

DOCUMENTO PROGRAMMATICO SICUREZZA dlg 196-2003

Versione: **1.0.1**
Aggiornato al: **25/11/2004**

A cura di: Ing. Sommaruga Andrea
Scritto con: OpenOffice 1.1.3

INDICE GENERALE

DLG 196/2003 IN BREVE.....	2
LE SCADENZE.....	2
PROROGA.....	2
COSA SI INTENDE PER DATO PERSONALE.....	3
CHI DEVE ADEGUARSI.....	3
GLI ADEMPIMENTI.....	3
I PASSI DA SEGUIRE.....	4
SANZIONI.....	4
GLOSSARIO.....	5
DPS.....	6
COSA E' IL DPS.....	6
SCOPO DEL DPS.....	6

DLG 196/2003 IN BREVE

Il testo unico privacy DLG 196/2003 che sostituisce la legge n. 675/1996, innova la normativa precedente, in vigore oramai da diversi anni, adeguandola ai mutamenti tecnologici avvenuti ed all'esperienza acquisita.

E' assolutamente obbligatorio essere in regola. Si rischiano sanzioni molte dure: multe fino a 120.000 Euro, reclusione fino a 3 anni, (risarcimento del danno patrimoniale e morale ex art. 2050).

LE SCADENZE

Attualmente il termine ultimo per adeguarsi è fissato per aziende, professionisti entro il 31/12/04, salvo le vecchie misure di sicurezza che devono essere già in essere. Anche per il DPS il termine è il 31/12/04 ma alla data di stesura di queste note si parla di un possibile ulteriore rinvio..

per le Pubbliche amministrazioni

- 31 DICEMBRE 2004, invece del 30 giugno 2004 (anche per la redazione del DPS)
- 31 MARZO 2005, invece del 31 dicembre 2004, per i casi in cui, alla data del 31 dicembre 2003, il titolare fosse stato in possesso di strumenti elettronici tecnicamente inadeguati;
- entro il 31/12/05 anziché 30/09/04 deve essere effettuata l'identificazione con atto di natura regolamentare dei tipi di dati e di operazioni ai sensi degli articoli 20, commi 2 e 3, e 21, comma 2 (dati sensibili e giudiziari).

PROROGA

Decreto legge n. 266 del 9 novembre 2004
pubblicato sulla G.U. n. 264 del 10 novembre 2004, recante
«Proroga o differimento di termini previsti da disposizioni legislative»

... omissis..

ART. 6

Trattamento dati personali

1. All'articolo 180, comma 1, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modifiche:
 - a) al comma 1 le parole: «31 dicembre 2004» sono sostituite dalle seguenti: «30 giugno 2005»;
 - b) al comma 3 le parole: «31 marzo 2005» sono sostituite dalle seguenti: «30 settembre 2005».

Le nuove scadenze:

Slitta il termine per l'adozione delle misure minime di sicurezza che non erano previste dal dpr n. 318/1999. Si tratta delle misure minime «nuove» introdotte dall'allegato B) al codice della privacy (dlgs n. 196/2003).

L'adempimento previsto dall'articolo 180, comma 1, del codice della privacy passa dal 31 dicembre 2004 al **30 giugno 2005**. Si tratta della seconda proroga: il testo iniziale del codice prevedeva addirittura la data del 30 giugno 2004.

Risulta prorogata anche la scadenza per la stesura del Documento programmatico sulla

DOCUMENTO PROGRAMMATICO SICUREZZA dlq 196-2003

Versione: **1.0.1**
Aggiornato al: **25/11/2004**

A cura di: Ing. Sommaruga Andrea
Scritto con: OpenOffice 1.1.3

sicurezza, che lo stesso garante ha definito in un suo parere quale misura nuova. Slitta inoltre il termine per l'adeguamento per il titolare del trattamento che dispone di strumenti elettronici, che per obiettive ragioni tecniche non consentono in tutto o in parte l'immediata applicazione delle misure minime previste dall'allegato B). Per tali situazioni il termine per l'adeguamento passa dal 31 marzo 2005 al **30 settembre 2005**. Per questi casi rimane sempre l'obbligo di compilare un atto avente data certa in cui si descrivono le ragioni tecniche relative agli elaboratori, compilazione che, nel silenzio del decreto legge, si ritiene debba avvenire al più tardi entro il **30 giugno 2005**.

COSA SI INTENDE PER DATO PERSONALE

Con dato personale si intende, per la Legislazione Italiana, qualunque dato atto a riconoscere una persona fisica o Società.

- a. il nome, il cognome, l'indirizzo, il numero di telefono, il codice fiscale, la partita I.V.A., dati bancari ed in genere tutti gli altri dati fiscali.
- b. informazioni circa la composizione del nucleo familiare, la professione esercitata da un determinato soggetto, sia fisico che giuridico, il titolo di studio ed altri dati di interesse generale.
- c. Dati biometrici: fotografie, radiografie, video, registrazioni, impronte
- d. informazioni relative al profilo creditizio, alla retribuzione
- e. informazioni relative alla salute di un soggetto, alla vita sessuale, alla partecipazione ad associazioni di categoria, a partiti, trattenute sindacali, cartelle cliniche, **rilevazioni di presenze**.

