

DECRETO LEGISLATIVO

196/2003

“CODICE DELLA PRIVACY”

INDICE

1 - Struttura della normativa

2 - Glossario

- *soggetti che effettuano il trattamento*
- *tipologie di dati*
- *altri termini utilizzati di frequente*

3 - Gli adempimenti

- *elenco dei principali adempimenti*
- *semplificazioni normative introdotte dal Garante*

4 - Le sanzioni

- *sanzioni principali*

INDICE

5 - Riepilogo

- *riepilogo adempimenti*
- *riepilogo semplificazioni*

PARTE 1

Struttura della normativa

1 - STRUTTURA DELLA NORMATIVA

Il “Codice della Privacy” è costituito da 186 articoli:

Parte I - Disposizioni Generali

- *Principi generali*
- *Diritti dell'interessato (tra cui l'art. 7 “Diritto di accesso ai dati personali [...]”)*
- *Regole generali per il trattamento dati (informativa/consenso)*
- *Soggetti che effettuano il trattamento (titolare/responsabile/incaricato)*
- *Sicurezza dei dati e dei sistemi (Misure Minime/DPS)*
- *Adempimenti (Notificazione)*

Parte II - Disposizioni relative a specifici settori

- *Trattamenti in ambito giudiziario*
- *Trattamenti da parte di forze di Polizia*
- *Difesa e sicurezza dello Stato*
- *Trattamenti in ambito pubblico*
- *Trattamenti in ambito sanitario*

1 - STRUTTURA DELLA NORMATIVA

Parte III - Tutela dell'interessato e sanzioni

- *Forme di tutela (come rivolgersi al Garante)*
- *Sanzioni*

Sul sito del Garante è possibile scaricare in ogni momento il testo consolidato vigente della normativa (ad oggi circa 20 modifiche o integrazioni successive all'entrata in vigore).

1 - STRUTTURA DELLA NORMATIVA

Il Garante ha emesso alcune Autorizzazioni Generali....

- *n. 1: trattamento dati sensibili [...] **rapporto di lavoro***
- *n. 2: trattamento dati sensibili [...] stato di salute*
- *n. 3: trattamento dati sensibili [...] associazioni e fondazioni*
- *n. 4: trattamento dati sensibili [...] liberi professionisti*
- *n. 5: trattamento dati sensibili [...] banche, assicurazioni, ecc.*
- *n. 6: trattamento dati sensibili [...] investigatori privati*
- *n. 7: trattamento dati a carattere giudiziario*

Rinnovate periodicamente (oggi in scadenza al 30 giugno 2011)

7

1 - STRUTTURA DELLA NORMATIVA

Il Garante ha emesso numerosi Provvedimenti, suddivisi in oltre 30 materie, quali:

- *videosorveglianza*
- *recupero crediti*
- *conservazione dati traffico telefonico e telematico*
- *spam (fax, e-mail, SMS)*
- *condominio*
- *trasporto pubblico*
- *... e numerosi altri sui più diversi argomenti...*

1 - STRUTTURA DELLA NORMATIVA

Il Garante pubblica periodicamente provvedimenti relativi a:

- *fondatezza/infondatezza di ricorsi*
- *prescrizioni in merito a segnalazioni*

Dal 1997 il Garante predispone annualmente una **relazione al Parlamento** in cui descrive e riepiloga le attività svolte nell'esercizio precedente.

- *2009: non ancora pubblicata*
- *2008: 548 pagine*
- *2007: 460 pagine*
- *2006: 456 pagine*

1 - STRUTTURA DELLA NORMATIVA

Dal 1999 il Garante pubblica una Newsletter settimanale che contiene interpretazioni, pareri e novità.

