INFORMATICA GIURIDICA
collana diretta da Michele Iaselli

Numero 13

L'AMMINISTRATORE DI SISTEMA

di Eric Falzone

ALTALEX
eBook 2010

L'AMMINISTRATORE DI SISTEMA: LUCI E OMBRE DEL PROVVEDIMENTO DEL GARANTE PRIVACY DEL 27 NOVEMBRE 2008

di Eric Falzone

Sommario

L'AMMINISTRATORE DI SISTEMA: LUCI E OMBRE DEL PROVVEDIMENTO DEL GARANTE PRIVACY DEL 27 NOVEMBRE 2008

Premessa

In data 27 novembre 2008 il Garante per la Protezione dei Dati Personali ha emesso il Provvedimento Generale denominato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (pubblicato nella Gazzetta Ufficiale n. 300 del 24 dicembre 2008) con l'intento di promuovere presso Titolari e pubblico la consapevolezza della delicatezza del ruolo di "Amministratore di Sistema", richiamando in particolar modo l'attenzione sulla necessità di prestare la massima attenzione ai rischi incombenti sui dati personali e alle criticità relative alle misure di sicurezza adottate connesse allo svolgimento di tale attività.
Con tale provvedimento il Garante Privacy ha inteso, infatti, dare rilievo all'interno del sistema di gestione privacy aziendale, al ruolo di amministratore di sistema evidenziandone l'importanza e imponendo ai Titolari misure di sicurezza di carattere tecnico e organizzativo che prevedono la selezione dei candidati sulla base di comprovate capacità tecniche, l'assegnazione ai soggetti individuati di adeguati livelli di responsabilità aziendale e la definizione e implementazione di procedure tecniche di supervisione e controllo sull'operato svolto.
In particolare l'Autorità Garante Privacy ha ravvisato la necessità di promuovere tra soggetti pubblici e privati la conoscenza di rischi e responsabilità connesse allo svolgimento di determinati ruoli tecnici in ambito informatico, quali il ruolo di amministratore di sistema, che comportano, quasi sempre, la concreta possibilità per i soggetti incaricati di accedere in modo privilegiato alle risorse del sistema informativo e di trattare in modo arbitrario e discrezionale i dati personali in esse contenuti.
In generale l'obiettivo del provvedimento è evitare che i Titolari affidino incautamente incarichi di amministratore di sistema o omettano di adottare "idonee e preventive" misure di sicurezza specificatamente previste per lo svolgimento di attività di amministrazione di sistemi informatici, esponendosi, così, al rischio di ingenti sanzioni amministrative e gravose responsabilità civili e penali derivanti da eventuali comportamenti illeciti dei soggetti individuati.

Capitolo I - Inquadramento normativo

Sommario: 1.1. Il Provvedimento generale del Garante Privacy del 27 Novembre 2008 - 1.2. Riferimenti normativi.

1.1. Il Provvedimento generale del Garante Privacy del 27 Novembre 2008

Il Provvedimento Generale del Garante Privacy del 27 Novembre 2008 denominato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e pubblicato nella G.U. n. 300 del 24 dicembre 2008, trae la sua origine dai compiti istituzionalmente attribuiti al Garante per la Protezione dei Dati Personali dall'articolo 154 del D.lgs. 196/03.
In particolare il provvedimento in questione si richiama all'articolo 154, comma 1, lettera h) del Codice Privacy che prevede tra i compiti dell'Autorità Garante Privacy 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" e all'articolo 154, comma 1, lettera c) che prevede anche la possibilità, da parte del Garante Privacy, di prescrivere misure e accorgimenti, specifici o di carattere generale, che i titolari di trattamento sono tenuti ad adottare.
Considerata, quindi, la natura amministrativa del Provvedimento, le misure e gli accorgimenti prescritti in materia di attribuzioni di funzioni di amministratore di sistema, sono da considerarsi misure di sicurezza a cui i titolari devo attenersi ai sensi dell'articolo 31 del D.lgs. 196/03 e non misure minime di sicurezza da adottare ai sensi dell'articolo 33 del D.lgs. 196/03.
Al fine di dare il massimo eco alla novità normativa, in data 14 Gennaio 2009, il Garante Privacy ha emesso un Comunicato stampa intitolato "Amministratori di sistema: occorre massima trasparenza sul loro operato. Il Garante fissa i criteri, quattro mesi per mettersi in regola" con il quale ha chiarito il senso e le motivazioni che stanno alla base dell'emanazione del suddetto provvedimento.
"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" in data 12 Febbraio 2009 il Garante Privacy ha emanato un Provvedimento a carattere generale intitolato "Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" pubblicato nella G.U. n. 45 del 24 febbraio 2009, con il quale ha ravvisato la necessità di prorogare i termini previsti per l'adempimento delle prescrizioni disponendo come termine ultimo per l'adozione delle misure e degli accorgimenti prescritti il 30 giugno 2009.
Contestualmente l'Autorità Garante per la Protezione dei Dati Personali, tenuto conto di quanto emerso a seguito di alcuni incontri svoltisi con associazioni rappresentative di categoria e delle memorie e dei quesiti ricevuti anche da singoli titolari del trattamento, ha deciso di dare avvio ad una consultazione pubblica con Deliberazione del 21 Aprile 2009 denominata "Amministratori di sistema: avvio di una consultazione pubblica" pubblicata nella G.U. n. 105 dell' 8 maggio 2009, al fine di acquisire ulteriori elementi di valutazione sull'impatto organizzativo e tecnico che le prescrizioni del provvedimento del 27 novembre 2008 possono avere sulle strutture aziendali dei titolari.
Con la suddetta Deliberazione il Garante Privacy ha altresì predisposto la pubblicazione sul sito dell'Autorità www.garanteprivacy.it alcune FAQ (risposte a quesiti posti più frequentemente) relative all'interpretazione del Provvedimento del 27 Novembre 2008.
Recependo alcune delle indicazioni emerse nel corso della consultazione pubblica per facilitare il corretto adempimento alle prescrizioni impartite, il Garante Privacy, con il Provvedimento a Carattere Generale del 25 giugno 2009 denominato "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento" pubblicato nella G.U. n. 149 del 30 giugno 2009, ha ritenuto di dover integrare e parzialmente modificare il Provvedimento del 27 Novembre 2008

prorogando contestualmente i termini previsti, disponendo che i titolari del trattamento adottino le misure e gli accorgimenti del Provvedimento, come modificato e integrato, entro il 15 dicembre 2009.
Infine in vista della scadenza del 15 dicembre 2009, termine entro il quale i titolari dovevano adeguarsi alle prescrizioni impartite in materia di amministratori di sistema, il Garante Privacy ha emesso un Comunicato Stampa datato 10 dicembre 2009 e denominato "Amministratori di sistema: precisazioni del Garante" con il quale ha ritenuto opportuno precisare alcuni aspetti tecnici e organizzativi al fine di evitare ingiustificati oneri economici per le aziende dovuti a informazioni imprecise o azioni commerciali e promozionali tecnicamente e deontologicamente non corrette promosse da aziende informatiche e consulenti aziendali senza scrupoli.