CHI DEVE ADEGUARSI

Devono adeguarsi tutti coloro che trattano dati personali: aziende, professionisti, cooperative, associazioni, P.A., scuole, comuni, ospedali, enti pubblici ecc. (ovvero chiunque tratti dati personali di clienti, cittadini, dipendenti, fornitori, utenti, pazienti, colleghi, soci, associati ecc.).

GLI ADEMPIMENTI

Ovviamente gli adempimenti sono diversi a seconda delle dimensioni della struttura e della tipologia di trattamento dati.

Nel caso di società con molti dipendenti o collaboratori la fase di identificazione degli incarichi, la definizione delle responsabilità dei singoli in base ai loro ruoli e la fase di inventario delle tipologie di dati trattati sarà piuttosto impegnativa.

Nelle grosse realtà le varie figure coinvolte Titolare -> Responsabili -> Incaricati saranno figure diverse con compiti diversi e questo, in termini di stesura del DPS, implica dettagliare accuratamente le procedure per le singole figure coinvolte.

In una piccola realtà, come quella di uno studio professionale, le figure in gioco sono meno: esiste ovviamente sempre il Titolare che sarà anche il Responsabile e tutte le persone che fanno parte dello studio saranno Incaricati con lo stesso ruolo. Nel DPS quindi si tratterà di definire solo i compiti del Responsabile e della tipologia di Incaricato che è uguale per tutti. Anche la fase di descrizione dei dati trattati probabilmente sarà molto più semplice perché si tratterà di descrivere la struttura degli archivi probabilmente salvati su un solo server.

Purtroppo il DPS è obbligatorio anche per le piccole strutture.

DOCUMENTO PROGRAMMATICO SICUREZZA dlq 196-2003

Versione: **1.0.1**
Aggiornato al: **25/11/2004**

A cura di: Ing. Sommaruga Andrea
Scritto con: OpenOffice 1.1.3

Per adeguarsi alla Legislazione occorre quindi:

Nominare le figure richieste dalla Legge (con lettera), di proteggere gli elaboratori contro il rischio di intrusione e di virus

Adottare delle misure fisiche di protezione (allarmi, stabilizzatori di corrente, armadi chiusi a chiave backup ecc.)

Compilare il I DPS (documento programmatico sulla sicurezza), che descrive i tipi di dati che vengono trattati, la modalità di trattamento e le protezioni che vengono prese a tutela dei dati raccolti. Il DPS, redatto su carta e munito di data certa, è la prova dell'avvenuto adeguamento. Ovviamente poi devono essere rispettate le procedure elencate nel DPS.

OBBLIGHI PER LIBERI PROFESSIONISTI

Non dimentichiamoci che il DLG 196/2003 è una rielaborazione del precedente DPR 318/99. La maggior parte delle norme relative al Trattamento dei Dati Personali era quindi già in vigore da anni. Le scadenze imposte dal DLG 196/2003 si riferiscono quindi alle sole misure nuove.

Il documento programmatico (rientra tra le nuove misure minime di sicurezza) deve essere redatto entro il 31/03/2004 (prorogato al 30/06/04, prorogato al 31/12/2004) quindi aggiornato con scadenza annuale entro il 31 marzo di ogni anno.

Le "vecchie" misure minime devono essere già attuate.

I PASSI DA SEGUIRE

Occorre programmare un adeguamento alle attrezzature informatiche abbandonando quelle che non risultano più idonee per criteri di sicurezza o affidabilità alla gestione di dati personali.

Come secondo punto occorre un inventario degli archivi informatici contenenti dati personali (esempio programmi con gestione di anagrafiche e liste di indirizzi). Attenzione: non tutto quello che viene memorizzato sui dischi dei calcolatori è necessariamente un dato personale.

Come terzo punto è necessario un inventario di tutte le misure di sicurezza prese. Misure fisiche come: allarmi, armadi, copie di sicurezza, antivirus ecc.. Misure logiche come: password, controllo accessi. Misure organizzative come: nomina delle varie figure richieste dalla Legge, invio Informative, raccolta di Consensi.

Come ultimo punto la stesura del documento riepilogativo, il DPS.

ATTENZIONE: questa Legge interpreta la sicurezza come un fatto dinamico quindi, una volta attivate le misure minime e scritto il DPS occorre mantenersi al passo verificando periodicamente l'attualità delle misure prese, il loro funzionamento e provvedendo all'aggiornamento periodico del DPS con cadenza annuale. Solo le nomine hanno durata illimitata salvo revoca.

