

LE NORME IN MATERIA DI PRIVACY E PROTEZIONE DEI DATI IN VIGORE DAL 1 GENNAIO 2004

Panoramica generale

Paolo Panella (Studio Panella)
www.panella.org

F.A.V. - Bologna – 25 Gennaio 2006

Introduzione

Dati e Informazioni

Introduzione

- “L’informazione è un bene aziendale che rappresenta un valore e che è necessario proteggere adeguatamente”

BS ISO17799 – 12/2000 – standard internazionale per la sicurezza delle informazioni (BS 7799 – 05/1999)

Introduzione

Riservatezza

- Prevenire l'accesso abusivo

Disponibilità

- Garantire l'accesso autorizzato

Integrità

- Prevenire l'alterazione

Introduzione

Sicurezza logica (IT)

- identificazioni, antivirus, cifratura, firma digitale, firewall, auditing lan, ...

Sicurezza fisica

- vigilanza, accessi, antincendio, custodia, UPS, allarmi, ...

Sicurezza organizzativa

- Ruoli, responsabilità, formazione, procedure, obiettivi, ...

La legge

- D.L. 675 – 31 dicembre 1996
- D.P.R. 318 – 28 luglio 1999

- D.L. 196 – 30 giugno 2003
(G.U.29/07/2003) In vigore dal 1/1/2004

La legge

- Art. 1 del D.Lgs. 196/03
- Art.51 della Costituzione Europea

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

La legge

Perchè

IERI	OGGI
Ambienti circoscritti	Nessun limite geografico
Persone definite	Chiunque
Limiti degli strumenti	Innalzamento esponenziale

La legge

- Tra il D.L. 675/96 ed il D.L. 196/03 sono stati pubblicati altri 14 decreti sull'argomento
- Si passa da “Testo unico... trattamento...” a “Codice di protezione...”
- Si passa da “...misure...” a “...obblighi...”

La legge

Art. 2050 c.c.:

- Chiunque cagiona danno ad altri nello svolgimento di una attività pericolosa, per sua natura o per la natura dei mezzi adoperati è tenuto al risarcimento **se non prova di avere adottato tutte le misure idonee ad evitare il danno.**

Finalità della Legge

**DEFINIZIONE DEL DIRITTO AL
RISPETTO ED ALLA PROTEZIONE
DEI DATI PERSONALI**

**DEFINIZIONE DELLE REGOLE E DEI
METODI DA APPLICARE**

**DEFINIZIONE DELLE SANZIONI
AMMINISTRATIVE E PENALI**

Finalità della Legge

- Fornire la garanzia alle persone fisiche e giuridiche oggetto di raccolta di informazioni che i loro dati non vengono diffusi e neppure utilizzati senza una esplicita autorizzazione.
- Garantire che i suddetti dati vengono conservati e protetti con la massima diligenza e cura.

[artt.1; 2 e 3](#)

Principi generali

- **IL TRATTAMENTO NON NECESSARIO E' ILLECITO.**
- **NON E' LECITO CHIEDERE IL CONSENSO PER UN TRATTAMENTO NON NECESSARIO.**
- **LA LEGGE INDICA I CASI LECITI.**

Principi generali

- In mancanza di autorizzazione non si può effettuare il trattamento dei dati !
- Si applicano le autorizzazioni generali e le deroghe previste dalla legge
- Per casi particolari le richieste di autorizzazione vanno inoltrate al Garante. In caso di mancata risposta entro 45 giorni debbono considerarsi rigettate. (art.26)

Principi generali

Diritti dell'Interessato

- ... ad ottenere:
 - Origine, finalità, logica
 - Estremi di titolare e responsabili
- ... a pretendere:
 - Aggiornamento, cancellazione, notifica di eventi
- ... a opporsi per:
 - Motivi legittimi, scopi commerciali, ...

artt.7; 8; 9 e 10

Definizioni

Classificazione dei dati

- **Dati personali**
 - **Dati identificativi** art.4 /b
 - **Dati sensibili** art.4 /d
 - **Dati giudiziari** art.4 /e

