

SEMPLIFICAZIONE PER TALUNI TRATTAMENTI

Come il Garante ha già evidenziato nel provvedimento del 19 giugno 2008 (in *Gazzetta Ufficiale* 1° luglio 2008, n. 152 e in www.garanteprivacy.it, doc. web n. 1526724), nonché mediante la segnalazione al Parlamento e al Governo in materia di misure minime di sicurezza del 19 giugno 2008, da parte di taluni titolari del trattamento le medesime misure di sicurezza possono essere attuate in modo semplificato, alla luce dell'esperienza applicativa e senza diminuire dal punto di vista sostanziale le cautele volte a prevenire determinati rischi (art. 34, comma 1 bis, del Codice, come introdotto dall'art. 29 cit.).

Sono state pertanto individuate alcune nuove modalità volte a semplificare incisivamente l'applicazione di varie regole contenute nell'Allegato B.

L'obiettivo è garantire egualmente un idoneo livello di sicurezza tenendo conto delle ridotte dimensioni di alcune realtà organizzative, nonché della particolare natura di alcuni trattamenti a fini esclusivamente amministrativo-contabili. Ciò, sulla base di una dettagliata ricognizione delle singole questioni e di approfondimenti svolti in ordine alle questioni applicative che sono state poste a vario titolo all'attenzione di questa Autorità, in particolare attraverso quesiti e segnalazioni.

Le modalità semplificate elencate nell'unito prospetto potranno essere applicate immediatamente dai soggetti interessati.

TUTTO CIÒ PREMESSO IL GARANTE

- a) ai sensi dell'art. 34, comma 1-bis, del Codice individua nell'unito prospetto che costituisce parte integrante del presente provvedimento le modalità semplificate per applicare le misure minime di sicurezza per il trattamento dei dati personali;
- b) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale della Repubblica italiana*.

Roma, 27 novembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

MISURE SEMPLIFICATE PER APPLICARE LE MISURE MINIME DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI

1. SOGGETTI CHE POSSONO AVVALERSI DELLA SEMPLIFICAZIONE

Le seguenti modalità semplificate sono applicabili dai soggetti pubblici o privati che:

- a) utilizzano dati personali non sensibili o che trattano come unici dati sensibili riferiti ai propri dipendenti e collaboratori anche a progetto quelli costituiti dallo stato di salute o malattia senza indicazione della relativa diagnosi, ovvero dall'adesione a organizzazioni sindacali o a carattere sindacale;
- b) trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese (cfr. art. 2083 cod. civ. e d.m. 18 aprile 2005, recante adeguamento alla disciplina comunitaria dei criteri di individuazione di piccole e medie imprese, pubblicato nella Gazzetta Ufficiale 12 ottobre 2005, n. 238).

2. TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI

I soggetti di cui al paragrafo 1 possono applicare le misure minime di sicurezza prescritte dalla disciplina in materia di trattamenti realizzati con l'ausilio di strumenti elettronici (art. 34 del Codice e regole da 1 a 26 dell'Allegato B.) osservando le modalità semplificate di seguito individuate.

2.1. Istruzioni agli incaricati del trattamento (modalità applicative delle regole di cui ai punti 4, 9, 18 e 21 dell'Allegato B.)

Le istruzioni in materia di misure minime di sicurezza previste dall'Allegato B. possono essere impartite agli incaricati del trattamento anche oralmente, con indicazioni di semplice e chiara formulazione.

2.2. Sistema di autenticazione informatica (modalità applicative delle regole di cui ai punti 1, 2, 3, 5, 6, 7, 8, 10 e 11 dell'Allegato B.)

Per l'accesso ai sistemi informatici si può utilizzare un qualsiasi sistema di autenticazione basato su un codice per identificare chi accede ai dati (di seguito, "username"), associato

a una parola chiave (di seguito: “password”), in modo che:

- a) l’username individui in modo univoco una sola persona, evitando che soggetti diversi utilizzino codici identici;
- b) la password sia conosciuta solo dalla persona che accede ai dati.

L’username deve essere disattivato quando l’incaricato non ha più la qualità che rende legittimo l’utilizzo dei dati (ad esempio, in quanto non opera più all’interno dell’organizzazione).

Può essere adottata, quale procedura di autenticazione anche la procedura di login disponibile sul sistema operativo delle postazioni di lavoro connesse a una rete.

