o accidentali. Per esempio, il firewall non vi serve a proteggere i dati in caso di perdita accidentale per guasto o furto del computer e tantomeno a proteggere i vostri archivi cartacei dalle conseguenze di un incendio.

D: Quali sono i tempi di attuazione della normativa sull'amministratore di rete?

R: Le misure dovranno essere adottate entro il 30 Giugno 2009. Per tutti i trattamenti di nuova attivazione entro 30 gg. giorni dalla data di inizio attività.

D: Quali sono le sanzioni per mancato adeguamento alla normativa?

R: In tema di omessa o inadeguata informativa, la sanzione per chi viola l'art. 13 diventa un'unica sanzione amministrativa da seimila euro a trentaseimila euro. Viene così completamente parificata la fattispecie, eliminando le differenze fra violazioni relative a dati sensibili o comuni.

Vengono poi aumentate le sanzioni pecuniarie per chi cede dati in violazione di legge (art. 162): si passa dalla previgente sanzione (da cinquemila euro a trentamila euro), ai diecimila euro a sessantamila euro. Nel caso invece di violazione dell'obbligo di comunicazione di dati sensibili da parte di medici solo per il tramite di altro medico designato dall'interessato (cioè violazione dell'art. 84 comma I) la sanzione va dai mille euro a seimila euro, e non più dai cinquecento ai tremila.

Molto importanti sono i due commi aggiunti all'art 162: Il comma 2-bis dispone che in caso di violazione di adempimenti sulle misure minime di sicurezza (art. 33) e di violazione della normativa in tema corretto trattamento dei dati (trattamento illecito art 167), viene applicata in ogni caso la sanzione amministrativa del pagamento di una somma da ventimila euro a centoventimila euro. Ciò significa che le due classiche violazioni privacy (non adottare le misure minime e violare la privacy del cittadino), che prima erano pressoché impunte, proprio perché sanzionate penalmente, ora diventano anche sanzione amministrativa

Violazione Amministrativa	Sanzione
Art. 161 Omessa informativa	Da 6.000 a 36.000 euro
Omessa informativa in caso di dati sensibili o giudiziari o di trattamenti che presentino rischi specifici	Da 10.000 a 60.000 euro
Art. 162 Cessione dei dati	Da 10.000 a 60.000 euro
Art. 163 Omessa o incompleta informativa al Garante	Da 10.000 a 60.000 euro
Art. 164 Mancata esibizione di informazioni o documenti richiesti dal Garante	Da 10.000 a 60.000 euro
Art. 167 Trattamento illecito di dati	Da 20.000 a 120.000 euro
Illecito Penale	Sanzione
Art. 167 Trattamento illecito di dati	Reclusione da 6 mesi a 3 anni
Art. 168 False dichiarazioni e notificazioni al Garante	Reclusione da 6 mesi a 3 anni
Art. 169 Mancata adozione delle misure di sicurezza	Arresto sino a 2 anni o ammenda da 20.000 a 50.000 euro
Art. 170 Inosservanza di provvedimenti del Garante	Reclusione da 3 mesi a 2 anni