Definizioni

a) "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;

b) "dati identificativi",

- i dati personali che permettono l'identificazione diretta dell'interessato;

Definizioni

c) “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;

Definizioni

d) "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;

Definizioni

e) "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;

f) "diffusione",

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

Definizioni

Responsabilità: figure

- **Titolare del trattamento** [art.28](#)
 - Il legale rappresentante / La proprietà.
 - Destinatario originale delle norme.
- **Responsabile del trattamento** [art.29](#)
 - Persone fisiche o giuridiche delegate ad attività di scelta, gestione e controllo
- **Incaricati del trattamento** [art.30](#)
 - Chiunque, delegato, esegua attività che comportano l'accesso ai dati per scopi leciti

Figure coinvolte

Titolare: funzioni

- Decide di effettuare un trattamento e ne fissa gli obiettivi.
- Decide le modalità di svolgimento dei trattamenti di dati
- Sceglie gli adeguati sistemi di protezione dei dati e la loro conservazione

Figure coinvolte

Titolare: obblighi

- Notificare al Garante, ove necessario, l'inizio e lo svolgimento di qualsiasi trattamento
- Scegliere le modalità di raccolta e verificare i requisiti dei dati
- Accertare che l'interessato sia stato debitamente informato
- Richiedere, ove necessario, l'autorizzazione per il trattamento di dati sensibili
- Adottare le idonee misure di sicurezza
- Vigilare sulla corretta applicazione della legge da parte dei soggetti a ciò preposti
- Verificare le operazioni in caso di cessazione del trattamento
- **Risarcire i danni causati dal trattamento dati effettuato.**

Figure coinvolte

I responsabili del trattamento

- Le persone fisiche, le persone giuridiche, le pubbliche amministrazioni e qualsiasi altro ente, associazione od organismo proposti dal titolare al trattamento dei dati
- Figura facoltativa

Figure coinvolte

Gli incaricati

- Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile
- Non sono chiamati a rispondere in caso di controversia con l'interessato

Figure coinvolte



Consenso

Caratteristiche

- Libero
- Informativa esaustiva
- Per parte o tutto il trattamento
- Scritto

Consenso

Non richiesto per...

- Adempiere ad obblighi di legge
- Eseguire operazioni da obblighi contrattuali
- Proviene da elenchi o documenti pubblici
- Necessario per l'incolumità dell'interessato
- Necessario per investigazioni difensive
- ...
- Effettuato in conformità con le "autorizzazioni generali" emesse dal Garante

Sanzioni

VIOLAZIONI AMMINISTRATIVE

- OMISSIONI
- INOSSERVANZE LIEVI
- MANCATA PUBBLICAZIONE
- PROCEDIMENTI DI APPLICAZIONE

Sanzioni

ILLECITI PENALI

- TRATTAMENTO ILLECITO
- FALSITA' NELLE DICHIARAZIONI
- OMISSIONE MISURE DI SICUREZZA
- INOSSERVANZA DEI PROVVEDIMENTI DEL GARANTE

Sanzioni

Le sanzioni penali

- **Trattamento illecito dei dati**
 - Reclusione da sei mesi a tre anni
- **Falsità nelle notifiche**
 - Reclusione da sei mesi a tre anni
- **Inosservanza dei provvedimenti**
 - Reclusione da tre mesi a due anni
- **Entro 30 giorni**
- **Niente appello - Solo Cassazione**

Sanzioni

Misure di Sicurezza

- Chiunque, essendovi tenuto, omette di adottare le misure minime ... è punito con l'arresto sino a due anni o con l'ammenda da diecimila a cinquantamila euro.