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, se l’accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della password, il titolare può assicurare la disponibilità di dati o strumenti elettronici con procedure o modalità predefinite. Riguardo a tali modalità, sono fornite preventive istruzioni agli incaricati e gli stessi sono informati degli interventi effettuati (ad esempio, prescrivendo ai lavoratori che si assentino dall’ufficio per ferie l’attivazione di modalità che consentano di inviare automaticamente messaggi di posta elettronica ad un altro recapito accessibile: si vedano le Linee-guida in materia di lavoro per posta elettronica e Internet approvate dal Garante e pubblicate nella Gazzetta ufficiale 10 marzo 2007 , n. 58 [doc. web n. 1387522]).

2.3. Sistema di autorizzazione (modalità applicative delle regole di cui ai punti 12, 13 e 14 dell’Allegato B.)

Qualora sia necessario diversificare l’ambito del trattamento consentito, possono essere assegnati agli incaricati —singolarmente o per categorie omogenee corrispondenti profili di autorizzazione, tramite un sistema di autorizzazione o funzioni di autorizzazione incorporate nelle applicazioni software o nei sistemi operativi, così da limitare l’accesso ai soli dati necessari per effettuare le operazioni di trattamento.

2.4. Altre misure di sicurezza (modalità applicative delle regole di cui ai punti 15, 16, 17 e 18 dell’Allegato B.)

I soggetti di cui al paragrafo 1 assicurano che l’ambito di trattamento assegnato ai singoli incaricati, nonché agli addetti alla gestione o alla manutenzione degli strumenti elettronici, sia coe-

rente con i principi di adeguatezza, proporzionalità e necessità, anche attraverso verifiche periodiche, provvedendo, quando è necessario, ad aggiornare i profili di autorizzazione eventualmente accordati.

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici (ad esempio, antivirus), anche con riferimento ai programmi di cui all'art. 615-quinquies del codice penale, nonché a correggerne difetti, sono effettuati almeno annualmente. Se il computer non è connesso a reti di comunicazione elettronica accessibili al pubblico (linee Adsl, accesso a Internet tramite rete aziendale, posta elettronica), l'aggiornamento deve essere almeno biennale.

I dati possono essere salvaguardati anche attraverso il loro salvataggio con frequenza almeno mensile. Il salvataggio periodico può non riguardare i dati non modificati dal momento dell'ultimo salvataggio effettuato (dati statici), purché ne esista una copia di sicurezza da cui effettuare eventualmente il ripristino.

2.5. Documento programmatico sulla sicurezza (modalità applicative delle regole di cui ai punti da 19.1 a 19.8 dell'Allegato B.)

2.5.1. Fermo restando che per alcuni casi è già previsto per disposizione di legge che si possa redigere un'autocertificazione in luogo del documento programmatico sulla sicurezza (vedi il precedente par. 1, lett. a); art. 29 d.l. n. 112/2008 cit.), i soggetti pubblici e privati che trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese, possono redigere un documento programmatico sulla sicurezza semplificato sulla base delle indicazioni di seguito riportate.

Il documento deve essere redatto prima dell'inizio del trattamento e deve essere aggiornato entro il 31 marzo di ogni anno nel caso in cui, nel corso dell'anno solare precedente, siano intervenute modifiche rispetto a quanto dichiarato nel precedente documento.

Il documento deve avere i seguenti contenuti:

- a) le coordinate identificative del titolare del trattamento, nonché, se designati, gli eventuali responsabili. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento;

- b) una descrizione generale del trattamento o dei trattamenti realizzati, che permetta di valutare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento. In tale descrizione vanno precisate le finalità del trattamento, le categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime, nonché i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;
- c) l'elenco, anche per categorie, degli incaricati del trattamento e delle relative responsabilità. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento con le relative responsabilità;
- d) una descrizione delle altre misure di sicurezza adottate per prevenire i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

3. MODALITÀ APPLICATIVE PER I TRATTAMENTI REALIZZATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI (MODALITÀ APPLICATIVE DELLE REGOLE DI CUI AI PUNTI 27, 28 E 29 DELL'ALLEGATO B.)

I soggetti di cui al paragrafo 1 possono adempiere all'obbligo di adottare le misure minime di sicurezza di cui all'art. 35 del Codice applicando le misure contenute nell'Allegato B. relativamente ai trattamenti realizzati senza l'ausilio di strumenti elettronici (regole da 27 a 29 dello stesso Allegato B.), con le modalità semplificate di seguito individuate.

