D.P.R. 28-07-1999, n. 318 - Privacy misure minime di sicurezza

Indice, Preambolo, Art.1, Art.2, Art.3, Art.4, Art.5, Art.6, Art.7, Art.8, Art.9, Art.10, ALLEGATO A, ALLEGATO B,

Indice

Preambolo

IL PRESIDENTE DELLA REPUBBLICA
Visto l'articolo 87, comma quinto, della Costituzione;
Visto l'articolo 15 della legge 31 dicembre 1996, n. 675, recante "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali";
Ritenuto che ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675, occorre individuare, in via preventiva, le misure minime di sicurezza per i dati personali oggetto di trattamento, al fine di assicurare il funzionamento delle misure sanzionatorie penali previste dall'articolo 36 della medesima legge;
Visto l'articolo 17, comma 1, lettera a), della legge 23 agosto 1988, n. 400;
Sentiti l'Autorità per l'informatica nella pubblica amministrazione e il Garante per la protezione dei dati personali;
Udito il parere del Consiglio di Stato, espresso dalla sezione consultiva per gli atti normativi nell'adunanza del 26 aprile 1999;
Ritenuto di dover comunque garantire la possibilità, in caso di più incaricati del trattamento, di limitare l'accesso a determinati dati personali attraverso la previsione di una specifica parola chiave per tali dati, senza operare, quindi, alcuna equiparazione tra tale ipotesi e quella relativa alla previsione di un'unica parola chiave per l'accesso al sistema;

Viste le deliberazioni del Consiglio dei Ministri, adottate nelle riunioni del 16 luglio e del 23 luglio 1999;
Sulla proposta del Ministro di grazia e giustizia;
Emana
il seguente regolamento:

Capo I
PRINCIPI GENERALI

Articolo 1

Definizioni

1. Ai fini del presente regolamento si applicano le definizioni elencate nell'articolo 1 della legge 31 dicembre 1996, n. 675, di seguito denominata legge. Ai medesimi fini si intendono per:
a) "misure minime": il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste nel presente regolamento, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'articolo 15, comma 1, della legge;
b) "strumenti": i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento;
c) "amministratori di sistema": i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

Capo II
TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI - O COMUNQUE AUTOMATIZZATI.
Sezione I
Trattamento dei dati personali effettuato mediante elaboratori non accessibili da altri elaboratori o terminali.

Articolo 2

Individuazione degli incaricati

1. Salvo quanto previsto dall'art.8, se il trattamento dei dati personali è effettuato per fini diversi da quelli di cui all'articolo 3 della legge mediante elaboratori non accessibili da altri elaboratori o terminali, devono essere adottate, anteriormente all'inizio del trattamento, le seguenti misure:
a) prevedere una parola chiave per l'accesso ai dati, fornirla agli incaricati del trattamento e, ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore, consentirne l'autonoma sostituzione, previa comunicazione ai soggetti preposti ai sensi della lettera b);
b) individuare per iscritto, quando vi è più di un incaricato del trattamento e sono in uso più parole chiave, i soggetti preposti alla loro custodia o che hanno accesso ad informazioni che concernono le medesime.

Sezione II
Trattamento dei dati personali effettuato mediante elaboratori - accessibili in rete

Articolo 3

Classificazione

1. Ai fini della presente sezione gli elaboratori accessibili in rete impiegati nel trattamento dei dati personali sono distinti in:
a) elaboratori accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico;
b) elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico.

Articolo 4

Codici identificativi e protezione degli elaboratori

1. Nel caso di trattamenti effettuati con gli elaboratori di cui all'articolo 3, oltre a quanto previsto dall'articolo 2 devono essere adottate le seguenti misure:
a) a ciascun utente o incaricato del trattamento deve essere attribuito un codice identificativo personale per l'utilizzazione dell'elaboratore; uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non può, neppure in tempi diversi, essere assegnato a persone diverse;
b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi;
c) gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale.

2. Le disposizioni di cui al comma 1, lettere a) e b), non si applicano ai trattamenti dei dati personali di cui è consentita la diffusione.

Articolo 5

Accesso ai dati particolari

1. Per il trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato ai sensi dell'articolo 3, l'accesso per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione. Se il trattamento è effettuato ai sensi dell'articolo 3, comma 1, lettera b), sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico.