SANZIONI

Multe da 3.000 a 50.0000 euro (elevabile al triplo).

Reclusione fino a 3 anni.

Possibilità di estinguere il reato penale, adeguandosi alla normativa e pagando una sanzione pecuniaria.

GLOSSARIO

DATI PERSONALI: Sono tutte le informazioni relative a persona fisica (persona giuridica, ente od associazione) identificate o identificabili. Es. Nome, cognome, indirizzo, numeri telefonici, n. Patente, P. IVA.

DATI SENSIBILI: Sono i dati che devono essere maggiormente tutelati, e sono relativi a razza o etnia, ad eventuali adesioni a partiti (ritenute sindacali), organizzazioni a carattere religioso, politico, associazioni di categoria, nonché dati personali idonei a rilevare lo stato di salute (cartelle mediche) e la vita sessuale del singolo.

BANCA DATI: E' una raccolta di dati personali.

MISURE DI SICUREZZA: Si tratta di custodire i documenti approntando degli accorgimenti (armadietti chiusi a chiave, firewall, wiping, accesso selezionato ai dati...)

TRATTAMENTO DEI DATI: Consiste in qualunque operazione o insieme di operazioni, eseguite o meno grazie ad un computer, riguardanti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

TITOLARE DEL TRATTAMENTO: E' la persona fisica, (la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo) che ha la competenza a decidere in ordine alle finalità, alle modalità del trattamento di dati personali ed alla loro sicurezza.

RESPONSABILE DEL TRATTAMENTO DEI DATI: E' la persona fisica (la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo) che il titolare (che decide) prepone al trattamento di dati personali. Titolare e responsabile possono essere la stessa persona. I compiti affidati ad esso devono essere analiticamente specificati per iscritto.

INCARICATO: E' colui/coloro che elabora i dati personali sulla base delle istruzioni scritte del titolare o del responsabile

INTERESSATO: E' la persona fisica (la persona giuridica, l'ente o l'associazione) a cui si riferiscono i dati personali trattati.

PASSWORD: E' la parola chiave, una sequenza di lettere e/o numeri, che serve per accordare l'accesso al sistema informatico agli utenti.

USER ID (Username): E' un codice identificativo personale formato da lettere e/o numeri. Viene sempre abbinato alla password (segreta).

AMMINISTRATORE DI SISTEMA: E' il soggetto che si occupa del sistema informatico e delle risorse operative

DPS

COSA E' IL DPS

E' l'unico documento in grado di attestare l'adeguamento della struttura alla normativa sulla tutela dei dati personali essendo dotato di data certa. Deve essere redatto entro il 31 dicembre 2004. Il DPS è un manuale di pianificazione della sicurezza dei dati in azienda: descrive come si tutelano i dati personali di dipendenti, collaboratori, clienti, utenti, fornitori ecc. in ogni fase e ad ogni livello (fisico, logico, organizzativo)

In ogni caso si tratta di un consistente piano di gestione della sicurezza, disponibilità ed integrità dei dati, avente data certa a prova formale dell'adeguamento sostenuto.

SCOPO DEL DPS

descrivere la situazione attuale facendo un'analisi dei rischi, una distribuzione dei compiti, un'esame delle misure approntate ed assegnando le responsabilità alle singole persone coinvolte.

E' un documento che, se scritto bene assume una certa complessità soprattutto per società di una certa dimensione con molte persone e con molti dati raccolti. Nel caso degli studi professionali comunque la complessità del documento resta limitata data la tipologia molto specifica dell'attività.

Il DPS deve essere un documento con data certa. Ci sono vari modi per ottenere la data certa tra cui il più semplice può essere il timbro postale su TUTTE LE PAGINE. In alternativa è possibile presentare il documento e Giurarlo in Tribunale (in questo caso il costo dell'operazione sarà la sola marca da bollo e la data certa è quella del documento. L'integrità delle successive pagine è documentata mediante il timbro di congiunzione che unisce tutti i fogli.

Un'alternativa per avere la data certa è quella di firmare digitalmente il documento per chi ha a disposizione un dispositivo di firma digitale (lettore e smart card).

Il DPS, oltre ad avere data certa, deve essere aggiornato annualmente. Il testo unico impone come data per la redazione e l'aggiornamento il 31 marzo di ogni anno, solo per questo anno il termine è stato prorogato al 31/12/04.

Una copia del DPS deve essere custodita presso la sede per essere consultabile e deve essere esibita in caso di controlli.

Il titolare del trattamento deve dare conto nella relazione accompagnatoria del bilancio aziendale annuale dell'avvenuta redazione/aggiornamento del DPS.

Una documentazione in linea con la norma BS7779 e le linee guida ISO 17799:2000 permette di costruire e mantenere nel tempo i processi che determinano e definiscono ruoli, responsabilità e procedure conformi agli obiettivi del Sistema di Gestione per la Sicurezza delle Informazioni.