



Associazione Periti Industriali della provincia di Padova

Decreto Legislativo n. 196 30/6/2003

Codice in materia di protezione dei dati personali

Il trattamento delle informazioni nello studio professionale

27 gennaio 2006

per.ind. Attilio Rampazzo

Attilio Rampazzo

perito industriale
IT Security Consultant
BSI Certified Lead Auditor BS 7799/ISO 27001

- iscritto al Collegio Periti Industriali della prov. di Padova dal 1980
- associato all'Associazione Periti Industriali di Padova dal 1991
- associato A.N.I.P., AICQ TV, ISMS IUG
- membro gruppi di lavoro CNPI, AICQ TV, ISMS IUG

Trentennale esperienza settore IT

si occupa prevalentemente di :

Studio/Realizzazione di applicazioni gestionali su mainframe
System Integration e Assessment di Sistemi Informativi
Office Automation / Internet
Information Security

Decreto Legislativo n. 196 30/6/2003

Codice in materia di protezione dei dati personali



Evoluzione della normativa

- ✚ Disciplinata nel settore privato e pubblico dalla **Legge 675/96** e successive modificazione e integrazioni
- ✚ Disciplinata nel settore delle telecomunicazioni dal **D.Lgs. 171/98**
- ✚ Disciplinata nel settore delle comunicazioni elettroniche a livello europeo dalla **Direttiva 2002/58/CE**
- ✚ Integrata dal **DPR 318/99** per quanto attiene la previsione delle misure minime di sicurezza
- ✚ Recentemente unificata in **Codice in materia di protezione dai dati personali (D.Lgs.196/2003)** entrato in vigore il **1 gennaio del 2004**

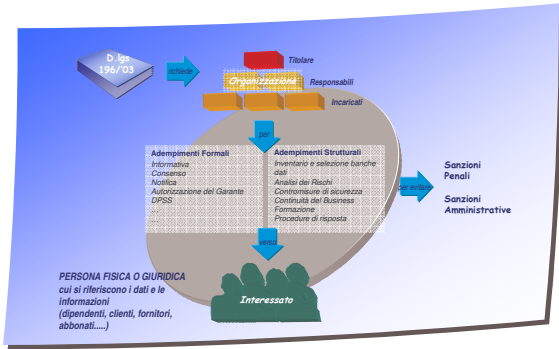
Il nuovo Codice sulla Privacy

- ✚ E' ispirato all'introduzione di maggiori garanzie nel trattamento dei dati personali
- ✚ Razionalizza e semplifica le norme già esistenti
- ✚ Contiene un generale riassetto della disciplina anche alla luce delle pronunce e dei pareri forniti nel corso di questi anni dal Garante in materia di protezione dei dati

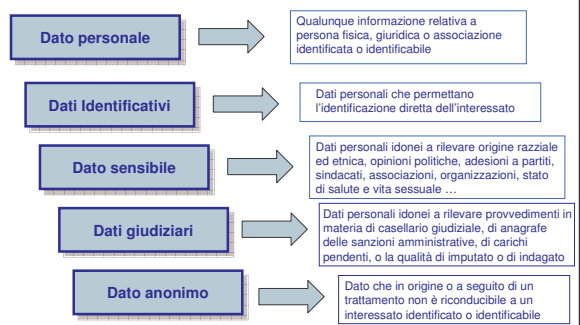
I destinatari della Normativa

- ✚ Il nuovo Codice sulla Privacy si applica a "chiunque tratti dati personali di terzi ... per finalità non personali", parliamo dunque di dati relativi a clienti, dipendenti, fornitori, utenti, cittadini, pazienti, colleghi, soci, associati etc ...
- ✚ Quindi sono interessati all'adeguamento:
 - ✚ tutte le imprese operanti nel settore privato
 - ✚ gli studi professionali
 - ✚ le pubbliche amministrazioni come comuni, ospedali, scuole, istituti universitari, etc ...
 - ✚ le associazioni
 - ✚ le cooperative
 - ✚ ...

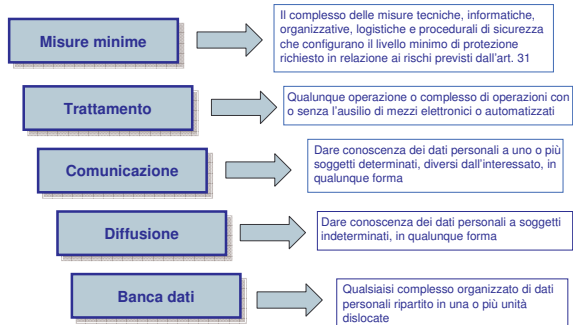
Uno sguardo allo schema di sintesi della legge 196/03 Codice in materia di protezione dei dati personali



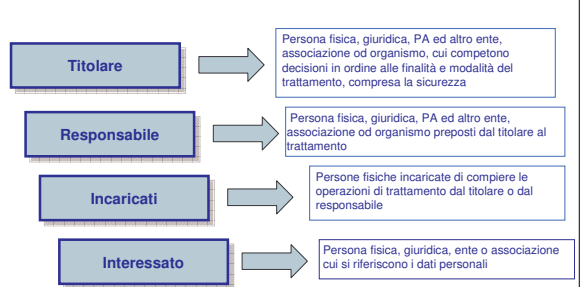
Le principali definizioni



Le principali definizioni



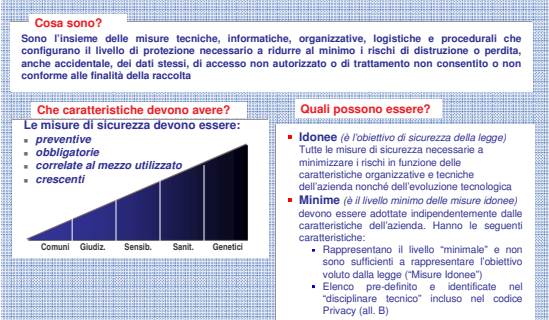
Le principali definizioni



Il legislatore pone la sicurezza come condizione fondamentale al trattamento di dati personali