2. L'autorizzazione, se riferita agli strumenti, deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento.

3. Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione.

4. L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.

5. La validità delle richieste di accesso ai dati personali è verificata prima di consentire l'accesso stesso.

6. Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

7. Le disposizioni di cui ai commi da 1 a 6 non si applicano al trattamento dei dati personali di cui è consentita la diffusione.

Articolo 6

Documento programmatico sulla sicurezza

1. Nel caso di trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato mediante gli elaboratori indicati nell'articolo 3, comma 1, lettera b), deve essere predisposto e aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

stessi:
a) i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
b) i criteri e le procedure per assicurare l'integrità dei dati;
c) i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;
d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.

2. L'efficacia delle misure di sicurezza adottate ai sensi del comma 1 deve essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale.

Articolo 7

Reimpiego dei supporti di memorizzazione

1. Nel caso di trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato con gli strumenti di cui all'articolo 3, i supporti già utilizzati per il trattamento possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.

Sezione III
Trattamento dei dati personali effettuato - per fini esclusivamente personali

Articolo 8

Parola chiave

1. Ai sensi dell'articolo 3 della legge, il trattamento per fini esclusivamente personali dei dati di cui agli articoli 22 e 24 della legge, effettuato con elaboratori stabilmente accessibili da altri elaboratori, è soggetto solo all'obbligo di proteggere l'accesso ai dati o al sistema mediante l'utilizzo di una parola chiave, qualora i dati siano organizzati in banche di dati.

Capo III
TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI.

Articolo 9

Trattamento di dati personali

1. Nel caso di trattamento di dati personali per fini diversi da quelli dell'articolo 3 della legge, effettuato con strumenti diversi da quelli previsti dal capo II, sono osservate le seguenti modalità:
a) nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni ai sensi degli articoli 8, comma 5, e 19 della legge, il titolare o, se designato, il responsabile devono prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
b) gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate.

2. Nel caso di trattamento di dati di cui agli articoli 22 e 24 della legge, oltre a quanto previsto nel comma 1, devono essere osservate le seguenti modalità:
a) se affidati agli incaricati del trattamento, gli atti e i documenti contenenti i dati sono conservati, fino alla restituzione, in contenitori muniti di serratura;
b) l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.

Articolo 10

Conservazione della documentazione relativa al trattamento

1. I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali di cui agli articoli 22 e 24 della legge devono essere conservati e custoditi con le modalità di cui all'articolo 9. Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