1.2. Riferimenti normativi

- Provvedimento a carattere generale del 27 novembre 2008: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - G.U. n. 300 del 24 dicembre 2008 - Doc. Web n. 1577499.
- Provvedimento a carattere generale del 25 giugno 2009: Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - G.U. n. 149 del 30 giugno 2009 - Doc. Web n. 1626595.
- Provvedimento a carattere generale del 27 novembre 2008: Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali - G.U. n. 287 del 9 dicembre 2008 - Doc. Web n. 1577499.
- Provvedimento a carattere generale del 12 febbraio 2009: Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - G.U. n. 45 del 24 febbraio 2009 - Doc. Web n. 1591970.
- Deliberazione del 21 aprile 2009 Amministratori di sistema: avvio di una consultazione pubblica - 21 aprile 2009 - G.U. n. 105 dell'8 maggio 2009 - Doc. Web n. 1611986.
- Comunicato stampa del 23 febbraio 2009 Amministratori di sistema: prorogati i termini per gli adempimenti.

Capitolo II - La figura dell'amministratore di sistema

Sommario: 2.1. Profili generali - 2.2. Amministratore di Sistema e Operatore di Sistema - 2.3. Il modello organizzativo privacy per gli Amministratori Di Sistema.

2.1. Profili generali

Generalmente in informatica, con il termine "Amministratore di Sistema" si fa riferimento a quel soggetto che, a vario titolo, compie operazioni di gestione e/o manutenzione di un sistema informativo aziendale.
In ambito privacy, la figura dell'Amministratore di Sistema è data introdotta per la prima volta con il Decreto del Presidente della Repubblica n. 318 del 28 Luglio 1999, che ne ha disciplinato il ruolo all'articolo 1), comma 1), lett. c) definendolo come 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".
Con l'entrata in vigore del D. lgs. 196/03 (testo unico abrogativo del D.P.R. 318/99), tale figura ha perso la sua collocazione formale tra le definizioni normative in materia di protezione dei dati personali, trovando solo richiami marginali e indiretti nell'Allegato B) relativamente a soggetti che compiono operazioni quali "backup" e "recovery" dei dati, custodia delle credenziali e gestione dei sistemi di autenticazione e di autorizzazione.
Partendo dal presupposto che l'Amministratore di Sistema è una figura essenziale per la sicurezza delle banche dati e per la corretta gestione del sistemi informativi, che comporta "la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali", il Garante Privacy con proprio Provvedimento del 27 Novembre 2008 ha deciso di reintrodurre tale figura nel panorama normativo italiano, prescrivendo ai titolari del trattamento l'adozione di specifiche misure tecniche ed organizzative di sicurezza.
A seguito dell'introduzione del Provvedimento del 27 Novembre 2008, la definizione informatica di "Amministratore di Sistema", ha così assunto connotati specifici e ha ampliato la sua portata fino ad includere "[…] 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 […]" nonché "[…] soggetti preposti ad attività riconducibili alle mansioni tipiche dei c.d. "amministratori di sistema" […]" o "[…] analoghe in rapporto a sistemi di elaborazione e banche di dati […].
Ai sensi del Provvedimento del 27 Novembre 2008 sono, pertanto, da considerare a tutti gli effetti Amministratori di Sistema i soggetti che in via continuativa svolgono operazioni di:

- Amministrazione di Sistemi Informatici (System Administrator)
- Amministrazione di Server (Server Administrator)
- Amministrazione di Apparati Hardware (Hardware Administrator)
- Amministrazione di Sistemi di Rete (Network Administrator)
- Amministrazione di Sistemi di Sicurezza (Security Administrator)
- Amministrazione di Software e Applicazioni (Application Administrator)
- Amministrazione di Database (Database Administrator)
- Amministrazione di Sistemi di Salvataggio Dati (Backup / Storage Administrator)
- Amministrazione di Sistemi di Ripristino Dati (Recovery Administrator)
- Amministrazione di Siti Web (Web Administrator)
- Altri soggetti addetti alla gestione o alla manutenzione di strumenti elettronici che per l'espletamento delle loro funzioni devono compiere operazioni di amministrazione.

Il Provvedimento prevede esplicitamente che "[…] non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono […] sui sistemi di elaborazione e sui sistemi software […]"; tali soggetti, pertanto, devono essere svolte inquadrati, come semplici addetti alla manutenzione di strumenti elettronici e non come amministratori di sistema.

