IL NUOVO CODICE SULLA PRIVACY

DECRETO LEGISLATIVO N. 196/2003

20 Settembre
Fondazione Ordine degli Ingegneri di Milano
Corso Venezia

Relatore Ing. Sommaruga Andrea Guido

Introduzione al Decreto Legislativo 196/2003

Il trattamento dati

L'adeguamento tecnico dei sistemi informativi e le misure minime di sicurezza

Il documento Programmatico sulla Sicurezza

sommaa@stcom.com

D.L.G. 196/2003

il D.L.G. 196/2003 nasce come evoluzione del precedente D.P.R. 318/1999 allo scopo di definire dei requisiti minimi di sicurezza per il trattamento dei dati.

sommaa@stcom.com

Dlg 196/2003: Proroghe

Nella G.U. del 2 marzo 2005 n.50 pubblica la Legge 1° marzo 2005, n.26 di conversione del
Decreto Legge n.314 del 30 dicembre 2004, (milleproroghe) con cui si spostano i termini di applicazione del D.Lgs. 196/2003 come segue:

- al 31 dicembre 2005 (invece del 30 giugno 2005) il termine per l'adozione delle nuove misure minime di sicurezza e del DPS.
- al 31 marzo 2006 (anzichè il 30 settembre 2005) il termine per l'adeguamento tecnologico ad opera dei titolari che dispongono di strumenti che per ragioni tecniche, non consentono l'immediata applicazione delle misure minime di sicurezza (sistemi obsoleti).

sommaa@stcom.com

Dlg 196/2003: Tipo di dati

I dati sono classificabili in tre categorie

- Comuni
- Sensibili
- Giudiziari

Il trattamento dei dati è classificabile in due categorie

- Manuale
- Automatizzato

sommaa@stcom.com

Dlg 196/2003: Figure previste

La normativa prevede tre tipi di figure

- Titolare del trattamento dati
- Responsabile/i del trattamento dati
- Incaricato/i del trattamento dati

Più eventualmente una quarta figura nel caso di utilizzo di calcolatori

- Amministratore/i del sistema informativo

sommaa@stcom.com

Dlg 196/2003: Titolare Trattamento

Il titolare del trattamento ha l'incarico di redigere il DPS o di farlo redigere da un responsabile incaricato.
Nei confronti della Legge il Titolare e' l'unico responsabile del trattamento.
Anche se ha la facoltà di nominare un responsabile è sempre il Titolare che deve rispondere di eventuali violazioni.

sommaa@stcom.com

Dlg 196/2003: Responsabile

Il Responsabile è nominato dal Titolare con Lettera di Incarico scritta.
L'incarico ha durata illimitata.

Il Responsabile deve garantire la corretta applicazione del DPS e procedere alle nomine degli incaricati al trattamento.

sommaa@stcom.com

Gli incaricati al trattamento sono le persone che, per lo svolgimento del loro lavoro, devono trattare i dati raccolti.

Sono nominati con lettera dal Responsabile.

Devono attenersi alle istruzioni ricevute.

sommaa@stcom.com

Art. 37. Notificazione del trattamento

1. Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:

a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;

b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;

c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;

d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;

e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;

f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

sommaa@stcom.com

Art. 40. Autorizzazioni generali

Le disposizioni del presente codice che prevedono un'autorizzazione del Garante sono applicate anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti, pubblicate nella *Gazzetta Ufficiale* della Repubblica italiana.