ALLEGATO A

Computer a prova di privacy(Garante 29.2.2000)Entro il prossimo 29 marzo tutte le pubbliche amministrazioni, e i privati che effettuano trattamenti di dati personali dovranno adottare le "misure minime di sicurezza" previste dal Governo con il regolamento 318 del 1999. Si tratta di una serie di disposizioni che vanno dall'uso delle password da parte del personale incaricato di accedere agli archivi dei dati alle modalità stesse di archiviazione. La necessità di rispettare i termini per adeguarsi alle norme è ribadita in una raccomandazione del Garante per la privacy del 29 febbraio. Nel testo l'Authority ricorda che sono previsti una serie di adempimenti da attuare per poter trattare i dati. Il regolamento prevede, tra l'altro, per trattamenti informatizzati, l'identificazione dell'utente, l'autorizzazione all'accesso alle funzioni, la registrazione degli ingressi e l'inserimento di una password che inibisca l'accesso al sistema o ai dati contenuti negli elaboratori stabilmente accessibili da altri computer. Il regolamento prevede inoltre l'individuazione di figure nuove come quella dell'amministratore di sistema che sovrintende alla gestione della base dati. Il Garante ricorda inoltre che quelle indicate sono "misure minime" destinate a valere in generale, mentre per quel che riguarda i dati "sensibili" in aggiunta a queste debbono essere previste altre cautele: in particolare se affidati agli incaricati, gli atti e i documenti concernenti i dati siano conservati, sino alla restituzione, in contenitori muniti di serratura, mentre l'accesso agli archivi deve essere controllato e vanno identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi. (3 marzo 2000)IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALINELLA riunione odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti e del dott. Giovanni Buttarelli, segretario generale;VISTO il d.P.R. 28 luglio 1999, n. 318, recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali a norma dell'art. 15, comma 2, della legge 31 dicembre 1996, n. 675;RITENUTA la necessità di richiamare l'attenzione dei soggetti tenuti all'applicazione di tali misure sulle prescrizioni contenute nel medesimo d.P.R. e sulla prossima scadenza del 29 marzo 2000;VISTA la documentazione in atti;VISTE le osservazioni in atti formulate dall'Ufficio ai sensi dell'art. 7, comma 2, lett. a), del d.P.R. n. 501/1998, con nota a firma del Segretario generale; RELATORE l'Ing. Claudio Manganelli;PREMESSO:La legge 31 dicembre 1996, n. 675 nell'introdurre una complessa disciplina a tutela del trattamento dei dati personali, ha focalizzato la sua attenzione anche sugli aspetti relativi alla sicurezza nel trattamento dei dati.Tale esigenza ha trovato attuazione nella Sezione III del Capo III della legge n. 675/1996, significativamente intitolata "Sicurezza nel trattamento dei dati, limiti alla utilizzabilità dei dati e risarcimento del danno".In detta sezione, all'articolo 15, comma 1, si afferma che "i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".Nello stesso articolo, al comma 2, viene stabilito che le misure minime di sicurezza da adottare in via preventiva sono individuate con regolamento emanato con decreto del Presidente della Repubblica e che esse sono adeguate successivamente, con cadenza almeno biennale," in relazione all'evoluzione tecnica del settore e all'esperienza maturata". Inoltre, all'articolo 18, si prevede che "chiunque cagioni danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento del danno ai sensi dell'articolo 2050 del codice civile".L'intervenuta emanazione del citato regolamento (D.P.R. n. 318/1999), che va ad aggiungersi alle norme di legge sopra richiamate, ha gettato le basi per una più

