Fondazione Luca Pacioli

CODICE DELLA PRIVACY

Documento Programmatico sulla Sicurezza

Documento n. 10 del 31 marzo 2004

CIRCOLARE

Via G. Paisiello, 24 – 00198 Roma – tel.: 06/85.440.1 (fax 06/85.440.223) – C.F.:80459660587
www.fondazionelucapacioli.it - fondazionelucapacioli@consrag.it

CODICE DELLA PRIVACY

Documento Programmatico sulla Sicurezza

Facciamo seguito alla Circolare "Codice della Privacy – Testo Unico in materia di dati personali (D.Lgs. 30 giugno 2003, n. 169)", documento n. 9 del 19 marzo 2004, con la quale si è fornita una prima informazione sulla nuova normativa in materia di Privacy. In tale ambito è stato analizzato anche l'adempimento relativo alla redazione del Documento Programmatico sulla Sicurezza (di seguito DPS), a proposito del quale, in una nota inviata al Garante, la Fondazione Luca Pacioli aveva sottoposto all'Autorità Garante due questioni:

1. L'individuazione del preciso ambito di applicazione dell'obbligo di redazione del DPS
2. Il termine entro il quale dovesse essere redatto il documento stesso.

Si comunica al riguardo che il 22 marzo scorso l'Autorità Garante ha fornito un parere (di cui si allega il testo), in risposta ad un quesito di Confindustria, nel quale vengono dati importanti spunti e chiarimenti in merito a termini e modalità di applicazione delle misure minime di sicurezza.

Con detto parere il Garante ha inteso rispondere anche ai dubbi sollevati dalla Fondazione Luca Pacioli in merito ai quali è stato precisato quanto segue:

1. l'obbligo di redazione del DPS coinvolge tutti i soggetti che trattino dati sensibili o giudiziari con l'ausilio di strumenti elettronici;
2. **il DPS dovrà essere redatto entro il 30 giugno 2004** sia da parte di chi è tenuto a redigerlo per la prima volta nel 2004 sia da parte di chi, già dotato di un DPS redatto o aggiornato nel 2003, ritenga necessario utilizzare un trimestre in più, rispetto al prossimo 31 marzo, per curare la stesura di un testo significativo e più impegnativo nella ricognizione dei rischi e degli interventi previsti.

L'Autorità Garante, inoltre, informa che, a breve, sarà disponibile un modello base semplificato di documento programmatico sulla sicurezza sul sito www.garanteprivacy.it.

Una volta delimitato l'ambito di applicazione della norma relativa al DPS, ci sembra opportuno evidenziare, in concreto, chi sono i soggetti tenuti alla redazione del documento.
In primo luogo si rileva che l'obbligo di redazione del DPS era già previsto dalla precedente normativa DPR 28 luglio 1999, n. 318, art. 6, che disponeva l'obbligo di redazione del DPS nel caso di trattamento dei dati sensibili o giudiziari effet-

tuati con strumenti elettronici accessibili mediante una rete di telecomunicazioni disponibili al pubblico. Comparando la vecchia disciplina e la nuova si desume una duplice novità:

- a differenza della normativa precedente sono ora tenuti alla redazione del DPS anche coloro che trattano dati sensibili e giudiziari con elaboratori non accessibili mediante una rete di telecomunicazioni disponibili al pubblico;
- è ampliata la categoria dei dati giudiziari, che adesso ricomprende anche altri dati personali, riferiti ad esempio a provvedimenti giudiziari non definitivi o alla semplice qualità di imputato o indagato.

Nonostante questo parziale ampliamento dei soggetti interessati dalla norma, ci sembra di poter affermare che, sostanzialmente, la cerchia dei soggetti interessati all'adempimento rimane invariata. Più nello specifico, sono ricompresi nel novero dei soggetti tenuti all'adempimento:

- le aziende e pubbliche amministrazioni che trattano dati sensibili e giudiziari con l'ausilio di strumenti informatici;
- i professionisti che trattano dati sensibili e giudiziari con l'ausilio di strumenti informatici.