Le misure di sicurezza previste dalla legge misure idonee e misure minime

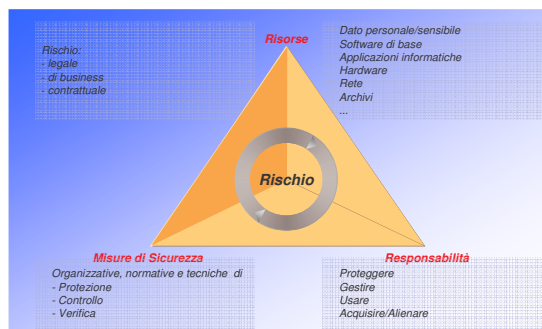


La corretta applicazione e gestione delle misure di sicurezza richiede il raggiungimento di specifici requisiti

La sicurezza delle informazioni permette di governare e proteggere il valore e i requisiti dei dati



La sicurezza dei dati personali riguarda le risorse da proteggere, le responsabilità da definire e si realizza attraverso il bilanciamento di interventi orientati al contenimento dei maggiori rischi...



Trattamento dei dati = attività pericolosa

Il trattamento è "un'attività pericolosa" (art. 2050 c.c.) e per i danni c'è l'inversione dell'onere della prova

Con l'applicazione dell'art. 2050 c.c. l'esclusione della responsabilità per violazione delle norme previste dal D.Lgs. 196/2003 si ottiene solo mediante la dimostrazione dell'avvenuta adozione di "tutte le misure idonee ad evitare il danno".

E' richiesto, quindi, un grado di diligenza molto più elevato.

Inoltre, con l'applicazione del "Codice sulla privacy" si verifica un'inversione dell'onere della prova e spetta al danneggiante (nella fattispecie il gestore del sistema informatico o titolare del trattamento) dimostrare che le cautele adottate risultano idonee, in relazione alle migliori tecniche messe a disposizione dallo sviluppo tecnologico del settore.

I principali adempimenti

- ✚ Nomina degli incaricati
- ✚ Nomina dei responsabili (facoltativa)
- ✚ Individuazione della tipologia di trattamenti effettuati
- ✚ Redazione della modulistica richiesta dalla legge (informativa, consenso)
- ✚ Elaborazione delle procedure di risposta alle richieste degli interessati e del Garante
- ✚ Individuazione ed implementazione delle misure idonee di sicurezza
- ✚ Implementazione delle misure minime di sicurezza
- ✚ Redazione del Documento Programmatico sulla Sicurezza
- ✚ Nei casi non espressamente esclusi dal Garante, notificazione del trattamento dei dati

Prossima Scadenza : 31 marzo 2006

- ✚ Implementazione delle misure minime di sicurezza – pena arresto fino a 2 anni del Titolare o pagamento di una somma da 10.000 a 50.000 euro
- ✚ Redazione del Documento Programmatico sulla Sicurezza – pena arresto fino a 2 anni del Titolare o pagamento di una somma da 10.000 a 50.000 euro
- ✚ Individuazione ed implementazione delle misure idonee di sicurezza
- ✚ Informativa agli interessati e raccolta consenso (quando dovuto) – pena pagamento di una somma da 3.000 a 18.000 euro in caso di trattamento di dati personali, e di una somma da 5.000 a 30.000 euro, (moltiplicabile per 3 a seconda delle condizioni economiche del contravventore), in caso di trattamento di dati sensibili o giudiziari

Obblighi generali di sicurezza (art. 31)

Custodia e controllo in modo da ridurre al minimo:
 distruzione e perdita dei dati anche accidentale
 accesso non autorizzato
 trattamento non consentito
 trattamento non conforme alle finalità della raccolta



Misure di sicurezza idonee

Obblighi specifici di sicurezza (art. 33)

Le misure minime di sicurezza

- Assicurano un livello minimo di protezione dei dati personali
- Sono obbligatorie, pena l'applicazione di sanzioni penali e amministrative
- Si applicano a tutte le tipologie di trattamento siano esse svolte nel settore privato che in quello pubblico
- Sono individuate rispettivamente per:
 - Trattamenti svolti con strumenti elettronici (art. 34)
 - Trattamenti svolti senza l'ausilio di strumenti elettronici (art. 35)

Misure Minime di Sicurezza

Trattamenti con strumenti elettronici (art. 34)

- Sistema di autenticazione informatica
- Procedure di gestione delle credenziali di autenticazione e sistema di autorizzazione
- Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito
- Misure di protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, ad accessi non autorizzati ed a determinati programmi informatici
- Procedure di Backup e procedure di Restore dei dati
- Piani di Business Continuity delle applicazioni / sistemi
- Documento Programmatico sulla Sicurezza (Piano della Sicurezza)

Misure di tutela e di garanzia

Il titolare che si avvale di soggetti esterni per l'installazione e l'adozione delle misure di sicurezza deve farsi rilasciare da questi una **descrizione scritta dell'intervento effettuato**



Attestato di *conformità* alle
Disposizioni del
Disciplinare Tecnico

Misure Minime di Sicurezza

Trattamenti con strumenti manuali (art. 35)

- Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- Previsione di procedure per una idonea custodia degli atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- Previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati

Domande

Grazie per l'attenzione

attilio@rampazzo.it