articolata disciplina della sicurezza specie nell'informatica e nella telematica, la cui importanza emerge anche dalla circostanza che le disposizioni dell'articolo 15 si applicano anche ai trattamenti pubblici in materia di polizia, giustizia, difesa e sicurezza dello Stato ai quali la legge n. 675 si applica solo in parte (art. 4 legge n. 675).Un richiamo a quanto disposto dall'art. 15, commi 2 e 3, è poi esplicitamente contenuto nll'art. 17, comma 4, del d. lg. n. 135/1999, recante "Disposizioni integrative della legge 31 dicembre 1996 n. 675, sul trattamento dei dati sensibili da parte dei soggetti pubblici".Ponendo attenzione al complessivo impianto normativo emerge con evidenza la finalità di ridurre al minimo i predetti rischi, mediante l'utilizzazione di sistemi di sicurezza costantemente adeguati nel tempo.Il tipo di tutela che viene assicurato si sviluppa in due diversi aspetti: da un lato l'articolo 18 della legge n. 675/1996 prevede che chiunque (compresi il titolare, il responsabile (se designato) e gli incaricati) debbano risarcire gli eventuali danni ai sensi dell'articolo 2050 del codice civile. Dall'altro, la legge prevede l'individuazione di misure minime di sicurezza la cui mancata adozione comporta anche l'irrogazione di una sanzione penale. L' art. 36 della legge prevede infatti che la responsabilità sussista qualora non siano rispettati, anche in parte, gli standard "minimi" di sicurezza prescritti dal regolamento.Si è, quindi, in presenza di una diversità sostanziale nella disciplina delle misure di sicurezza, indicata dallo stesso articolo 15 della legge n. 675/1996. Da un lato quelle previste al comma 1, destinate ad operare una costante riduzione del rischio, non individuate, ma individuabili sulla base di soluzioni tecniche concretamente disponibili (la cui mancata predisposizione comporta responsabilità civile in caso di danno). Dall'altro, le misure "minime" previste al comma 2, specificamente individuate all'interno di un ulteriore atto (il regolamento), che contiene i vari precetti della norma contenuta nell'articolo 36, la cui violazione, come si è detto, comporta una sanzione di carattere penale.Pertanto, il regolamento non è destinato a contenere tutte le regole tecniche da adottare in ogni caso per la sicurezza dei dati personali, in riferimento alle diverse modalità di trattamento utilizzate, e individua unicamente quei requisiti minimi il cui mancato rispetto comporta una maggiore esposizione a rischio del bene giuridico che la norma vuole tutelare.Tale strumento è stato impostato in chiave di flessibilità, essendo destinato ad un aggiornamento avente cadenza biennale, all'evidente fine di evitare una sua oggettiva "staticità" a fronte di un evoluzione tecnologica per sua natura "dinamica". Il regolamento non intende quindi individuare le "migliori" misure evidenziate dalla scienza tecnica in un dato momento, mirando più semplicemente ad enucleare un minimo denominatore comune delle misure di sicurezza disponibili, tale da poter definire le stesse come "minime".In ciò può essere pertanto meglio compresa la diversità esistente tra l'obbligo di "massima" riduzione del rischio previsto dal comma 1 (che impone un costante aggiornamento verso la migliore tecnica) e la diversa previsione di misure "minime" comuni a varie metodologie di trattamento dei dati (misure che sono anzitutto la condizione necessaria per l'applicazione dello strumento sanzionatorio avente natura penale).In coerenza con la legge da cui promana, il regolamento previsto dalla legge n. 675 si rivolge a tutti i soggetti - pubblici e privati - che nell'ambito delle loro attività pongono in essere un trattamento di dati personali.Il Governo ha ritenuto pertanto necessario individuare categorie omogenee di modalità di trattamento di dati, al fine di correlare la soglia minima di sicurezza da un lato alla tipologia dei dati e, dall'altro, allo strumento tecnico utilizzato per l'elaborazione. Si è ritenuto peraltro di non poter prescindere dalla distinzione già operata dalla norma generale tra dati "comuni" e "sensibili" dovendosi tenere in debito conto la diversa valenza di questi ultimi nel quadro di una differente intensità del grado di tutela per essi previsto.Una prima grande distinzione operata dal regolamento ha avuto riguardo alle modalità delle operazioni svolte per effettuare il trattamento: da una parte quelle effettuate in sostanza con l'ausilio di supporti cartacei, dall'altra quelle poste in essere anche in parte mediante strumenti elettronici o comunque automatizzati.Tale ultima modalità è stata a sua volta distinta in ulteriori tre categorie:a) trattamenti di dati personali mediante elaboratori non accessibili da altri elaboratori o terminali (art. 2 D.P.R. n. 318/1999);b) trattamenti di dati personali effettuati mediante elaboratori accessibili in rete (artt. 3 e 7 D.P.R. n. 318/1999), categoria a sua volta distinta in:- elaboratori accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico (art. 3, comma 1, lett. a), D.P.R. n. 318/1999);- elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico (art. 3, comma 1, lett. b), D.P.R. n. 318/1999);c) trattamenti di dati personali effettuati per fini esclusivamente personali (ai sensi dell'articolo 3 della legge 675/1996) mediante elaboratori stabilmente accessibili da altri elaboratori.Poiché l'ottica con cui sono state previste le singole misure di sicurezza è collegata non solo alla protezione dei sistemi o delle trasmissioni in quanto tali, ma, più direttamente nella protezione dei dati personali, il livello di sicurezza si modifica di conseguenza in relazione alla presenza o meno dei dati stessi. Così pure, nel caso siano contestualmente presenti dati "comuni" e "sensibili", è necessario osservare le misure previste per la categoria più elevata..Va evidenziato inoltre come nel regolamento il Governo abbia preferito non individuare per ogni singola misura di sicurezza i soggetti tenuti ad adottarla. Tale individuazione dipende quindi dalle attribuzioni del titolare del trattamento e dai ruoli e degli incarichi conferiti in concreto all'interno della relativa struttura.Quanto alle definizioni, il regolamento, oltre ad utilizzare quelle già contenute nella legge 675, prevede all'art. 1 quelle di:· "misure minime" intendendo per esse il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi a cui fa riferimento l'articolo 15, comma 1, della legge (misure che possono ad esempio comportare, nei casi previsti nei successivi articoli: l'identificazione dell'utente, l'autorizzazione all'accesso alle funzioni, ai servizi, ai locali, ai dati e la registrazione degli ingressi, nonché limiti al riutilizzo di supporti per l'archiviazione elettronica o automatizzata o cartacea);· "strumenti", intendendo per essi i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento;·