3.1. Agli incaricati sono impartite, anche oralmente, istruzioni finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

3.2. 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 dai medesimi incaricati fino alla restituzione in modo che a essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

34. PROROGA DELLE MISURE E ACCORGIMENTI PRESCRITTI AI TITOLARI DEI TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI RELATIVAMENTE ALLE ATTRIBUZIONI DELLE FUNZIONI DI AMMINISTRATORE DI SISTEMA (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale reggente;

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 del medesimo Codice;

Visto il provvedimento del Garante del 27 novembre 2008 relativo a “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; Visto il punto 3 del dispositivo del predetto provvedimento, il quale prescrive che le misure e gli accorgimenti di cui al punto 2 del medesimo dispositivo siano introdotti, per i trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del provvedimento stesso, al più presto e comunque entro e non oltre il termine di centoventi giorni dalla medesima data, mentre, per i trattamenti che avranno inizio dopo il termine di trenta giorni dalla pubblicazione, tali accorgimenti e misure siano introdotti anteriormente all'inizio del trattamento dei dati;

Tenuto conto dei quesiti pervenuti sia da singoli titolari del trattamento sia da alcune associazioni rappresentative di categoria, relativi all'esatta interpretazione degli adempimenti prescritti dal citato provvedimento del 27 novembre 2008;

Considerata l'ampia platea di soggetti interessati all'adempimento del suddetto provvedimento e la conseguente necessità di assicurare la massima diffusione e la più completa e precisa conoscenza delle prescrizioni in esso contenute;

Riservata la possibilità, all'esito di un attento esame dei quesiti già pervenuti e di quelli che

(*) Gazzetta Ufficiale 24 febbraio 2009, n. 45 [doc. *web* n. 1591970]

potranno essere sottoposti all'attenzione del Garante, anche a seguito dell'attività di consultazione attualmente in corso all'interno di alcune associazioni professionali e di categoria, di fornire chiarimenti in merito attraverso risposte ai quesiti più frequenti da diffondere anche tramite il sito Internet dell'Autorità;

Ritenuta l'opportunità di unificare i termini previsti per l'adempimento delle prescrizioni di cui al citato provvedimento del 27 novembre 2008 e ravvisata altresì la necessità di prorogare tali termini, disponendo che tutti i titolari del trattamento (qualunque sia la data di inizio dei trattamenti che li riguardano) adottino le misure e gli accorgimenti di cui al punto 2 del dispositivo di tale provvedimento entro il 30 giugno 2009;

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

Relatore il prof. Francesco Pizzetti;

DISPONE:

- a) di unificare e contestualmente prorogare i termini per l'adempimento delle prescrizioni di cui al citato provvedimento del 27 novembre 2008, prescrivendo che tutti i titolari del trattamento interessati (qualunque sia la data di inizio dei trattamenti che li riguardano) adottino le misure e gli accorgimenti di cui al punto 2 del dispositivo del provvedimento medesimo entro il 30 giugno 2009;
- b) di trasmettere copia del presente provvedimento al Ministero della giustizia-Ufficio pubblicazione leggi e decreti per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 12 febbraio 2009

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE REGGENTE
De Paoli

35. MISURE E ACCORGIMENTI PRESCRITTI AI TITOLARI DEI TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI RELATIVAMENTE ALLE ATTRIBUZIONI DELLE FUNZIONI DI AMMINISTRATORE DI SISTEMA (*)

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 cd. "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

(*) Gazzetta Ufficiale 24 dicembre 2008, n. 300 [doc. *web* n. 1577499], in inglese [doc. *web* n. 1583535]

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 sistemistiche;

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 modifica (1).

La disciplina di protezione dei dati previgente al Codice del 2003 definiva l'amministratore di

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

sistema, individuandolo quale “soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione” (art. 1, comma 1, lett. c) d.P.R. 318/1999).

Il Codice non ha invece incluso questa figura tra le proprie definizioni normative. Tuttavia le funzioni tipiche dell'amministrazione di un sistema sono richiamate nel menzionato Allegato B, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione.

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

Nel corso delle attività ispettive disposte negli ultimi anni dal Garante è stato possibile rilevare quale importanza annettano ai ruoli di system administrator (e di network administrator o database administrator) la gran parte di aziende e di grandi organizzazioni pubbliche e private, al di là delle definizioni giuridiche, individuando tali figure nell'ambito di piani di sicurezza o di documenti programmatici e designandoli a volte quali responsabili.

In altri casi, non soltanto in organizzazioni di piccole dimensioni, si è invece riscontrata, anche a elevati livelli di responsabilità, una carente consapevolezza delle criticità insite nello svolgimento delle predette mansioni, con preoccupante sottovalutazione dei rischi derivanti dall'azione incontrollata di chi dovrebbe essere preposto anche a compiti di vigilanza e controllo del corretto utilizzo di un sistema informatico.

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

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 inidonea 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; Provv. 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; Prov. Garante 6 novembre 2008):

a. Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

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

b. Designazioni individuali

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

c. Elenco degli amministratori di 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 orga-