Titolare del trattamento dati

Grafill s.r.l.

Via Principe di Palagonia 87/91 - Palermo 90100 PA

Rappresentante legale: Mineo Mineo Maria Concetta

DPS

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto ai sensi del
CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
art. 34 e Allegato B, regola 19, del d. lg. 30 giugno 2003, n. 196

Data: 05/03/2006

PARTE I

Capitolo 1

1.1 Premessa

Il Documento Programmatico sulla Sicurezza è una misura minima di sicurezza per la protezione dei dati personali. Il DPS era già previsto dal DPR 318/99, ma è stato interamente rivisitato dal ***CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI*** (d. lg. n. 196 del 30 giugno 2003).
In base al nuovo Codice:

- la misura minima del DPS deve essere ora adottata dal titolare di un trattamento di dati sensibili o giudiziari effettuato con strumenti elettronici, attraverso l'organo, ufficio o persona fisica a ciò legittimata in base all'ordinamento aziendale o della pubblica amministrazione interessata (art. 34, comma 1, lett. g), del Codice; regola 19 dell'Allegato B).
- Il DPS deve essere redatto da alcuni soggetti che non vi erano precedentemente tenuti (ad esempio, da chi trattava dati sensibili o giudiziari, ma con elaboratori non accessibili mediante una rete di telecomunicazioni disponibili al pubblico).
- a differenza del passato, la categoria dei dati giudiziari è oggi rappresentata anche da altri dati personali, riferiti ad esempio a provvedimenti giudiziari non definitivi o alla semplice qualità di imputato o indagato (v. art. 4 del Codice).
- il contenuto stesso del DPS è arricchito da nuovi elementi che si aggiungono a quelli necessari in base alla precedente disciplina o ne specificano alcuni aspetti. Ad esempio, nel DPS occorre descrivere ora i criteri e le modalità per ripristinare la disponibilità dei dati in caso di distruzione o danneggiamento delle informazioni o degli strumenti elettronici; occorre individuare poi i criteri da adottare per cifrare o per separare i dati idonei a rivelare lo stato di salute e la vita sessuale trattati da organismi sanitari ed esercenti le professioni sanitarie (regole 19.8 e 24 dell'Allegato B).

1.2 Campo di applicazione

Chi tratta dati sensibili e giudiziari con elaboratori elettronici deve redigere il Documento Programmatico sulla Sicurezza.
I termini previsti per l'adeguamento sono: il 31 Dicembre per l'anno 2005 e il 31 Marzo a partire dal 2006.
I destinatari dell'obbligo sono:

- sia coloro che abbiano dovuto redigere il Dps per la prima volta nel 2004;
- sia chi, già dotato di un Dps redatto o aggiornato nel 2003, abbia dovuto riaggiornarlo nel 2004.

Il Documento programmatico sulla sicurezza deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

1.3 Definizioni

Trattamento

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Dato personale

Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero identificazione personale.

Dati sensibili

I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati giudiziari

I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Titolare

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Incaricati

Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato

La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Comunicazione

Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Diffusione

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Dato anonimo

Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Blocco

La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Banca dati

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Comunicazione elettronica

Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico.
Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

Misure minime

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

Strumenti elettronici

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Autenticazione informatica

L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Credenziali di autenticazione

I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica.

Parola chiave

Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Profilo di autorizzazione

L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Sistema di autorizzazione

L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Capitolo 2
RUOLI, COMPITI E NOMINA DEI SOGGETTI

2.1 Titolare del Trattamento

Il **Titolare del trattamento è** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il **Titolare del trattamento** deve assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni
fornite per iscritto.

Il **Titolare del trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Responsabili del trattamento dati** che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi del CODICE IN MATERIA DI DATI PERSONALI. Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile della sicurezza dei dati**, ne assumerà tutte le responsabilità e funzioni.