"amministratori di sistema", riferendosi ai soggetti cui è conferito il compito di sovraintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.Quanto agli effetti che il regolamento spiega sui trattamenti effettuati a fini esclusivamente personali, l'articolo 3 della legge li eccettua, anzitutto, dall'osservanza di diversi obblighi normativi fissati dalla medesima legge, a condizione che i "dati non siano destinati ad una comunicazione sistematica o alla diffusione". Nella seconda parte, però, la citata disposizione limita la portata di detta statuizione, disponendo che sono comunque applicabili gli articoli 15, comma 1, 18 e 36 della legge stessa, anche per ciò che riguarda, quindi, le misure minime di sicurezza.Le peculiari caratteristiche ed i limiti di questo particolare tipo di trattamento, che la stessa norma generale considera come categoria a sé stante, hanno però reso opportuno prevedere misure di sicurezza che tenessero conto in misura adeguata il minore rischio insito in tale attività.Considerato poi che anche alcune osservazioni formulate nella fase di predisposizione del regolamento sia dal Consiglio di Stato, sia dal Garante andavano nella direzione di limitare per quanto possibile l'ambito di applicazione della norma penale in materia di sicurezza, con l'intuibile intento di evitare un'applicazione irragionevole delle sanzioni, il Governo ha previsto la sua applicazione soltanto ai trattamenti effettuati mediante elaboratori accessibili da altri elaboratori, escludendo in tal modo vari computer e, in particolare quelli "stand alone". Per quelli caratterizzati invece dalla predetta accessibilità la misura minima di sicurezza è stata individuata nel solo obbligo per il soggetto titolare di utilizzare una parola chiave che inibisca l'accesso al sistema o anche solamente ai dati.L'ultima parte del regolamento è dedicata al trattamento di dati effettuato mediante strumenti diversi da quelli elettronici o comunque automatizzati (artt. 9 e 10). Si tratta di situazioni diffuse in cui la tenuta di dati è operata per mezzo di supporti cartacei come avviene, ad esempio, presso gli archivi (sia di privati, sia di pubbliche amministrazioni).Anche in questo caso, nell'individuare le misure minime di sicurezza, il D.P.R. fa riferimento a cautele spesso già adottate di fatto. In proposito, sebbene la tenuta di archivi e l'individuazione dei soggetti che possono prendere conoscenza delle informazioni sia già disciplinata per alcuni uffici pubblici, il regolamento non ha portato ad estendere necessariamente quel tipo di misure, peraltro tipiche degli attuali modelli organizzativi del lavoro delle istituzioni pubbliche, anche ai privati.E' stato previsto piuttosto che debbano essere osservate le seguenti modalità:q nel designare per iscritto gli incaricati del trattamento e nell'impartire le istruzioni, il titolare o, se designato, il responsabile devono prescrivere che i soggetti designati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati (art. 9, comma 1, lett. a);q gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni eseguite (art. 9, comma 1, lett. b)).Nel caso invece l'attività riguardi dati di tipo "sensibile" o di natura giudiziaria, in aggiunta alle misure sopra descritte occorre prevedere che:se affidati agli incaricati, gli atti e i documenti concernenti i dati siano conservati, sino alla restituzione, in contenitori muniti di serratura;l'accesso agli archivi sia controllato e siano identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.Con queste modalità devono essere conservati anche i supporti cartacei contenenti la riproduzione di informazioni relative al trattamento dei dati di cui all'art. 22 e all'art. 24 della legge.Con riferimento all'obbligo di predisporre le misure minime di sicurezza anteriormente all'inizio del trattamento, appare quindi opportuno richiamare l'attenzione degli operatori sulla circostanza che l'articolo 41, comma 3, della legge 675 prevede, per l'effettiva e concreta adozione delle misure stesse, un termine di sei mesi decorrente dalla data di entrata in vigore del regolamento (29 settembre 1999) e che è pertanto fissato al 29 marzo 2000.CIO' PREMESSO, IL GARANTE:richiama l'attenzione di tutti i soggetti pubblici e privati tenuti al rispetto del d.P.R. n. 318/1999 sulle prescrizioni in esso contenute e sulle connesse sanzioni, nonché sulla prevista scadenza del 29 marzo 2000 prevista per l'applicazione delle misure minime di sicurezza.