Per quanto attiene all'ambito dei professionisti, non sorgono dubbi per gli obblighi in capo a medici o avvocati che, per la natura dell'attività svolta, possono ritenersi chiamati abitualmente al trattamento di dati sensibili e giudiziari.
Diverso il discorso per quanto riguarda le professioni economico-contabili. Non sembra infatti possa ravvisarsi in questa area il trattamento di dati sensibili o giudiziari. Per quanto attiene la compilazione delle dichiarazioni dei redditi, infatti, non sembra sia contemplato alcun trattamento di dati sensibili, neanche in relazione alle spese sanitarie per le quali è possibile risalire unicamente agli importi e non allo stato di salute del contribuente. Pertanto, a nostro avviso, i ragionieri e i dottori commercialisti non dovrebbero essere tenuti alla redazione del documento.
Nonostante questa indicazione di massima, consigliamo comunque la predisposizione di un documento costruito secondo lo schema del DPS a supporto della predisposizione delle altre misure di sicurezza che comunque dovranno essere adottate (si veda in merito la Circolare n. 9 del 19 marzo 2004).

Allegato 1
Parere del Garante per la protezione dei dati personali

Parere - 22 marzo 2004

Obblighi di sicurezza e documento programmatico: al 30 giugno la redazione del "dps"

Confindustria
Viale dell'Astronomia, n. 30
00144 – R O M A

Oggetto: prima applicazione del Codice in materia di protezione dei dati personali in materia di "misure minime" di sicurezza (artt. 31-36 e Allegato B) al d.lg. n. 196/2003).

Il Codice entrato in vigore il 1° gennaio 2004 ha confermato e aggiornato la disciplina in materia di sicurezza dei dati personali e dei sistemi informatici e telematici introdotta nel 1996.
Diversi principi affermati dal nuovo Codice non sono nuovi per gli operatori.
In particolare è stato confermato il principio (evidenziato con maggiore chiarezza dalle nuove disposizioni) secondo cui le "misure minime", di importanza tale da indurre il legislatore a prevedere anche una sanzione penale, sono solo una parte degli accorgimenti obbligatori in materia di sicurezza (art. 33 del Codice).
In materia, come già previsto dalla legge n. 675/1996, si distinguono *due distinti obblighi*:

a) l'obbligo più generale di ridurre al minimo determinati rischi.
Occorre custodire e controllare i dati personali oggetto di trattamento per contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dei casi consentiti o altrimenti trattati in modo illecito.
Resta in vigore, oltre alle cosiddette "misure minime", l'obbligo di adottare ogni altra misura di sicurezza idonea a fronteggiare le predette evenienze, avuto riguardo alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle caratteristiche del trattamento, di cui si devono valutare comunque i rischi (art. 31).
Come in passato, l'inosservanza di questo obbligo rende il trattamento illecito anche se non si determina un danno per gli interessati; viola inoltre i loro diritti, compreso il diritto fondamentale alla protezione dei dati personali che può essere esercitato nei confronti del titolare del trattamento (artt. 1 e 7, comma 3, del Codice), ed espone a responsabilità civile per danno anche non patrimoniale qualora, davanti al giudice ordinario, non si dimostri di aver adottato tutte le misure idonee ad evitarlo (artt. 15 e 152 del Codice);

b) nell'ambito del predetto obbligo più generale, il dovere di adottare in ogni caso le "misure minime".
Nel quadro degli accorgimenti più ampi da adottare per effetto dell'obbligo ora richiamato, occorre assicurare comunque un livello minimo di protezione dei dati personali.
Pertanto, in aggiunta alle conseguenze appena ricordate, il Codice conferma l'impianto secondo il quale l'omessa adozione di alcune misure indispensabili ("minime"), le cui modalità sono specificate tassativamente nell'Allegato B) del Codice, *costituisce anche reato* (art. 169 del Codice, che prevede l'arresto sino a due anni o l'ammenda da 10 mila euro a 50 mila euro, e l'eventuale "ravvedimento ope-

roso" di chi adempie puntualmente alle prescrizioni impartite dal Garante una volta accertato il reato ed effettua un pagamento in sede amministrativa, ottenendo così l'estinzione del reato).

1. LE NUOVE "MISURE MINIME": TERMINI PER L'ADOZIONE

1.1. Il Codice, come previsto dalla legge n. 675/1996 e come dovrà avvenire periodicamente in base all'evoluzione tecnologica (art. 36 del Codice), ha *aggiornato l'elenco* delle "misure minime" le cui modalità di applicazione, sulla base di alcune prescrizioni di ordine generale (artt. 33-35 del Codice), sono indicate analiticamente nelle 29 regole incluse nell'Allegato B) del medesimo Codice.
Analogamente a quanto avveniva in passato, *le misure minime sono diverse* a seconda che il trattamento sia effettuato o meno con strumenti elettronici, oppure riguardi dati sensibili o giudiziari.
Per alcune di esse sono previste scadenze periodiche, ma le "misure minime" che erano già obbligatorie in passato devono essere adottate ancora oggi *senza* attendere il decorso di termini transitori.