2.2. Amministratore di Sistema e Operatore di Sistema

Con il Provvedimento del 27 Novembre 2008 il Garante Privacy "[…] non ha inteso equiparare gli operatori di sistema di cui agli articoli del Codice penale relativi ai delitti informatici, con gli amministratori di sistema […]" in quanto questi ultimi sono da considerarsi semplicemente dei "[…] particolari operatori di sistema, dotati di specifici privilegi […]".
Partendo da questa affermazione, risulta, quindi, necessario precisare ulteriormente il rapporto che intercorre tra "Operatore del Sistema" – figura che assume rilevanza come circostanza aggravante in caso di delitto informatico - e "Amministratore di Sistema".
Osservando il panorama legislativo italiano, si evince che non esiste una definizione legislativa, né tantomeno un´interpretazione giurisprudenziale e dottrinale univoca e sedimentata di "Operatore del Sistema".
L'espressione "Operatore del Sistema", infatti, trae la sua origine dalla traduzione letterale del termine inglese "System Operator", che in ambito informatico anglosassone identifica colui che sorveglia o fa funzionare un sistema informatico multiutente.
Attenendosi strettamente al significato originario del termine, parte minoritaria della dottrina italiana, ritiene che "per operatore di sistema debba intendersi quella particolare figura di tecnico dell'informatica che assume la qualifica di system administrator. Questi presiede al corretto funzionamento del sistema e della rete, stabilisce le condizioni e le procedure che legittimano gli utenti all'accesso, organizza la condivisione delle risorse disponibili, ha, in altri termini, piena disponibilità dell'intera struttura informatica."
Parte maggioritaria della dottrina, invece, discostandosi dal significato originale, ritiene che "l'operatore di sistema non è […] soltanto colui che professionalmente - in via continuativa o quantomeno non occasionale - si trova ad operare quale operatore programmatore, sistemista o analista sull´hardware o sul software di un sistema informatico , ma anche il soggetto che di fatto, in relazione alle funzioni svolte […] si trova nella condizione di poter intervenire - direttamente o per interposta persona,nell´esercizio e/o a causa delle sue funzioni - sui dati o sui programmi. Ciò a prescindere sia dalla natura "intrinsecamente" informatica dell´incarico svolto o del ruolo ricoperto, sia dalla natura del rapporto con l´ente."
Secondo tale dottrina è ricompreso nella categoria di operatore di sistema "chiunque sia legittimato ad operare sul sistema (anche nella qualifica di semplice addetto alla immissione dei dati)" o chiunque si trovi in una "condizione privilegiata, di garanzia e tutela del sistema nel suo insieme" volendo così porre in risalto il collegamento funzionale esistente tra un determinato soggetto ed uno specifico sistema informatico in virtù del rapporto privilegiato e fiduciario derivante del ruolo e della mansione aziendale ricoperta.
In definitiva, il Garante Privacy, con il proprio Provvedimento del 27 Novembre 2008, ha deciso di aderire per la teoria maggioritaria, inquadrando l'Amministratore di Sistema come un particolare Operatore di Sistema, con competenze, mansioni, operatività, ambito di autonomia e responsabilità più elevati.

2.3. Il modello organizzativo privacy per gli Amministratori Di Sistema

Il Garante Privacy con il Provvedimento del 27 Novembre 2008, ha inteso introdurre come misura di sicurezza per i Titolari del trattamento, l'adozione di un modello organizzativo privacy per gli amministratori di sistema.
Tale modello dovrà essere realizzato nel rispetto dei principi fondamentali in materia di protezione dei dati personali e in osservanza delle specifiche prescrizioni del Garante Privacy in materia di amministratori di sistema; inoltre dovrà essere inserito e integrato nel Sistema di Gestione Privacy Aziendale e armonizzato con l'eventuale Sistema di Gestione 231 ove adottato.
In particolare i Titolari del trattamento, per progettare e implementare un corretto e modello organizzativo privacy per gli amministratori di sistema, dovranno sempre rispettare il seguente iter procedimentale previsto dal Provvedimento:

•Valutare le competenze tecniche e le caratteristiche soggettive dei potenziali amministratori di sistema (Art. 2.1.a del Provvedimento 27/11/08)

•Designare individualmente gli amministratori di sistema selezionati (Art. 2.1.b del Provvedimento 27/11/08)
•Aggiornare il Documento Programmatico sulla Sicurezza e redigere un documento interno contenente gli estremi identificativi e l'elenco delle funzioni attribuite ad ogni amministratore di sistema designato (Art. 2.1.c del Provvedimento 27/11/08)
•Contrattualizzare e regolamentare gli eventuali servizi di amministrazione di sistema affidati in outsourcing (Art. 2.1.d del Provvedimento 27/11/08)
•Implementare un sistema di verifica e controllo dell'operato degli amministratori di sistema designati (Art. 2.1.e del Provvedimento 27/11/08)
•Adottare una soluzione tecnologica idonea per la registrazione degli accessi effettuati dagli amministratori di sistema designati (Art. 2.1.f del Provvedimento 27/11/08)

Capitolo III - La valutazione delle competenze dell'amministratore di sistema

Sommario: 3.1. La valutazione delle competenze dell'Amministratore di Sistema.

3.1. La valutazione delle competenze dell'Amministratore di Sistema

"[…] 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 […]"

Ai sensi dell'articolo 2 comma 1 lettera a) del Provvedimento del 27 Novembre 2008 "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."
Incombe, pertanto, sul Titolare l'onere di valutare accuratamente le competenze professionali del soggetto candidato alla posizione di amministratore di sistema, prima di una sua formale designazione, al fine di non incorrere in "culpa in eligendo" ovvero la colpa per aver effettuato un'incauta scelta.
Per tale motivo il Titolare dovrebbe designare l'amministratore di sistema selezionandolo tra le seguenti categorie di soggetti:

- Laureati in Informatica
- Laureati in Ingegneria Informatica
- Laureati in Matematica con Indirizzo Informatico
- Laureati in altre Facoltà con indirizzo Informatico
- Periti Informatici
- Diplomati in altri Istituti con Indirizzo Informatico

Tali soggetti dovrebbero, inoltre, aver maturato un'esperienza almeno triennale nella specifica area intervento e preferibilmente avere ottenuto almeno una delle seguenti certificazioni professionali attinenti all'incarico assegnato:

- Certificazione EUCIP - IT Administrator
- Certificazione MCSA - Microsoft Certified Systems Administrator
- Certificazione MCDBA - Microsoft Certified Database Administrator
- Certificazione MCITP - Microsoft Certified IT Professional: Database Administrator
- Certificazione Red Hat
- Certificazione LPIC-3 "Core" and LPI Specialty - Senior Level Linux Professional
- Certificazione Ubuntu Certified Professional
- Certificazione SCSA - Sun Certified System Administrator
- Certificazione SCNA - Sun Certified Network Administrator
- Certificazione SCSECA - Sun Certified Security Administrator
- Certificazione SCEA - Sun Certified Enterprise Architect
- Certificazione CCSP – Cisco Certified Security Professional
- Certificazione CCNP - Cisco Certified Network Professional
- Certificazione CISM - Certified Information Security Manager
- Certificazione SCNS - Security Certified Network Specialist
- Certificazione SCNP - Security Certified Network Professional
- Certificazione SCNA - Security Certified Network Architect
- Certificazione CMDBA - Certified MySQL Database Administrator
- Certificazione Oracle Database Administrator Certified Professional
- Certificazione Oracle Enterprise Linux Administrator

