PROVVEDIMENTO 27 novembre 2008
Semplificazione delle misure minime 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 9.12.2008)

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 (decreto legislativo 30 giugno 2003, n. 196) e, in particolare gli articoli 33 ss., nonche' 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 e' stato, fra l'altro, modificato l'art. 34 del codice;
Ritenuta l'esigenza di individuare alcune modalita' 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», nonche' rispetto a «trattamenti comunque effettuati per correnti finalita' 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 modalita' semplificate, da aggiornare periodicamente, sia data la piu' ampia pubblicita' anche attraverso il sito Internet dell'Autorita' (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 modalita' 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) e' stata sostituita da un obbligo di autocertificazione (resa dal titolare del trattamento ai sensi dell'art. 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, nonche' a quelli effettuati da chiunque per correnti finalita' amministrative e contabili in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante deve individuare modalita' semplificate di applicazione dell'allegato B) sentito il Ministro per la semplificazione normativa.
Tale individuazione avviene mediante il presente provvedimento, che sara' aggiornato con cadenza periodica.
Semplificazione per taluni trattamenti
Come il Garante ha gia' evidenziato nel provvedimento del 19 giugno 2008 (in Gazzetta Ufficiale 1° luglio 2008, n.152 e in http://www.garanteprivacy.it/, doc. web n. 1526724), nonche' 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, comma1â€'bis, del codice, come introdotto dall'art.29 cit.).
Sono state pertanto individuate alcune nuove modalita' volte a semplificare incisivamente l'applicazione di varie regole contenute nell'allegato B).
L'obiettivo e' garantire egualmente un idoneo livello di sicurezza tenendo conto delle ridotte dimensioni di alcune realta' organizzative, nonche' della particolare natura di alcuni trattamenti a fini esclusivamente amministrativo-contabili. Cio', 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 Autorita', in particolare attraverso quesiti e segnalazioni.
Le modalita' 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 modalita' 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 nella Gazzetta Ufficiale della Repubblica italiana.
Roma, 27 novembre 2008

Il presidente
Pizzetti

Il relatore
Pizzetti

Il segretario generale
Buttarelli

Allegato A)

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

1. Soggetti che possono avvalersi della semplificazione.
Le seguenti modalita' 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 finalita' 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 modalita' semplificate di seguito individuate.
2.1. Istruzioni agli incaricati del trattamento (modalita' 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 (modalita' applicative delle regole di cui ai punti 1, 2, 3, 5, 6, 7, 8, 10 e 11 dell'allegatoB))
Per l'accesso ai sistemi informatici si puo' 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 piu' la qualita' che rende legittimo l'utilizzo dei dati (ad esempio, in quanto non opera piu' all'interno dell'organizzazione).
Puo' 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 necessita' di operativita' e di sicurezza del sistema, se l'accesso

ai dati e agli strumenti elettronici e' consentito esclusivamente mediante uso della password, il titolare puo' assicurare la disponibilita' di dati o strumenti elettronici con procedure o modalita' predefinite. Riguardo a tali modalita', 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 modalita' 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 (modalita' 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, cosi' da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

2.4. Altre misure di sicurezza (modalita' 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, nonche' agli addetti alla gestione o alla manutenzione degli strumenti elettronici, sia coerente con i principi di adeguatezza, proporzionalita' e necessita', anche attraverso verifiche periodiche, provvedendo, quando e' necessario, ad aggiornare i profili di autorizzazione eventualmente accordati.

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilita' di strumenti elettronici (ad esempio, antivirus), anche con riferimento ai programmi di cui all'art. 615-quinquies del codice penale, nonche' a correggerne difetti, sono effettuati almeno annualmente. Se il computer non e' 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 puo' non riguardare i dati non modificati dal momento dell'ultimo salvataggio effettuato (dati statici), purche' ne esista una copia di sicurezza da cui effettuare eventualmente il ripristino.

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

2.5.1. Fermo restando che per alcuni casi e' gia' 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 finalita' 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 31marzo 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, nonche', se designati, gli eventuali responsabili. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalita' attraverso le quali e' 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 finalita' del trattamento, le categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime, nonche' 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 responsabilita'. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalita' attraverso le quali e' possibile individuare l'elenco aggiornato dei responsabili del trattamento con le relative responsabilita';
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 finalita' della raccolta.
3. Modalita' applicative per i trattamenti realizzati senza l'ausilio di strumenti elettronici (modalita' 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 modalita' 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.