1.2. Il termine transitorio che permette di adottare le misure entro il 30 giugno 2004 riguarda solo *le nuove misure* (art. 180, comma 1, d.lg. n. 196/2003; per la precedente disciplina, v. gli artt. 15, comma 2 e 41 l. n. 675/1996, il d.P.R. n. 318/1999 e la l. n. 325/2000).
É previsto un periodo più ampio per l'adeguamento (fino al 1° gennaio 2005) solo se, in un caso del tutto particolare, ricorrano obiettive ragioni di natura tecnica.
Si tratta dell'ipotesi specifica (che riguarda solo i trattamenti effettuati con strumenti elettronici) in cui il titolare del trattamento, alla data del 1° gennaio scorso, disponeva di strumenti elettronici che, per le predette obiettive ragioni esclusivamente tecniche, documentate in un *atto a data certa* da redigere al più tardi entro il 30 giugno 2004, non consentono di applicare immediatamente, in tutto o in parte, le *nuove* misure minime. Sempre in questo circoscritto caso, nel quale si è obbligati a prevenire comunque un incremento dei rischi (art. 180, comma 3, del Codice), occorre conservare il documento a data certa il quale non va trasmesso al Garante, che può però richiederne l'esibizione in sede di accertamento anche ispettivo (artt. 157 ss. del Codice).
Per quanto riguarda le modalità per far risultare una "data certa" si dovrà applicare la disciplina civilistica in materia di prova documentale (v. in particolare, gli artt. 2702-2704 del codice civile) e si potranno tenere presenti i suggerimenti formulati dal Garante in un parere del 2000 qui allegato, e redatto a proposito di un analogo documento previsto in tema di sicurezza (art. 1 l. n. 325/2000).
In materia di "misure minime", anche quando si rediga il documento a data certa, non va pertanto effettuata alcuna comunicazione al Garante; dalla circostanza che l'Autorità abbia ricevuto eventuali note in proposito, spesso peraltro succinte, il titolare del trattamento non potrà inoltre desumere, anche in caso di mancato riscontro, alcun assenso o autorizzazione del Garante a proseguire il trattamento dei dati con le modalità dichiarate.

2. IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

2.1 Anche la redazione del DPS *è una "misura minima"*, prevista dall'Allegato B).
Si tratta di una misura non nuova, sebbene sia aumentato il numero dei soggetti che deve redigere il DPS e sia parzialmente diverso il suo necessario contenuto.
Infatti, la precedente disciplina *prevedeva già* l'obbligo di predisporre e aggiornare il DPS, almeno annualmente, in caso di trattamento di dati sensibili o relativi a determinati provvedimenti giudiziari effettuato mediante elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico (artt. 22 e 24 l. n. 675/1996; art. 6 d. P.R. n. 318/1999).
I soggetti tenuti a predisporre il DPS hanno potuto redigerlo per la prima volta entro il *29 marzo 2000* o, al più tardi, entro il *31 dicembre 2000* (artt. 15, comma 2 e 41, comma 3 l. n. 675/1996; l. n. 325/2000); dovendo rispettare l'obbligo di revisione almeno annuale, hanno dovuto aggiornare il DPS negli anni successivi, anche nel 2003.

2.2. 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)).
Come accennato, 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).
Inoltre, 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).
Infine, 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)).

2.3. Benché non si tratti a rigore di una misura "nuova", è quindi legittimamente sostenibile che il DPS da redigere quest'anno per la prima volta, o da aggiornare, possa essere predisposto *al più tardi entro il 30 giugno 2004*, anziché necessariamente entro il 31 marzo, data che è invece prevista a regime per i prossimi anni, a partire dal 2005 (cfr. regola 19).
Si perviene a questa conclusione per tutti i destinatari dell'obbligo:
a) sia per coloro che devono redigere il DPS per la prima volta nel 2004;
b) sia per chi, già dotato di un DPS redatto o aggiornato nel 2003, ritenga necessario utilizzare un trimestre in più, rispetto al prossimo 31 marzo, per curare la stesura di un testo significativo e più impegnativo nella ricognizione dei rischi e degli interventi previsti.
Il termine più ampio del 30 giugno 2004 permetterà di utilizzare facoltativamente il modello-base e semplificato di DPS che il Garante è in procinto di porre a disposizione dei titolari del trattamento interessati, soprattutto per le realtà medio-piccole che non si attiveranno entro il 31 marzo.
Non sussistono infine margini per sostenere che il DPS possa essere redatto per la prima volta o aggiornato solo nel 2005. Il DPS è peraltro una misura da adottare con un documento, anziché un accorgimento da applicare direttamente a strumenti elettronici, per cui non è possibile invocare un differimento al 2005 neppure in applicazione dello speciale meccanismo già descritto a proposito delle obiettive ragioni tecniche relative a strumenti elettronici.