In ogni caso, il soggetto da designare Amministratore di Sistema dovrebbe almeno possedere le seguenti competenze e capacità:
•analisi, progettazione e sviluppo, anche in collaborazione con consulenti esterni, di sistemi informativi, di programmi applicativi e di reti di telecomunicazione;
•sviluppo in maniera autonoma e indipendente di piccoli pacchetti software nell'ambito di applicazioni aziendali (quali a titolo esemplificativo sistemi di acquisizione ed elaborazione dati, banche dati…)
•realizzazione e gestione di piccole reti lan e wlan aziendali;
•installazione e configurazione di server, di client, di router, di firewall ed di altri apparati di rete;
•assistenza agli utenti nell'utilizzo degli strumenti elettronici aziendali fornendo consulenza e formazione di base in ambito software e hardware.

Per quanto concerne i requisiti morali che deve possedere il soggetto da designare amministratore di sistema la "Risposta n. 20 alle domande più frequenti (FAQ) del Provvedimento sugli Amministratori di sistema del 27 Novembre 2008" specifica che "[…] le caratteristiche da prendere in considerazione, al comma 2, lettera a), del dispositivo […]" sono " […] esperienza […] capacità e […] affidabilità del soggetto designato. Si tratta quindi di qualità tecniche, professionali e di condotta, non di requisiti morali."
Pertanto, per adempiere correttamente alle disposizioni del Provvedimento del 27 Novembre 2008, risulta obbligatorio per il Titolare solamente l'accertamento dei requisiti professionali posseduti dal soggetto che si intende designare amministratore di sistema e non anche dei requisiti morali.
Chiaramente considerata la specificità, l'importanza e la criticità del ruolo di amministratore di sistema, la cui condotta può dar seguito a sanzioni penali oltre che amministrative e civili, sarebbe buona norma verificare la concreta affidabilità e serietà del soggetto da designare anche in termini di passata condotta professionale e personale.

Capitolo IV - La designazione dell'amministratore di sistema

Sommario: 4.1. La designazione dell'Amministratore di Sistema.

4.1. La designazione dell'Amministratore di Sistema

"[…]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 […]"

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

"Servizi in outsourcing

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

Ai sensi dell'articolo 2 comma 1 lettera b) del Provvedimento del 27 Novembre 2008 "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."
Il Titolare può scegliere indifferentemente di designare come amministratore di sistema o una persona fisica o una persona giuridica.
Qualora opti per la designazione di una persona fisica potrà utilizzare in alternativa la figura di "incaricato del trattamento" ai sensi dell'art. 30 del D.lgs. 196/03 o la figura di "responsabile del trattamento" ai sensi dell'art. 29 del D.lgs. 196/03.
"[…] nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice" il titolare dovrà "attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29."
Pertanto in caso di designazione di una persona fisica quale amministratore di sistema, il soggetto candidato dovrà essere "individuato tra 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" e la designazione dovrà essere effettuata per iscritto e individuare puntualmente l'ambito del trattamento consentito.
Qualora ai sensi dell'articolo 2 comma 1 lettera d) del Provvedimento del 27 Novembre 2008, il Titolare decida di affidare in outsourcing a una persona giuridica il servizio di amministrazione di sistema, dovrà forzatamente utilizzare per la designazione la figura del "responsabile del trattamento" ai sensi dell'art. 29 del d.lgs. 196/03.
In tal caso i "compiti affidati al responsabile" saranno "analiticamente specificati per iscritto dal titolare" e il responsabile effettuerà "il trattamento attenendosi alle istruzioni impartite

dal titolare il quale, anche tramite verifiche periodiche" vigilerà sulla loro puntuale osservanza.
Inoltre, dovranno essere conservati direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche a cui il Titolare o l'Outsourcer affideranno mansioni operative di amministrazione di sistema in quanto, ai sensi dell'articolo 2 comma 1 lettera c) del Provvedimento del 27 Novembre 2008, "Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante."
Per "estremi identificativi", come precisato dalla "Risposta n. 21 alle domande più frequenti (FAQ) del Provvedimento sugli Amministratori di sistema del 27 Novembre 2008", si intende quel "[…] minimo insieme di dati identificativi utili a individuare il soggetto nell'ambito dell'organizzazione di appartenenza. In molti casi possono coincidere con nome, cognome, funzione o area organizzativa di appartenenza."
Il documento interno contenente l'Elenco Nominativo degli Amministratori di Sistema potrà essere integrato in una specifica sezione del Documento Programmatico sulla Sicurezza del Titolare dedicata agli Amministratori di Sistema o essere inserito come un suo allegato al fine di renderne più agevole la gestione e l'aggiornamento.
"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", il Titolare ha l'obbligo di rendere noti o conoscibili al personale dipendente gli estremi identificativi degli amministratori di sistema "[…] quale forma di trasparenza interna all'organizzazione a tutela dei lavoratori […]".
Tale obbligo si rende necessario "[…] nel caso in cui un amministratore di sistema, oltre a intervenire sotto il profilo tecnico […] tratti anche dati personali riferiti ai lavoratori […] o sia nelle condizioni di acquisire conoscenza di dati a essi riferiti […]" e può essere assolto inserendo gli estremi identificativi degli Amministratori di Sistema designati nell'Informativa Privacy Dipendenti ex art. 13 del D.lgs. 196/03 o nel Disciplinare Interno sull'utilizzo degli strumenti elettronici ex Provvedimento del Garante Privacy n. 13/2007 "Lavoro: le linee guida del Garante per posta elettronica e internet" o, in alternativa, utilizzando altri strumenti di comunicazione interna (quali a titolo esemplificativo intranet aziendale, ordini di servizio, bollettini…).

Capitolo V - La registrazione degli accessi e la verifica delle attività dell'amministratore di sistema

Sommario: 5.1. La registrazione degli accessi dell'Amministratore di Sistema - 5.2. La verifica delle attività dell'Amministratore di Sistema.

