

INFORMATIVA SULLA PROTEZIONE DEI DATI PERSONALI

SCADENZA

DOCUMENTO PROGRAMMATICO SICUREZZA (DPS)

31 MARZO 2006

Il Codice della Privacy

Decreto Legislativo 30 giugno 2003, n. 196

“Codice in materia di protezione dei dati personali”

Informazioni essenziali di “chi” e “come” deve adeguarsi

Si ricorda che la Legge sulla Privacy è divenuta operativa il primo gennaio 2004 e che le varie proroghe dovute ai Decreti definiti “milleproroghe” riguardano esclusivamente la redazione del Documento programmatico sulla Sicurezza (D.P.S.S.) e l'adozione delle misure minime di sicurezza sui computer che, per motivi oggettivi certificati da documento avente data certa, non si potevano adeguare immediatamente, mentre le informative ai clienti, le lettere di nomina ai responsabili e di incarico al personale interno dovevano già essere predisposte dall'entrata in vigore del D.Leg. 196/2003.

Cos'è il Codice della Privacy

Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

Il "codice" garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Chi è tenuto ad adeguarsi

Il codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da **chiunque** è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato; quindi tutti coloro che, per motivi professionali, in forma organizzata trattano dati, con o senza l'ausilio di strumenti elettronici.

(liberi professionisti, alberghi, ristoranti, medici, avvocati ..., Pubblica Amministrazione, Enti o Associazioni ecc.)

Definizioni

a) "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;

b) "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 di identificazione personale;

c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

Collegio dei Geometri

Forlì - Cesena

- d) "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;
- e) "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 60e61 del codice di procedura penale;
- f) "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;
- g) "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;
- h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- i) "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- l) "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;
- m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
-

Ai fini del codice si intende, altresì, per:

- a) "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;
- b) "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- c) "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- d) "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;
- e) "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;
- f) "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;
- g) "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.

Collegio dei Geometri

Forlì - Cesena

Cosa fare per adeguarsi

Dotare la propria Azienda delle “misure minime” di sicurezza, attivandosi con l’implementazione nel sistema organizzativo di una serie di documenti da distribuire a responsabili interni - o esterni - e ad incaricati, e proteggere i personal computer contro la perdita, anche accidentale, dei dati contenuti.

Documenti richiesti

informativa e consenso all’interessato
informativa e consenso dei dipendenti
lettere di nomina agli incaricati
istruzioni finalizzate alla conservazione dei documenti cartacei
istruzioni finalizzate alla gestione e conservazione delle password
lettere di designazione del responsabile
lettere di designazione dell’amministratore del sistema
lettere di designazione del custode delle password
lettere di designazione dei responsabili esterni: commercialista, consulente del lavoro, studio legale ...
policy aziendale sul corretto utilizzo delle risorse informatiche
....

Verifica dei P.C. ed eventuale adozione di

Password di autenticazione
Criterio di autorizzazione alle banche dati
Analisi dei rischi dovuti alle risorse umane ed ambientali
Sistema operativo degli elaboratori
Rete internet
Software antivirus
Firewall
Server di rete
Procedure operative di salvataggio e custodia delle copie di backup
Procedure operative per il ripristino dei dati e del sistema

Redazione del Documento Programmatico sulla Sicurezza (D.P.S.S.) comprendente:

1. l’elenco dei trattamenti di dati personali (punto 19.1 del disciplinare), mediante:
 - la individuazione dei tipi di dati personali trattati
 - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti
2. la distribuzione dei compiti e delle responsabilità, nell’ambito delle strutture preposte al trattamento dei dati (analisi del mansionario privacy, punto 19.2 del disciplinare) e previsione di interventi formativi degli incaricati del trattamento (punto 19.6 del disciplinare)
3. l’analisi dei rischi che incombono sui dati (punto 19.3 del disciplinare)
4. le misure, già adottate e da adottare, per garantire l’integrità e la disponibilità dei dati (punto 19.4 del disciplinare)
5. i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento (punto 19.5 del disciplinare)
6. i criteri da adottare, per garantire l’adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all’esterno (punto 19.7 del disciplinare)
7. le procedure da seguire per il controllo sullo stato della sicurezza
8. dichiarazioni d’impegno e firma.

Il presente sunto deve essere considerato soltanto una rapida presentazione di ciò che è la Legge sulla Privacy, una semplice guida operativa delle modalità e procedure da seguire per una esatta esecuzione della modulistica richiesta, senza volersi sostituire a qualsiasi documento ufficiale da utilizzare al fine degli adeguamenti previsti dal Codice.