2.2 Responsabile del Trattamento dati

Il Responsabile del trattamento dati è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui sono affidate le seguenti responsabilità e compiti:

- Garantire che tutte le misure di sicurezza dati personali previste siano applicate.
- Redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati.
- Redigere ed aggiornare ad ogni variazione l'elenco degli uffici in cui vengono trattati i dati.
- Redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento.
- Se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione.
- Redigere e di aggiornare ad ogni variazione l'elenco delle sedi e degli uffici in cui viene effettuato il trattamento dei dati.
- Nominare per ciascun ufficio in cui viene effettuato il trattamento dei dati, un incaricato con il compito di controllare i sistemi, le apparecchiature, e se previsti, i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.
- Definire e verificare periodicamente le modalità di acceso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità.
- Decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.
- Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Responsabili della gestione e della manutenzione degli strumenti**

elettronici.

- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Incaricati della custodia delle copie delle credenziali** qualora vi sia più di un incaricato del trattamento.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Incaricati delle copie di sicurezza delle banche dati**.
- Custodire e conservare i supporti utilizzati per le copie dei dati.

Nomina del responsabile della sicurezza dei dati personali

La nomina di ciascun Responsabile della sicurezza dei dati personali deve essere effettuata dal Titolare del trattamento con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione. Copia della lettera di nomina accettata deve essere conservata a cura del Titolare del trattamento in luogo sicuro.

Il Titolare del trattamento deve informare ciascun Responsabile del trattamento dati personali delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

La nomina del Responsabile della sicurezza dei dati personali è a tempo indeterminato, e decade per revoca o dimissioni dello stesso. può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

2.3 Incaricati alla gestione e manutenzione degli strumenti elettronici

2.3.1 Compiti dei responsabili della gestione e della manutenzione degli strumenti elettronici

L' **Incaricato della gestione e della manutenzione degli strumenti elettronici** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di Banche di dati.
E' onere del **Responsabile del trattamento**, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici**.

E' compito degli **Incaricati della gestione e della manutenzione degli strumenti elettronici**:

- Attivare le credenziali di autenticazione agli **Incaricati del trattamento,** su indicazione del **Responsabile del trattamento,** per tutti i trattamenti effettuati con strumenti informatici.
- Definire quali politiche adottare per la protezione dei sistemi contro i virus informatici e verificarne l'efficacia con cadenza almeno semestrale.
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers").
- Informare il **Responsabile della sicurezza dei dati personali** nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Qualora il **Responsabile del trattamento** ritenga di non nominare alcun **Incaricato della gestione e della manutenzione degli strumenti elettronici**, ne assumerà tutte le responsabilità e funzioni.

2.3.2 Nomina dei responsabili della gestione e della manutenzione degli strumenti elettronici

Il **Responsabile del trattamento dati** nomina uno o più soggetti **Incaricati della gestione e della manutenzione degli strumenti elettronici** a cui è conferito il compito di sovrintendere al buon funzionamento delle risorse del sistema informativo e delle **Banche di dati**.

Anche se non espressamente previsto dalla norma, è opportuno che il **Responsabile della sicurezza dei dati personali** nomini uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici**, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.

Il **Responsabile della sicurezza dei dati personali** deve informare ciascun **Incaricato della gestione e della manutenzione degli strumenti elettronici** delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

La nomina di uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici** deve essere effettuata con una lettera di incarico e deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile del trattamento dati personali** in luogo sicuro.

La nomina dell'**Incaricato della gestione e della manutenzione degli strumenti elettronici** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso. Tale nomina può essere revocata in qualsiasi momento dal **Responsabile del trattamento** senza preavviso, ed eventualmente affidata ad altro soggetto.

2.5 Incaricato delle copie di sicurezza delle banche dati

2.5.1 Compiti degli incaricati delle copie di sicurezza delle banche dati

L'**Incaricato delle copie di sicurezza delle banche dati** è la persona fisica o la persona giuridica che ha il compito di sovrintendere alla esecuzione periodica delle copie di sicurezza delle Banche di dati personali gestite.