5.1. La registrazione degli accessi dell'Amministratore di Sistema

"[…] 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 […]"

Ai sensi dell'articolo 2 comma 1 lettera f) del Provvedimento del 27 Novembre 2008 "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 […]"
La definizione legislativa di "accesso logico" può essere ricavata dall'articolo 1 comma 1) lettera b) del Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale" che definisce "autenticazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso".
Con la terminologia "registrazione degli accessi logici ai sistemi di elaborazione" il Garante Privacy, però, si riferisce esclusivamente alla registrazione degli eventi generati da uno strumento elettronico mediante il proprio sistema di autenticazione al momento dell'accesso, della disconnessione o del semplice tentativo di accesso da parte di un amministratore di sistema.
Nell'ottica del provvedimento, infatti, la registrazione degli accessi logici si rende necessaria per garantire la tracciabilità delle attività svolte dagli amministratori di sistema e permettere al Titolare la verifica periodica delle operazioni da questi effettivamente compiute.
Tra gli accessi logici a sistemi e archivi elettronici sono comprese le autenticazioni nei confronti dei data base management system (DBMS) e gli accessi logici ai client.
Sempre ai sensi dell'articolo 2 comma 1 lettera f) "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".
Tecnicamente con il termine "file di log" o semplicemente "log" si definisce quel "giornale di bordo" nel quale vengono registrate in ordine cronologico tutte le operazioni eseguite su un elaboratore elettronico.
Il log è un file sequenziale sempre aperto in scrittura, che viene chiuso e conservato a cadenze regolari e reso disponibile per una serie di operazioni tecniche di amministrazione (quali a titolo esemplificativo analisi delle segnalazioni di errore, produzione di statistiche, analisi di operazioni compiute…) nel quale sono registrati i riferimenti allo "username" utilizzato, la data e l'ora e la descrizione di un evento.
L'insieme degli eventi censiti nel sistema di log deve comprendere tutti gli eventi di accesso effettuati dagli amministratori di sistema su tutti i sistemi di elaborazione con cui vengono trattati, anche indirettamente, dati personali.
La raccolta dei log serve per verificare anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso…).
In un sistema di elaborazione dati, coesistono diversi tipi di log:

- Log di sistema
- Log di applicazione
- Log di base dati

Per quanto concerne le modalità di registrazione e conservazione dei log degli accessi effettuati dagli amministratori di sistema, la valutazione

della procedura più idonea deve essere valutata dal Titolare in base al sistema informativo aziendale e ai risultati dell'analisi dei rischi.
Al fine di rispettare le caratteristiche di integrità, inalterabilità e completezza dei file di log, è comunque buona norma che il Titolare progetti e implementi il sistema di registrazione dei log attenendosi alle best practice internazionali in materia di Computer Forensic.

5.2. La verifica delle attività dell'Amministratore di Sistema

"[…]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 o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti"

Ai sensi dell'articolo 2 comma 1 lettera e) del Provvedimento del 27 Novembre 2008 "L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari […] in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti […]"
Tale obbligo si collega alle prescrizioni previste dall'art. 29 del D.lgs. 196/03, che impongono al responsabile di effettuare "[…] il trattamento attenendosi alle istruzioni impartite […]" e al Titolare di vigilare sulla loro puntuale osservanza "anche tramite verifiche periodiche.
La verifica dovrà avvenire su base periodica infrannuale e dovrà avere come oggetto l'analisi dell'operato dell'amministratore di sistema nell'esercizio delle sue funzioni al fine di accertarsi che le attività svolte risultino conformi alle mansioni assegnate e alle istruzioni impartite.

Capitolo VI - I casi di esclusione e le responsabilità dell'amministratore di sistema

Sommario: 6.1. I casi di esclusione - 6.2. Le responsabilità dell'Amministratore di Sistema - 6.3. La legalità del provvedimento.

6.1. I casi di esclusione

Il Provvedimento del 27 Novembre 2008 "prescrive l'adozione delle […] misure ai titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici […] salvo per quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili […] oggetto delle misure di semplificazione introdotte di recente per legge […]"
Pertanto ai sensi dell'articolo 5 del D.lgs. 196/03 è soggetto alle prescrizioni del Provvedimento del 27 Novembre 2008 chiunque è stabilito nel territorio dello Stato Italiano o in un luogo comunque soggetto alla sovranità dello Stato Italiano ed effettua trattamenti di dati personali con strumenti elettronici ovvero chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti elettronici situati nel territorio dello Stato Italiano.
Ai sensi dell'articolo 1 comma 1-bis del D. lgs. 196/03, sono, invece, esenti dall'applicazione delle prescrizioni del Provvedimento del 27 Novembre 2008 "i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori […] senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale […]" e i soggetti che trattano esclusivamente dati personali "[…] per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani […]" in quanto tali trattamenti pongono minori rischi per gli interessati.
Pertanto in via generale, il Provvedimento del 27 Novembre 2008 in materia di amministratori di sistema non si applica a quei soggetti "[…] dotati di sistemi informatici di modesta e limitata entità e comunque non particolarmente complessi […] che possano fare a meno di una figura professionale specificamente dedicata alla amministrazione dei sistemi […]" che rientrano trai soggetti pubblici o privati per cui è prevista la semplificazione delle misure di sicurezza di cui all'articolo 1 del Provvedimento Carattere Generale 27 Novembre 2008 denominato "Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali".

6.2. Le responsabilità dell'Amministratore di Sistema

Per quanto riguarda le responsabilità civili e penali che gravano sui soggetti che ricoprono il ruolo di amministratore di sistema, il Garante Privacy con il Provvedimento del 27 Novembre 2008 non assume una chiara e precisa posizione.
In linea generale, le responsabilità dell'amministratore di sistema dipendono dal tipo di ruolo e di inquadramento privacy (incaricato o responsabile) definite dal Titolare e dal grado di autonomia decisionale e di spesa ad esso concesso.
In ogni caso i principali reati privacy in cui può facilmente incorrere un amministratore di sistema nell'esercizio delle funzioni attribuite sono sicuramente il trattamento illecito di dati e la mancata adozione di misure minime di sicurezza.
Inoltre in caso di reati informatici è sempre considerata circostanza aggravante, la commissione del delitto da parte di un soggetto che ricopre il ruolo di amministratore di sistema, in quanto viene meno la natura fiduciaria instaurata con il Titolare del trattamento.