(art.169)

- **Ravvedimento operoso (max 6 mesi) + ammenda di 12.500 €**

Sanzioni

DIRITTO AZIENDALE

- Rescissione di un rapporto di lavoro
- L'azienda ha diritto a rescindere il contratto di lavoro di un dipendente che, regolarmente informato, non ottemperi alle disposizioni di legge

Come comportarsi

- **Adempimenti di Legge (tutti)**
- **Adempimenti significativi**
 - Valutazione delle possibili conseguenze
- **Nessuna azione**
 - Valutazione delle possibili conseguenze

Come comportarsi



Come comportarsi

Azioni da intraprendere

- Definire un piano di attività
- Valutare l'impatto della legge sull'organizzazione dell'azienda
- Valutare l'impatto della legge sulle attività dell'azienda
- Definire i ruoli e le mansioni

Come comportarsi

Azioni da intraprendere

- Pianificare i punti ed i passaggi per la redazione del Documento Programmatico sulla Sicurezza
- Definire il programma periodico di adeguamento e revisione dei documenti
- Definire il programma periodico di formazione ed aggiornamento dei dipendenti

Come comportarsi

Area Informatica

- Descrizione del sistema informativo ed informatico Aziendale
- Criteri e procedure per la eventuale trasmissione dei dati
- Criteri e procedure per la salvaguardia ed archiviazione dei dati in forma elettronica
- Criteri di archiviazione fisica dei supporti
- Criteri di protezione da virus informatici (in entrata ed in uscita).

Come comportarsi

Struttura fisica

- Descrizione delle protezioni delle aree e dei locali (criteri tecnici ed organizzativi)
- Criteri di restrizione e controllo degli accessi
- Modalità di esecuzione delle misure minime di sicurezza

Come comportarsi

Informativa addetti

- **Struttura organizzativa e gerarchica**
- **Piano di formazione per gli incaricati del trattamento**
- **Programma di revisione ed adeguamento del documento**
- **Informativa su leggi, doveri, diritti, comportamenti**

Come comportarsi

Analisi dei dati (tipo)

- **Analisi del trattamento dei dati personali / riservati**
- **Analisi del trattamento dei dati sensibili / particolari**
- **Comunicazione di trattamento al Garante della Privacy**
- **Risposta entro 90 gg. / tacito assenso**

Come comportarsi

Analisi dei dati (utilizzo)

- Identificazione delle classi di rischio
- Analisi dei rischi e dei danni conseguenti
- Criteri e procedure per assicurare l'integrità dei dati

Indice articoli

- Obblighi [art.31](#)
- Misure minime da adottare [artt.33 e 58](#)
- Trattamento con e senza strumenti elettronici [artt.34 e 35](#)
- Modalità di notificazione [artt.37 e 38](#)
- Obblighi di comunicazione [art.39](#)
- Autorizzazioni [artt.40 e 41](#)

Documentazione

- Piano delle attività da intraprendere
- Stesura del Documento Programmatico sulla Sicurezza
- Scelta dell'eventuale software
- Scelta dei dispositivi di protezione
- Piano di istruzione del personale
- Monitoraggio del progetto

Attività

Operativa

- Installazione del software
- Installazione dei dispositivi
- Informativa diretta al personale
- Monitoraggio di sistemi, eventi, comunicazioni e rete (Auditing)

Auditing

- Attività dell'intero sistema
- Attività dei singoli utenti
 - Tempi di utilizzo
 - Percorsi di rete e collegamenti
 - Tipo di attività eseguita
 - Contenuti del traffico generato
 - Discrepanze con gli standard

CONCLUSIONI

Valore aggiunto ? Perché ?

Il garante pubblica già da mesi, nel Suo Sito WEB, un indice delle Aziende che hanno compilato la notifica di trattamento comprensivo dei riferimenti dei Titolari della Privacy .

E' l'avvio di una nuova certificazione ?

CONCLUSIONI

Chiunque intergisca con l'Azienda che può contare su tale “certificazione” sa di affidarsi ad una struttura organizzata che tutela la riservatezza delle informazioni affidatele.

L'Azienda che opera nel rispetto del D.L.196 si caute da azioni legali nei suoi confronti e diviene parte di una sorta di “catena della sicurezza”.