Art. 41. Richieste di autorizzazione

Il titolare del trattamento che rientra nell'ambito di applicazione di un'autorizzazione rilasciata ai sensi dell'articolo 40 non è tenuto a presentare al Garante una richiesta di autorizzazione se il trattamento che intende effettuare è conforme alle relative prescrizioni.

sommaa@stcom.com

Dlg 196/2003: Liberi Professionisti

I liberi professionisti, iscritti ad Albi professionali, non sono tenuti a dare comunicazione del trattamento dati al Garante salvo particolari casi di trattamento di dati Sensibili.

sommaa@stcom.com

Dlg 196/2003: Liberi Professionisti

Per i professionisti c'e' l'obbligo di comunicazione al Garante se trattano dati:

- Dati genetici o biometrici che indicano posizione geografica di persone mediante rete
- Dati idonei a rilevare stato di salute e vita sessuale, serivizi sanitari on-line
- Dati trattati con l'ausilio di strumenti elettronici volti a definire la personalità ed il profilo dell'interessato
- Dati sensibili raccolti in banche dati al fine della selezione personale conto terzi
- Dati registrati in banche dati elettroniche relativi a rischi solvibilità economica, situazione partimoniale e comportamenti illeciti o fraudolenti.

sommaa@stcom.com

Dlg 196/2003: Comunicazione Garante

La comunicazione al Garante è possibile solo via telematica con apposizione della firma digitale e con pagamenti telematici via carta di credito.

Deve essere fatta una sola volta prima di iniziare il trattamento

sommaa@stcom.com

Dlg 196/2003: Illeciti Penali

La Legge prevede delle sanzioni anche molto pesanti per le violazioni al Codice della Privacy.

La violazione più grave resta il trattamento illecito di dati personali per il quale sono previste pene con reclusione da 6 mesi a tre anni a seconda dei casi.

sommaa@stcom.com

CAPO II - REGISTRI PUBBLICI ED ALBI PROFESSIONALI

Art. 61. Utilizzazione di dati pubblici

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici, anche individuando i casi in cui deve essere indicata la fonte di acquisizione dei dati e prevedendo garanzie appropriate per l'associazione di dati provenienti da più archivi, tenendo presente quanto previsto dalla Raccomandazione n. R (91)10 del Consiglio d'Europa in relazione all'articolo 11.

2. Agli effetti dell'applicazione del presente codice i dati personali diversi da quelli sensibili o giudiziari, che devono essere inseriti in un albo professionale in conformità alla legge o ad un regolamento, possono essere comunicati a soggetti pubblici e privati o diffusi, ai sensi dell'articolo 19, commi 2 e 3, anche mediante reti di comunicazione elettronica. Può essere altresì menzionata l'esistenza di provvedimenti che dispongono la sospensione o che incidono sull'esercizio della professione.

3. L'ordine o collegio professionale può, a richiesta della persona iscritta nell'albo che vi ha interesse, integrare i dati di cui al comma 2 con ulteriori dati pertinenti e non eccedenti in relazione all'attività professionale.

4. A richiesta dell'interessato l'ordine o collegio professionale può altresì fornire a terzi notizie o informazioni relative, in particolare, a speciali qualificazioni professionali non menzionate nell'albo, ovvero alla disponibilità ad assumere incarichi o a ricevere materiale informativo a carattere scientifico inerente anche a convegni o seminari.

sommaa@stcom.com

Dlg 196/2003: Informativa

L'informativa è una lettera inviata a tutti i soggetti di cui si raccolgono i dati per metterli al corrente delle modalita' e della finalità del trattamento dei loro dati e per ricordare che la Legge prevede il diritto di accesso / rettifica dei dati raccolti.

Le lettere informative inviate precedentemente ai sensi del DPR 318/99 devono essere reinviate.

sommaa@stcom.com

Il consenso è un documento che viene fatto preventivamente firmare dai soggetti dei quali si deve raccogliere i dati.
La richiesta di consenso preventivo è obbligatoria qualora si raccolgano dati sensibili.
Non c'e' obbligo di consenso per la raccolta di dati necessari all'adempimento di obblighi di Legge.
Il consenso richiesto ai sensi del DPR 318/99 non ha più valore.

sommaa@stcom.com

Il DPS è un documento che descrive le procedure da adottare per rendere sicuro il trattamento dei dati effettuato sia manualmente che con l'ausilio di materiale elettronico o audiovisivo.