6.3. La legalità del provvedimento

Il Provvedimento del 27 Novembre 2008 prescrive l'adozione di misure di sicurezza in materia di Amministratori di Sistema sulla base dei poteri attribuiti al Garante Privacy dall'art. 154, comma 1, lett. c) del D.lgs. 196/03, il quale prevede che "[…] il Garante […] ha il compito di […] prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143 […].

Considerato, però, che l'art. 143 del Codice Privacy disciplina il "Procedimento per i reclami" ovvero che "Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante […] prescrive al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti […]" appare del tutto infondato il presupposto normativo sul quale si regge la prescrizione di adozione di specifiche misure per tutti i titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice salvo i casi di esclusione.

Sulla base di quanto detto appare evidente che il Provvedimento in questione risulta viziato di eccesso di potere e in quanto tale atto amministrativo annullabile.

Pertanto alla luce di quanto finora detto, le prescrizioni di cui al Provvedimento del 27 Novembre 2008 non possono essere considerate misure di sicurezza obbligatorie, né tanto meno misure minime di sicurezza ai sensi dell'art 33 del D.lgs. 196/03 in quanto essendo la mancata adozione di misure minime di sicurezza considerata reato, l'introduzione di nuove tipologie di misure minime di sicurezza è sempre soggetta a riserva di legge.

Conclusioni

Alla luce di quanto sinora illustrato, l'amministratore di sistema risulta una figura imprescindibile per la corretta implementazione e gestione dei sistemi informativi aziendali, nonchè per la protezione dei dati personali e per la sicurezza delle informazioni.
Il soggetto da designare amministratore di sistema, dovrà sempre essere una persona fisica o giuridica dalle comprovate capacità tecniche, dotato di esperienza pluriennale e competenze specifiche in ambito sistemistico e di programmazione in grado di gestire con ampia autonomia i sistemi informativi presenti in azienda.
Considerata l'estrema importanza e delicatezza del ruolo, qualora il titolare opti per un amministratore di sistema interno, il soggetto da designare dovrà avere la massima fiducia da parte della Direzione Aziendale ed essere inquadrato con un ruolo idoneo al grado di responsabilità assegnato e godere di ampia autonomia decisionale e di spesa in ambito informatico.
Al fine di supervisionare l'operato degli amministratori di sistema designati, infine, il titolare dovrà implementare un sistema di raccolta e gestione dei log di access, che dovrà essere affidato ad un soggetto terzo in maniera tale da garantire inalterabilità e inaccessibilità dei log e imparzialità nelle operazioni di verifica periodica delle operazioni compiute dagli amministratori di sistema.

Allegato I

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

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

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

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

VISTO il Codice in materia di protezione dei dati personali (D.lgs. 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 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; Provv. Garante 6 novembre 2008), debbano essere allo stato esclusi dall'ambito applicativo del presente provvedimento;

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

RELATORE il prof. Francesco Pizzetti;

PREMESSO:

1. Considerazioni preliminari

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.
Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.
La rilevanza, la specificità e la particolare criticità del ruolo dell'amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante. Ci si riferisce, in particolare, all'abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615 ter) e di frode informatica (art. 640 ter), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (artt. 635 bis e ter) e di danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinquies) di recente modifica. [1]
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

[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".

fiduciaria delle relative mansioni, analoga a quella che, in un contesto del tutto differente, caratterizza determinati incarichi di custodia e altre attività per il cui svolgimento è previsto il possesso di particolari requisiti tecnico-organizzativi, di onorabilità, professionali, morali o di condotta, a oggi non contemplati per lo svolgimento di uno dei ruoli più delicati della "Società dell'informazione".[2]

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

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

Con il presente provvedimento il Garante intende pertanto richiamare tutti i titolari di trattamenti effettuati, anche in parte, mediante strumenti elettronici alla necessità di prestare massima attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema.

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

[2] 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.lgs. 7 marzo 2005, n. 82).

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

4.4. Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da 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 in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.

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

d. Servizi in outsourcing

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

e. Verifica delle 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 o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

f. Registrazione degli accessi

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;

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

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

4. 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.[3]

Roma, 27 novembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

[3] Aggiunto in base al provvedimento del 25 giugno 2009.

Provvedimento "Amministratori di sistema" del 27 novembre 2008

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

Risposte alle domande più frequenti (FAQ)

1 Cosa deve intendersi per "amministratore di sistema"?

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

3 Il caso di uso esclusivo di un personal computer da parte di un solo amministratore di sistema rientra nell'ambito applicativo del provvedimento?

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

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

6 Chiarire i casi di esclusione dall'obbligo di adempiere al provvedimento.

7 Cosa si intende per descrizione analitica degli ambiti di operatività consentiti all'ADS?

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

9 Cosa si intende per access log (log-in, log-out, tentativi falliti di accesso, altro?...)

10 Laddove il file di log contenga informazioni più ampie, va preso tutto il log o solo la riga relativa all'access log?

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

12 Come va interpretata la caratteristica di inalterabilità dei log?

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

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

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

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

17 Cosa si intende per "consultazione in chiaro"?

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

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

20 Nella designazione degli amministratori di sistema occorre valutare i requisiti morali?

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

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

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

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

1) Cosa deve intendersi per "amministratore di sistema"?

In assenza di definizioni normative e tecniche condivise, nell'ambito del provvedimento del Garante l'amministratore di sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
Il Garante non ha inteso equiparare gli "operatori di sistema" di cui agli articoli del Codice penale relativi ai delitti informatici, con gli "amministratori di sistema": questi ultimi sono dei particolari operatori di sistema, dotati di specifici privilegi.
Anche il riferimento al D.P.R. 318/1999 nella premessa del provvedimento è puramente descrittivo poiché la figura definita in quell'atto normativo (ormai abrogato) è di minore portata rispetto a quella cui si fa riferimento nel provvedimento.
Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (p. es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software.

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

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

3) Il caso di uso esclusivo di un personal computer da parte di un solo amministratore di sistema rientra nell'ambito applicativo del provvedimento?