E' onere del **Responsabile della sicurezza dei dati personali**, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati delle copie di sicurezza delle banche dati**.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce, con il supporto tecnico dell' **Incaricato della gestione e della manutenzione degli strumenti elettronici** la periodicità con cui debbono essere effettuate le copie di sicurezza delle Banche di Dati trattate.

I criteri debbono essere concordati con l' **Incaricato della gestione e della manutenzione degli strumenti elettronici** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni **Banca di dati** debbono essere definite le seguenti specifiche:

- Il "Tipo di supporto" da utilizzare per le "Copie di Back-Up".
- Il numero di "Copie di Back-Up" effettuate ogni volta.
- Se i supporti utilizzati per le "Copie di Back-Up" sono riutilizzati e in questo caso con quale periodicità.
- Se per effettuare le "Copie di Back-Up" si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle "Copie di Back-Up".
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- L'Incaricato del trattamento a cui è stato assegnato il compito di effettuare le "Copie di Back-Up".
- Le istruzioni e i comandi necessari per effettuare le "Copie di Back-Up".

E' compito degli **Incaricati delle copie di sicurezza delle banche dati**:

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal **Responsabile della sicurezza dei dati personali**.
- Assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro.
- Assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato.
- Di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.
- Di segnalare tempestivamente al Responsabile della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Qualora il **Responsabile del trattamento** ritenga di non nominare alcun **Incaricato delle copie di sicurezza delle banche dati**, ne assumerà tutte le responsabilità e funzioni.

2.5.2 Nomina degli incaricati delle copie di sicurezza delle banche dati

Il **Responsabile del trattamento** nomina uno o più soggetti **Incaricati delle copie di sicurezza delle banche dati** a cui è conferito il compito di compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite.

Anche se non espressamente previsto dalla norma, è opportuno che il **Responsabile della sicurezza dei dati personali** nomini uno o più **Incaricati delle copie di sicurezza delle banche dati**, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.

Il **Responsabile della sicurezza dei dati personali** deve informare ciascun **Incaricato delle copie di sicurezza delle banche dati** delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

La nomina di uno o più **Incaricati delle copie di sicurezza delle banche dati** deve essere effettuata con una lettera di incarico e deve essere controfirmata per accettazione.

Copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve consegnare a ciascun **Incaricato delle copie di sicurezza delle banche dati** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

2.7 Incaricato del trattamento dei dati personali

2.7.1 Compiti degli incaricati del trattamento dei dati personali

Gli **Incaricati del trattamento** sono le persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali dal **Responsabile del trattamento**.
In particolare gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- Gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo.
- La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
- La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- L'incaricato del trattamento deve modificarla al primo utilizzo e, successivamente, almeno ogni sei mesi.
- In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi.
- Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.
- Gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali
- 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 dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

2.7.2 Nomina degli incaricati del trattamento dei dati personali

La nomina di ciascun **Incaricato del trattamento dei dati personali** deve essere effettuata dal **Responsabile del trattamento** con una **lettera di incarico** in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata dall'interessato per presa visione.

Copia della lettera di nomina firmata deve essere conservata a cura del **Responsabile del trattamento** in luogo sicuro.

Il **Responsabile del trattamento** deve informare ciascun **Incaricato del trattamento dei dati**

personali delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Il **Responsabile del trattamento** deve consegnare a ciascun **Incaricato del trattamento dei dati personali** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

Gli **Incaricati del trattamento dei dati personali** devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli **Incaricati del trattamento dei dati personali** deve essere assegnata una **parola chiave** ed un **codice di autenticazione informatica**.

Agli **Incaricati del trattamento dei dati personali** è prescritto di adottare le necessarie cautele per assicurare la segretezza della **parola chiave** e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato.

La nomina dell'**Incaricato del trattamento dei dati personali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso. Tale nomina essere revocata in qualsiasi momento dal **Responsabile del trattamento** dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.