3. RELAZIONE ACCOMPAGNATORIA AL BILANCIO D'ESERCIZIO

3.1 Le scelte di fondo sulle modalità di trattamento sotto il profilo della sicurezza competono alle persone e agli organi legittimati ad adottare decisioni ed esprimere a vari livelli, in base al proprio ordinamento interno, la volontà della società, ente o altro organismo titolare del trattamento (art. 4, comma 1, lett. f), del Codice).
In questo quadro, il Codice ha introdotto una nuova regola per rendere meglio edotti gli organi di vertice del titolare del trattamento e responsabilizzarli in materia di sicurezza, attraverso l'obbligo di riferire nella relazione di accompagnamento a ciascun bilancio di esercizio circa l'avvenuta redazione o aggiornamento del DPS che sia obbligatorio come misura "minima" o che sia stato comunque adottato (regola 26 Allegato B)).
Anche questa menzione rappresenta una misura "minima" nuova, indicata tra quelle di "tutela e garanzia" (regole 25 e 26).
3.2 I soggetti pubblici e privati tenuti in passato a predisporre o aggiornare il DPS, e che per il 2004 possono come detto aggiornarlo entro il 30 giugno del presente anno, dovranno riferire secondo la regola 26 *già a partire dalla relazione sul bilancio di esercizio per il 2003*, con riferimento al DPS già eventualmente aggiornato per il 2004, oppure menzionando l'adozione o aggiornamento avvenuto nel

2003 e indicando sinteticamente che si aggiornerà il DPS entro il 30 giugno 2004.
I soggetti pubblici e privati tenuti invece per la prima volta a redigere il DPS nel 2004 (come si è detto entro il 30 giugno), non devono indicare nella relazione alcunché se il DPS 2003 o il DPS 2004 non sono stati adottati. I medesimi soggetti, qualora alla data in cui predispongono la predetta relazione abbiano redatto già il DPS 2004, indicheranno invece tale circostanza; potranno infine indicare facoltativamente quanto eventualmente già fatto nel 2003 e, sempre facoltativamente, l'aggiornamento 2004 *in itinere*.
Diamo in conclusione risposta alla Vostra richiesta nei predetti termini, tenendo presenti altri quesiti pervenuti su questioni collegate e allegando una tabella esemplificativa delle principali scadenze.

Il Segretario generale
(dott. Giovanni Buttarelli)

Disposizioni transitorie

Termini
Adempimenti

30 giugno 2004
Adozione per il 2004 di tutte le "misure minime" non previste dalla precedente disciplinaTermine ultimo per predisporre il documento a data certa per descrivere le obiettive ragioni tecniche che non consentono di applicare immediatamente alcune nuove misure minime *(documento utilizzabile unicamente nel caso del tutto particolare previsto dall'art. 180, comma 2, del Codice per i soli strumenti elettronici)*.

1° gennaio 2005
Adozione nuove misure minime su strumenti elettronici non previste in base alla precedente disciplina *(solo per i soggetti legittimati a predisporre il predetto documento a data certa)*.

Documento programmatico sulla sicurezza
Relazione accompagnatoria al bilancio d'esercizio
Misure
Soggetti già tenuti a redigere o aggiornare il DPS (1)
Soggetti non obbligati a redigere o aggiornare il DPS in base alla previgente disciplina

DPS 2004
Aggiornamento DPS entro il **30 giugno 2004.**
Redazione DPS entro il **30 giugno 2004.**

Relazione accompagnatoria del bilancio esercizio 2003
Riferimento al DPS redatto o aggiornato nel 2003 (con facoltà di indicazione aggiuntiva dell'aggiornamento 2004 *in itinere*), oppure menzione dell'aggiornamento eventualmente già effettuato nel 2004.
Nessun riferimento se il DPS 2003 o il DPS 2004 non sono stati adottati, oppure riferimento al DPS eventualmente già adottato nel 2004. Facoltà di indicazione del DPS eventualmente predisposto nel 2003 e facoltà di indicazione dell'aggiornamento 2004 *in itinere*.

(1) titolari di un trattamento di dati sensibili o relativi a provvedimenti giudiziari di cui agli artt. 22 e 24 della legge n. 675/1996, effettuato mediante elaboratori accessibili mediante una rete di telecomunicazione disponibili al pubblico.