A titolo esemplificativo, tra gli ultimi numeri:

11 gennaio 2010:

- **Illecite alcune foto di George Clooney** (*violare la riservatezza con foto di dimore private protette alla vista esterna*)
- **No a raccolte indiscriminate sull'HIV negli studi medici** (*il medico non può raccogliere informazioni sulla sieropositività di ogni paziente che si rivolge per la prima volta allo studio, se ciò non è indispensabile*)
- **Sfruttamento illecito dell'immagine: stop del Garante** (*non è possibile sfruttare commercialmente l'immagine di una persona, anche se nota, senza il suo consenso*)

1 - STRUTTURA DELLA NORMATIVA

10 dicembre 2009:

- **No al telemarketing con numeri casuali**
- **Riscossione: maggiori garanzie per i contribuenti**
- **Vigilanza più “vigilata” negli aeroporti** (autorizzazione a trattamento dati biometrici dei dipendenti di una ditta di vigilanza aeroportuale)

17 novembre 2009:

- **Stop a fax selvaggio** (nuovo intervento per combattere l'invio di pubblicità indesiderata via fax)
- **Lavoro: anonimato per la diagnosi HIV**
- **No ai dati sanitari sul sito del Comune** (indicazione stato di salute o indigenza nelle delibere consiliari in cui si concedono contributi sociali)
- **A Madrid fissati standard internazionali per la privacy**

1 - STRUTTURA DELLA NORMATIVA

Nel sito del Garante è possibile consultare ed accedere a:

- *normativa,*
- *provvedimenti,*
- *comunicati stampa,*
- *risposte ai quesiti più frequenti,*
- *newsletter*

www.garanteprivacy.it

PARTE 2

Glossario

2 - GLOSSARIO (Soggetti che effettuano il trattamento)

Garante (art. 4):

l'organo collegiale autonomo cui è riconosciuta l'autorità in materia di protezione dei dati personali (autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675).

- Presidente: Francesco Pizzetti
- Vice Presidente: Giuseppe Chiaravallotti
- Altri componenti: Mauro Paissan, Giuseppe Fortunato

Vengono eletti dal Parlamento. Rimangono in carica 7 anni con un mandato non rinnovabile.

2 - GLOSSARIO (Soggetti che effettuano il trattamento)

Interessato (art. 4):

la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

2 - GLOSSARIO (Soggetti che effettuano il trattamento)

Titolare (art. 4):

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;

2 - GLOSSARIO (Soggetti che effettuano il trattamento)

Titolare (art. 28):

1. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

E' il Titolare che pone cura ed attenzione alle fasi di selezione, designazione e controllo degli Amministratori di Sistema (ADS).

2 - GLOSSARIO (Soggetti che effettuano il trattamento)

Responsabile (art. 4):

la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

2 - GLOSSARIO (Soggetti che effettuano il trattamento)

Responsabile (art. 29):

1. Il responsabile è designato dal titolare facoltativamente.
2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.
4. **I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.**

2 - GLOSSARIO (Soggetti che effettuano il trattamento)

Incaricati (art. 4):

le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

2 - GLOSSARIO (Soggetti che effettuano il trattamento)

Incaricato (art. 30):

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

2. **La designazione è effettuata per iscritto** e individua puntualmente l'ambito del trattamento consentito.

Si considera tale anche la documentata preposizione della persona fisica ad una **unità** per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

2 - GLOSSARIO (Altri termini utilizzati di frequente)

Trattamento (art. 4):

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.

2 - GLOSSARIO (Tipologie di dati)

Dati personali (art. 4):

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;

2 - GLOSSARIO (Tipologie di dati)

Dati sensibili (art. 4):

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;

Alcune fonti tipiche di dati sensibili in azienda:

- buste paga (p.es. trattenute sindacali)
- fascicolo del dipendente (possibili dati inerenti la salute)
- curricula

2 - GLOSSARIO (Tipologie di dati)

Dati giudiziari (art. 4):

i dati personali idonei a rivelare provvedimenti [...] 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

PARTE 3

Gli adempimenti

3 - GLI ADEMPIMENTI

I principali adempimenti previsti dal D. Lgs. 196/2003 sono:

- Trattamento dei dati: INFORMATIVA e CONSENSO
- Soggetti che effettuano i trattamenti: NOMINE
- Misure Minime di Sicurezza (MMS)
- Documento Programmatico sulla Sicurezza (DPS)
- **Gestione Amministratori di Sistema**

3 - GLI ADEMPIMENTI (Informativa e consenso)

Informativa (art. 13):

L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati **oralmente o per iscritto** circa:

- a) finalità e modalità del trattamento cui sono destinati i dati;
- b) natura obbligatoria o facoltativa del conferimento dei dati;
- c) le conseguenze di un eventuale rifiuto di rispondere;
- d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati [...]
- e) i diritti di cui all'articolo 7 (accesso e correzione dati);
- f) gli estremi identificativi del titolare e del responsabile

3 - GLI ADEMPIMENTI (Informativa e consenso)

Informativa: SEMPLIFICAZIONI / 1

Per correnti finalità amministrative e contabili è possibile ed auspicabile:

- fornire un'unica informativa per tutti i trattamenti
- predisporre un'informativa con linguaggio semplice e non frammentata
- indicare le informazioni essenziali
- redigere una prima informativa breve, da integrarsi con una indicazione anche orale delle principali caratteristiche del trattamento
- rinviare ad un testo più completo ed articolato, facilmente accessibile (p.es. internet, intranet, bacheca, ecc.)

3 - GLI ADEMPIMENTI (Informativa e consenso)

Informativa: **SEMPLIFICAZIONI / 2**

- E' necessaria un'informativa *ad hoc* in caso di trattamenti particolari (p.es. dati genetici)

3 - GLI ADEMPIMENTI (Informativa e consenso)

Consenso (art. 23):

Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato, che può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.

Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

3 - GLI ADEMPIMENTI (Informativa e consenso)

Casi nei quali può essere effettuato il trattamento senza consenso (art. 24):

- è necessario per adempiere obblighi di legge
- è necessario per eseguire obblighi derivanti da un contratto
- riguarda dati provenienti da pubblici registri, elenchi, ecc.
- riguarda dati relativi allo svolgimento di attività economiche

3 - GLI ADEMPIMENTI (Informativa e consenso)

Tipici destinatari in ambito aziendale di informativa e consenso:

- Dipendenti (informativa)
- Collaboratori (informativa e consenso)
- Clienti e potenziali clienti (informativa e consenso^(*))
- Fornitori e potenziali fornitori (informativa)
- Offerte di collaborazione (informativa)

(*) salvo eccezioni, così come *descritte nel doc. web n. 1526724.*

3 - GLI ADEMPIMENTI (Informativa e consenso)

Consenso: SEMPLIFICAZIONI

Il consenso per attività di marketing può non rendersi necessario verso clienti cui si è già venduto un prodotto o prestato un servizio, a condizione che:

- il servizio proposto sia analogo a quello già venduto
- si interrompa immediatamente su richiesta dell'interessato

Il Garante raccomanda di NON chiedere il consenso se:

- il trattamento è svolto per obblighi contrattuali, precontrattuali, normativi o per finalità amministrative e contabili
- i dati provengono da pubblici registri o elenchi pubblici

3 - GLI ADEMPIMENTI (Nomine)

Obbligo di nomina scritta!

Come visto in precedenza, sia il **RESPONSABILE** che l'**INCARICATO** devono essere designati per iscritto.

3 - GLI ADEMPIMENTI (Nomine)

I contenuti di ciascuna nomina di incaricato:

- Lettera di nomina
- Descrizione dei trattamenti di pertinenza
- Copia Norme comportamentali:
 - trattamenti manuali
 - trattamenti con strumenti elettronici

SEMPLIFICAZIONI

In casi particolari, le istruzioni possono essere impartite oralmente con indicazioni semplici e di chiara formulazione.