Non è possibile rispondere in generale. In diversi casi, anche con un personal computer possono essere effettuati delicati trattamenti rispetto ai quali il titolare ha il dovere di prevedere e mettere in atto anche le misure e gli accorgimenti previsti nel provvedimento. Nel caso-limite di un titolare che svolga funzioni di unico amministratore di sistema, come può accadere in piccolissime realtà d'impresa, non si applicheranno le previsioni relative alla verifica delle attività dell'amministratore né la tenuta del log degli accessi informatici.

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

Si, anche i client, intesi come "postazioni di lavoro informatizzate", sono compresi tra i sistemi per cui devono essere registrati gli accessi degli ADS.
Nei casi più semplici tale requisito può essere soddisfatto tramite funzionalità già disponibili nei più diffusi sistemi operativi, senza richiedere necessariamente l'uso di strumenti software o hardware aggiuntivi. Per esempio, la registrazione locale dei dati di accesso su una postazione, in determinati contesti, può essere ritenuta idonea al corretto adempimento qualora goda di sufficienti garanzie di integrità.
Sarà comunque con valutazione del titolare che dovrà essere considerata l'idoneità degli strumenti disponibili oppure l'adozione di strumenti più sofisticati, quali la raccolta dei log centralizzata e l'utilizzo di dispositivi non riscrivibili o di tecniche crittografiche per la verifica dell'integrità delle registrazioni.

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

È da sottoporre a verifica l'attività svolta dall'amministratore di sistema nell'esercizio delle sue funzioni. Va verificato che le attività svolte dall'amministratore di sistema siano conformi alle

mansioni attribuite, ivi compreso il profilo relativo alla sicurezza.

6) Chiarire i casi di esclusione dall'obbligo di adempiere al provvedimento.

Sono esclusi i trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle misure di semplificazione introdotte nel corso del 2008 per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 27 novembre 2008).

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

Il provvedimento prevede che all'atto della designazione di un amministratore di sistema, venga fatta "elencazione analitica" degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, ovvero la descrizione puntuale degli stessi, evitando l'attribuzione di ambiti insufficientemente definiti, analogamente a quanto previsto al comma 4 dell'art. 29 del Codice riguardante i responsabili del trattamento.

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

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

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

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

Gli event record generati dai sistemi di autenticazione contengono usualmente i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento (timestamp) e una descrizione dell'evento (sistema di elaborazione o software utilizzato, se si tratti di un evento di log-in, di log-out, o di una condizione di errore, quale linea di comunicazione o dispositivo terminale sia stato utilizzato…).

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

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

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

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

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

Caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di log sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con apposito software. Il requisito può essere ragionevolmente soddisfatto con la strumentazione software in dotazione, nei casi più semplici, e con l'eventuale esportazione

periodica dei dati di log su supporti di memorizzazione non riscrivibili. In casi più complessi i titolari potranno ritenere di adottare sistemi più sofisticati, quali i log server centralizzati e "certificati".
È ben noto che il problema dell'attendibilità dei dati di audit, in genere, riguarda in primo luogo la effettiva generazione degli auditable event e, successivamente, la loro corretta registrazione e manutenzione. Tuttavia il provvedimento del Garante non affronta questi aspetti, prevedendo soltanto, come forma minima di documentazione dell'uso di un sistema informativo, la generazione del log degli "accessi" (login) e la loro archiviazione per almeno sei mesi in condizioni di ragionevole sicurezza e con strumenti adatti, in base al contesto in cui avviene il trattamento, senza alcuna pretesa di instaurare in modo generalizzato, e solo con le prescrizioni del provvedimento, un regime rigoroso di registrazione degli usage data dei sistemi informativi.

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

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

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

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

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

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

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

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

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

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

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

Sì.

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

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

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

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

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

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

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

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

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

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

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

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

Allegato II

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

(G.U. n. 45 del 24 febbraio 2009)

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. lgs. 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 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

Allegato III

Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - 25 giugno 2009

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

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. Filippo Patroni Griffi, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (D. lgs. 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 (di seguito, "Provvedimento");

VISTO il provvedimento del Garante del 12 febbraio 2009 con cui si è disposto di unificare e contestualmente prorogare i termini per l'adempimento delle prescrizioni di cui al citato Provvedimento procrastinandone la scadenza al 30 giugno 2009, pubblicato sulla G.U. n. 45 del 24 febbraio 2009;

VISTO il provvedimento del Garante del 21 aprile 2009 con cui si è deciso di attivare una consultazione pubblica volta ad acquisire osservazioni e commenti da parte dei titolari del trattamento ai quali il provvedimento si rivolge con esclusivo riferimento a quanto prescritto al punto 2 del Provvedimento, dando tempo fino al 31 maggio 2009 per far pervenire osservazioni e commenti, pubblicato sulla G.U. n. 105 dell'8 maggio 2009;

TENUTO CONTO dei numerosi contributi pervenuti, sia da singoli titolari del trattamento sia da associazioni rappresentative di categoria, che evidenziano taluni problemi applicativi relativi alla completa attuazione di alcune delle misure e degli accorgimenti prescritti nel Provvedimento;

CONSIDERATO che, oltre ai predetti contributi, sono pervenute anche richieste di differimento dei termini indicati nel provvedimento del 12 febbraio 2009;

RILEVATA pertanto l'opportunità di integrare e parzialmente modificare il Provvedimento recependo alcune delle indicazioni emerse nel corso della consultazione pubblica per facilitare il corretto adempimento alle prescrizioni impartite, senza compromettere il livello di tutela assicurato agli interessati;

RITENUTO, in particolare, di prevedere che le prescrizioni relative alla conservazione degli estremi identificativi degli amministratori di sistema e alla verifica delle attività da questi svolte possano essere rimesse al responsabile del trattamento, all'atto della sua designazione da parte del titolare o anche tramite opportune clausole contrattuali;

RITENUTA, altresì, la necessità di prorogare i termini previsti per l'adempimento delle prescrizioni, 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 del Provvedimento, come modificato e integrato dal presente provvedimento, entro il 15 dicembre 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 apportare in premessa del Provvedimento le seguenti modifiche:

1. al punto 4.3, primo capoverso, le parole "nel documento programmatico sulla sicurezza, oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque" sono eliminate;

2. al punto 4.3, terzo capoverso, la parola "deve" è sostituita dalle parole "o il responsabile del trattamento devono";

3. al punto 4.4, primo capoverso, dopo la parola "titolari" sono aggiunte le parole "o dei responsabili";

b) di apportare al punto 2 del Provvedimento le seguenti modifiche:

1. alla lettera c), primo capoverso, le parole "nel documento programmatico sulla sicurezza oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque" sono eliminate; al secondo capoverso, alla fine del penultimo periodo dopo la parentesi, sono aggiunte le parole "o tramite procedure formalizzate a istanza del lavoratore".