ALLEGATO B

Applicazione delle misure minime di sicurezza di cui al decreto del Presidente della Repubblica n. 318/1999. Modifica da apportare al modello per la notificazione del trattamento dei dati personali. (Deliberazione n. 8)
(G.U. n. 65, 18 marzo 2000, Serie Generale)
IL GARANTE PER LA PROTEZIONE
DEI DATI PERSONALI
Nella riunione odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice-presidente, del prof. Ugo De Siervo, dell'ing. Claudio Manganelli, componenti e del dott. Giovanni Buttarelli, segretario generale;
Premesso che:
l'art. 7 della legge 31 dicembre 1996, n. 675, prevede per i titolari che intendano procedere ad un trattamento di dati l'obbligo di darne notificazione al Garante e, in caso di successive modifiche apportate per i profili indicati nel medesimo articolo, di comunicarle attraverso una successiva notificazione;
l'art. 12, commi 1 e 3, del decreto del Presidente della Repubblica 31 marzo 1998, n. 501, stabilisce che le notificazioni sono effettuate utilizzando modelli conformi allo schema predisposto dal Garante;
detti modelli sono stati predisposti e resi disponibili al pubblico, in particolare attraverso convenzioni con

Poste italiane S.p.a. ed altri soggetti ed organismi interessati;
l'art. 15, commi 2 e 3, della legge n. 675/1996 stabilisce che con regolamento devono essere individuate le misure minime di sicurezza relative ai dati personali oggetto di trattamento;
il regolamento è stato emanato con decreto del Presidente della Repubblica n. 318 del 28 luglio 1999;
ai sensi dell'art. 41, comma 3, della legge n. 675/1996 il termine per l'adozione delle misure minime di sicurezza previste da tale decreto del Presidente della Repubblica è fissato al 29 marzo 2000;
Considerato che:
il modello di notificazione sarà aggiornato e perfezionato nel suo complesso entro la fine del corrente anno, in base all'esperienza acquisita e tenendo conto delle novità intercorse;
l'applicazione del decreto del Presidente della Repubblica n. 318/1999 potrebbe indurre numerosi titolari dei trattamenti a modificare la precedente notificazione ai sensi dell'art. 7, commi 2 e 4, della citata legge, relativamente al riquadro d) del modello adottato dal Garante ai sensi del richiamato art. 12 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;
si potrebbe così determinare l'afflusso al Garante di un enorme numero di notificazioni non necessarie in quanto non è indispensabile annotare nel registro generale dei trattamenti, in questa fase transitoria, modifiche di notificazioni già effettuate derivanti dall'adempimento di un obbligo di legge;
Viste le osservazioni in atti formulate dall'Ufficio ai sensi dell'art. 7, comma 2, lettera a), del decreto del Presidente della Repubblica n. 501/1998, con nota a firma del segretario generale;
Relatore il prof. Ugo De Siervo;
Delibera:
[Articolo unico]
a) Di inserire nel riquadro d) ("descrizione generale delle misure adottate per la sicurezza dei dati") dei modelli di notificazione al Garante del trattamento dei dati personali l'avvertenza che figura in allegato alla presente deliberazione;
b) di dare atto che i soggetti che hanno notificato i trattamenti dei dati personali prima del 29 marzo 2000 non devono presentare una nuova notificazione di modifica in relazione al medesimo riquadro d) qualora abbiano adottato le misure previste dal decreto del Presidente della Repubblica n. 318 del 28 luglio 1999;
c) di consentire ai titolari dei trattamenti, in riferimento a nuove notificazioni, di continuare ad utilizzare i modelli precedentemente approvati dal Garante.
Allegato
Nel riquadro d) (descrizione generale delle misure adottate per la sicurezza dei dati), è inserita la seguente avvertenza:
i soggetti che hanno notificato il trattamento dei dati personali prima del 29 marzo 2000 non devono effettuare una nuova notificazione per modificare il presente riquadro, qualora abbiano adottato le misure minime previste dal decreto del Presidente della Repubblica n. 318 del 28 luglio 1999 ("Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'art. 15, comma 2, della legge 31 dicembre 1996, n. 675").