3 - GLI ADEMPIMENTI (Misure Minime di Sicurezza)

E' obbligatorio adottare misure minime di protezione:

- Sistema di autenticazione (login e password)
- Aggiornamento periodico incaricati e addetti
- Protezione strumenti e dati (antivirus, firewall)
- Aggiornare strumenti di protezione (programmi e S.O.)
- Gestione del backup e ripristino dati
- Tenuta del Documento Programmatico sulla Sicurezza

SEMPLIFICAZIONI

In casi particolari sono concessi tempi più ampi per attività quali il cambio della password e l'esecuzione dei backup.

3 - GLI ADEMPIMENTI (DPS)

Struttura del documento:

- Descrizione del sistema informativo
- Elenco dei trattamenti di dati personali (informatici)
- Valutazione dei rischi
- Misure in essere e da adottare
- Backup e ripristino dei dati
- Identificazione nominativa degli ADS anche se appartenenti ad una struttura esterna (consulenti)

SEMPLIFICAZIONI

In casi particolari al posto del DPS è sufficiente una autodichiarazione o la redazione di un DPS semplificato.

3 - GLI ADEMPIMENTI (DPS)

Gestire gli Amministratori di Sistema in un DPS:

Il DPS dovrà essere integrato con gli estremi identificativi delle persone fisiche amministratori di sistema.

In attesa della sua riedizione (marzo 2010) può essere redatto un elenco da inserire in via temporanea. Esso deve comunque essere mantenuto **aggiornato** e disponibile in caso di accertamento da parte del Garante.

PARTE 4

Le sanzioni

4 - LE SANZIONI (ACCERTAMENTI E CONTROLLI)

Accertamenti (art. 157 e segg.)

- Il Garante può richiedere al Titolare, al Responsabile, all'interessato o a terzi di esibire documenti o fornire informazioni.
- Il Garante può disporre accessi a dati e verifiche a luoghi
- Controlli a cura di personale dell'Ufficio del Garante
- Il Garante può avvalersi anche di altri organi dello Stato

4 - LE SANZIONI (VIOLAZIONI AMMINISTRATIVE)

Omessa o inidonea informativa (art. 161):

- Da 6.000 a 36.000 euro di sanzione amministrativa

Altre fattispecie (art. 162):

- **Cessione di dati in violazione all'art. 16**
Da 10.000 a 60.000 euro di sanzione amministrativa
- **Violazione delle misure minime dell'art. 33**
Da 10.000 a 120.000 euro di sanzione amministrativa

4 - LE SANZIONI (ILLECITI PENALI)

Trattamento illecito dei dati:

- Da 6 a 18 mesi di reclusione (dati sensibili)