2. alla lettera d), le parole "il titolare deve" sono sostituite con "il titolare o il responsabile esterno devono";

3. alla lettera e), dopo le parole "titolari del trattamento" sono inserite le parole "o dei responsabili";

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

c) di prorogare al 15 dicembre 2009 i termini per l'adempimento delle prescrizioni di cui al punto 2 del Provvedimento, come modificate e integrate dal punto b) del presente provvedimento;

d) 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, 25 giugno 2009

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Patroni Griffi

Allegato IV

Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali - 27 novembre 2008

(G.U. n. 287 del 9 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. lgs
. 30 giugno 2003, n. 196) e, in particolare gli articoli 33 ss., nonché il relativo Allegato B) contenente il disciplinare tecnico in materia di misure minime di sicurezza;

VISTO l'art. 29 del decreto-legge 25 giugno 2008, n. 112, come modificato dalla legge di conversione 6 agosto 2008, n. 133, con il quale è stato, fra l'altro, modificato l'art. 34 del Codice;

RITENUTA l'esigenza di individuare alcune modalità semplificate di applicazione del predetto disciplinare tecnico da parte dei "soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale", nonché rispetto a "trattamenti comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani", nel rispetto dei diritti degli interessati (comma 1-bis art. 34 cit.);

RILEVATA l'ulteriore esigenza che di tali modalità semplificate, da aggiornare periodicamente, sia data la più ampia pubblicità anche attraverso il sito Internet dell'Autorità
(http://www.garanteprivacy.it);

VISTO il parere del Ministro per la semplificazione normativa formulato con nota del 21 novembre 2008, sullo schema preliminare del presente provvedimento trasmesso con nota del 3 novembre 2008;

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

Il presente provvedimento individua modalità semplificate di applicazione delle misure minime di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali, di seguito indicato come Allegato B).

La disciplina sulle misure minime di sicurezza

I soggetti che trattano dati personali sono tenuti a proteggerli attraverso adeguate misure di sicurezza.
Alcune di esse sono individuate puntualmente dal Codice e delineano il livello minimo di protezione dei dati: si tratta delle misure indicate dagli articoli 33 ss. del Codice, da adottare nei modi previsti dall'Allegato B).
Di recente sono state introdotte con disposizione di legge alcune semplificazioni relative ai trattamenti effettuati con strumenti elettronici da parte dei soggetti che utilizzano soltanto dati personali non sensibili e che trattano, come unici dati sensibili, quelli inerenti allo stato di salute o alla malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero all'adesione a organizzazioni sindacali o a carattere sindacale.
Per questi casi, la tenuta di un aggiornato documento programmatico sulla sicurezza (art. 34, comma 1, lett. g) del Codice) è stata sostituita da un obbligo di autocertificazione (resa dal titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445) di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte (art. 29 d.l. 25

giugno 2008, n. 112, come modificato dalla legge di conversione 6 agosto 2008, n. 133).
In relazione ai trattamenti sopra menzionati, nonché a quelli effettuati da chiunque per correnti finalità amministrative e contabili in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante deve individuare modalità semplificate di applicazione dell'Allegato B) sentito il Ministro per la semplificazione normativa.
Tale individuazione avviene mediante il presente provvedimento, che sarà aggiornato con cadenza periodica.

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 CIO' 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 coerente con i princìpi 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.

Le Collane

MASSIMARIO

diretta da Luigi Viola

Autovelox
I maltrattamenti in famiglia
Decreto ingiuntivo
Violazione degli obblighi di assistenza familiare
Condominio

FORMAZIONE

diretta da Luigi Viola

La contabilità degli studi professionali
L'affido condiviso
Provvedimenti cautelari d'urgenza
La testimonianza scritta
Le opposizioni nella procedura esecutiva
Mediazione e conciliazione
Pubblico spettacolo: disciplina delle opere

INFORMATICA GIURIDICA

diretta da Michele Iaselli

Il Commercio Elettronico
Misure minime di sicurezza
La ricerca dei documenti giuridici
Privacy e marketing diretto
I nuovi reati informatici
Diritto d'autore e siti web
La PEC - Posta Elettronica Certificata
La prova digitale nel processo penale
Privacy e nuove tecnologie
Diritto e web 2.0
Consapevolezza fa rima con riservatezza
I nuovi contratti informatici
L'amministratore di sistema

DIRITTO DELLO SPORT

diretta da Gabriele Nicolella

Lavoro sportivo professionistico
Ordinamento e giustizia dello sport
Diritto penale sportivo
La previdenza sportiva
Giustizia sportiva nazionale e internazionale
Trasferimenti internazionali e normativa Fifa

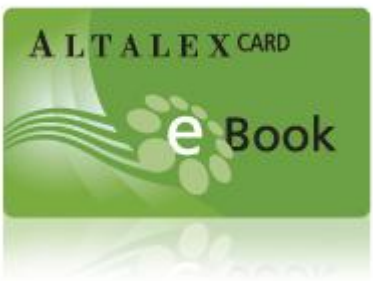
CRIMINA

diretta da Simone Marani

Guida in stato di ebbrezza
Detenzione di stupefacenti: spaccio e uso personale
Il reato di stalking
I rimedi revocatori del giudicato penale
Il reato di violenza sessuale
Il reato di immigrazione clandestina
Stupefacenti: l'attenuante della lieve entità
Il processo penale minorile
Il reato circostanziato
La legittima difesa
Il delitto di furto
Pedopornografia
Il delitto di usura

CODICI IN BORSA

Codice delle assicurazioni private
Codice della strada
Codice civile
Codice commentato del processo civile



Altalex Card è la soluzione ideale per l'acquisto degli eBooks! Scopri tutti i vantaggi esclusivi su www.altalexebook.it.