sommaa@stcom.com

Il DPS deve contenere a grandi linee:

- Elenco dei trattamenti
- Compiti e responsabilita'
- Analisi dei rischi
- Contromisure
- Piano di Disaster/Recovery
- Formazione continua

sommaa@stcom.com

Nell'Elenco trattamenti deve descrivere

- Tipi dati trattati
- Incaricati al trattamento
- Responsabile del trattamento
- Tipologia ed ubicazione banche dati

sommaa@stcom.com

Tra i compiti e le responsabilità si devono dettagliare le seguenti figure:

Sicurezza

- Responsabile del trattamento
- Responsabile del ced
- Amministratore di sistema

Controllo

- Persona delegata ad effettuare una verifica annuale alla correttezza delle norme

sommaa@stcom.com

Analisi dei Rischi

Fattori di rischio ed entità del rischio

- Cadute di tensione, blackout
- Guasti Hardware
- Problemi software
- Errori umani

Minacce esterne

- Intrusioni
- Furti di hardvare
- Furti di documenti o tabulati
- Furti di password

sommaa@stcom.com

Contromisure da adottare

Protezione dei dati

- Misure fisiche (antifurto, chiavi ecc)
- Protezione sistemi informativi (firewall, antivirus...)
- Backup periodici (backup giornalieri, mensili, annuali)

Password e Log e Controlli

- Utilizzo password cambiate ogni 60 gg
- Verifica periodica LOG dei firewall e degli antivirus
- Verifica funzionamento backup

Procedure di verifica e Controllo

- Verifica rispetto DPS e regolamenti
- Verifica porogrammi installati sulle macchine

sommaa@stcom.com

Disaster Recovery

Il Responsabile dei backup deve:

- Conservare con cura i nastri di backup in luogo idoneo e non accessibile. (non nella stessa sede del CED)

Il Responsabile del trattamento deve:

- Identificare un eventuale sede alternativa per il recovery in caso di danni gravi ai locali CED
- Accordi con i fornitori per avere le macchine in caso di disastro in un tempo massimo stabilito.
- Mantenere una lista aggiornata delle licenze del software installato e dei manuali operativi per il ripristino dei sistemi.

sommaa@stcom.com

Formazione Permanente

La sicurezza non è un fatto statico ma:

- Deve essere prevista una revisione periodica del DPS (al massimo annuale)
- Devono essere previsti degli eventi formativi per illustrare agli Incaricati le eventuali variazioni procedurali
- Deve essere adottato un regolamento interno per l'utilizzo delle attrezzature elettroniche
- Deve essere prevista la fase formativa per tutti gli eventuali neoassunti o collaboratori esterni

sommaa@stcom.com

Ultima osservazione sul DLG 196/2003

la norma, nel caso di attrezzature informatiche, prevede tutti adempimenti a carico dell'utente finale dei programmi.
In fase di acquisto di nuovo software, sia che si tratti di un sistema operativo o che si tratti di un programma di videoscrittura, conviene richiedere al fornitore la Certificazione del programma acquistato ai sensi del DLG 196/2003.

Probabilmente il fornitore non vorrà rilasciare la certificazione ma è corretto ?

sommaa@stcom.com

Open Source: La Licenza

Come tutte le cose anche questa presentazione è coperta da licenza d'uso:

Copyright (c) 2004 – Ing. Sommaruga Andrea Guido

è garantito il permesso di copiare, distribuire e/o modificare questo documento seguendo i termini della **Licenza per Documentazione Libera GNU**, Versione 1.2, oppure ogni versione successiva pubblicata dalla Free Software Foundation;

- senza Sezioni Non Modificabili
- senza Testi Copertina
- senza Testi di Retro Copertina
- Mantenendo intatte le indicazioni di Copyright (c)

la versione originale in inglese della licenza è disponibile su www.gnu.org/copyleft/fdl.html

sommaa@stcom.com