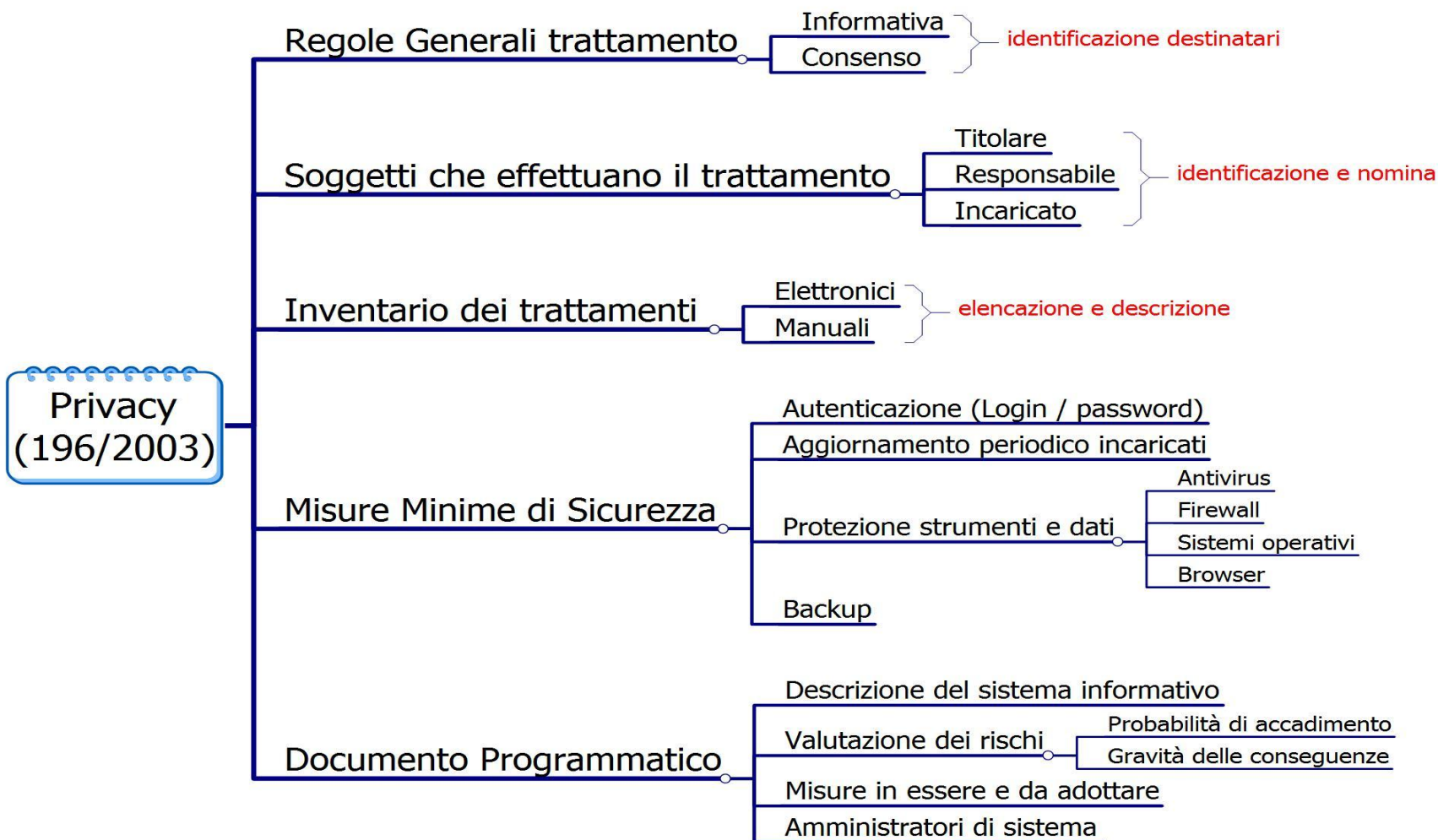
Omissione Misure Minime di Sicurezza:

- Fino a 2 anni di reclusione

PARTE 5

Riepilogo

5 - RIEPILOGO ADEMPIMENTI



5 - RIEPILOGO SEMPLIFICAZIONI

Doc Web
1526724

- 1 - Informativa Semplificazione e leggibilità
- 2 - Incaricati Designazione per unità operativa
- 3 - Notifica Non necessaria per finalità amm./cont
- 4 - Consenso Da non chiedere per obblighi contrattuali, finalità amministrative o dati da pubblici registri
- 5 - Marketing Si può fare senza consenso verso i clienti già in essere, per prodotti o servizi simili a quelli già venduti

5 - RIEPILOGO SEMPLIFICAZIONI

Doc Web
1571218

1. Semplificazione per

Trattamenti elettronici dati NON sensibili
Trattamenti elettronici dati sensibili (solo dipendenti e collaboratori)

2. Trattamenti elettronici

Istruzioni agli incaricati anche orali
Antivirus: aggiornamento annuale (biennale se non c'è internet)
Backup almeno mensile

3. DPS

Possibile autocertificazione per le aziende (1.)

4. Trattamenti manuali

Istruzioni agli incaricati anche orali
Istruzioni finalizzate al controllo ed alla custodia
Custodia dei documenti contenenti dati sensibili