



Manuale Informativo

Decreto Legislativo 30 giugno 2003, n. 196

“Codice in materia di protezione dei dati personali”

INDEX

- ***Il D.Lgs. 196/2003***
 - Termini e Fondamenti
- ***Gli attori***
 - Organizzazione e Responsabilità
- ***Gli interessati***
 - Diritti e Consenso
- ***Le Misure di sicurezza***
 - Trattamento con strumenti informatici
 - Trattamento senza strumenti informatici
- ***Il DPS***
 - Aspetti generali e Contenuti
- ***Illeciti e Sanzioni***
 - Sanzioni Amministrative e Sanzioni Penali
- **Allegato**

Il D. Lgs. 196/2003

Il Codice in materia di protezione dei dati personali, D. lgs. 196/2003, riunisce in un unico contesto tutta la normativa in tema di privacy: la l. 675/96 e gli altri decreti legislativi e regolamenti che si sono succeduti negli ultimi anni.

Il Codice può essere considerato l'insieme di regole per garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale

Che cos'è un dato personale?

I dati personali sono tutte le informazioni relative a:

- persone fisiche
- persone giuridiche
- enti e associazioni

che consentano l'identificazione diretta o indiretta di questi stessi soggetti

Si distinguono inoltre:

- **Dati sensibili:** dati idonei a rivelare razza, religione, opinioni politiche o filosofiche, salute, abitudini sessuali
- **Dati giudiziari:** dati idonei a rivelare provvedimenti iscritti nel casellario giudiziario o relativi a qualità di imputato o indagato

Il D.Lgs. 196/2003 - *Termini e fondamentali*

Cosa si intende per trattamento dei dati personali?

Qualunque operazione o complesso di operazioni effettuate anche senza l'ausilio di strumenti elettronici concernenti la:

- Raccolta
- Registrazione
- Organizzazione
- Conservazione
- Consultazione
- Elaborazione
- Modificazione
- Selezione
- Estrazione
- Raffronto
- Utilizzo
- Interconnessione
- Blocco
- Comunicazione
- Diffusione
- Cancellazione
- Distruzione dei dati se non registrati in una banca dati

Adempimenti

I dati personali, oggetto di trattamento, devono essere:

- trattati in modo lecito e secondo correttezza (INTEGRITA', RISERVATEZZA)
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini
- compatibili con tali scopi (RISERVATEZZA) esatti e, se necessario, aggiornati da chi autorizzato (INTEGRITA', RISERVATEZZA)
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati (INTEGRITA')
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati (INTEGRITA', RISERVATEZZA)
- verificabili dall'interessato (DISPONIBILITA').

Chi sono gli attori?

Titolare trattamenti

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.

Il Titolare al trattamento deve, tra l'altro, menzionare nella relazione accompagnatoria del Bilancio di esercizio la redazione del DPS.

Responsabile trattamenti

La nomina del responsabile è meramente facoltativa e compete al solo Titolare (art.29).

Inoltre se designato:

deve essere 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;

ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti;

i compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

Responsabile trattamenti

- Gestisce i trattamenti e obbligatoriamente, garantisce il rispetto dei requisiti di legge e della normativa interna (Regolamenti, Linee Guida)
- E' il referente per gli interessati nell'esercizio dei loro diritti
- Definisce l'organizzazione più idonea
- Nomina gli incaricati
- Garantisce la formazione degli incaricati
- Vigila sul trattamento effettuato dagli incaricati
- Garantisce l'aggiornamento dei trattamenti
- Informa tutti i dipendenti sulle policy privacy (es. Regolamento Sistemi Informatici, procedure, etc....)

Incaricato

La designazione degli incaricati (art 30):

- deve essere espressa e specifica;
- deve effettuarsi in ogni caso per iscritto e con riguardo a specifiche mansioni;
- può riguardare una persona fisica o una unità organizzativa per la quale sia individuato per iscritto l'ambito del trattamento consentito agli addetti ivi preposti.

I diritti dell'Interessato

Diritto di sapere se esistono o meno dati che lo riguardano ed ottenere l'indicazione:

- dell'origine dei dati personali;
- delle finalità e modalità del trattamento;
- della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- degli estremi identificativi del titolare, dei responsabili e del rappresentante;
- dei soggetti ai quali i dati personali possono essere comunicati di responsabili o incaricati.

Diritto di opporsi, in tutto o in parte, per motivi legittimi al trattamento dei dati personali che lo riguardano.

Informativa e consenso

(Artt. 13, 16, 23, 26)

Prima di procedere al trattamento dei dati personali è necessario fornire l'informativa privacy e richiedere il consenso ai soggetti interessati.

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'art. 13

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

Trattamento con e senza strumenti informatici

Misure minime di sicurezza (Art.31, Allegato B del D.lgs. 196/2003)

L'art. 31 prevede l'obbligo generale di ridurre al minimo i rischi di distruzione o dispersione dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Ciò è possibile custodendo e controllando i dati trattati anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento.

L'allegato B al codice distingue le misure minime di sicurezza a seconda che si tratti di:

- *Trattamenti con strumenti elettronici*
- *Trattamenti senza l'ausilio di strumenti elettronici*

Misure minime di sicurezza (Art.34, Allegato B del D.lgs. 196/2003)

Trattamento con l'ausilio di strumenti informatici:

- Autenticazione informatica
- Adozione di procedure di gestione delle credenziali di autenticazione
- Utilizzazione di un sistema di autorizzazione
- Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- Adozione di procedure per la custodia di copie di sicurezza
- Tenuta di un aggiornato Documento Programmatico sulla Sicurezza

Misure minime di sicurezza (Art.35, Allegato B del D.lgs. 196/2003)

Trattamento senza l'ausilio di strumenti informatici:

- Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati
- Previsione di procedure per un'idonea custodia degli atti e documenti affidati agli incaricati
- 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

Misure minime di sicurezza

L' Amministratore dei Sistemi Informativi ha come adempimenti:

- Gestione Profili e Password
- Gestione Backup, Ripristino e supporti rimuovibili
- Gestione Antivirus, patch e cifratura dati sensibili
- Conservazione Incarichi Fornitori
- Definizione, Eliminazione e Modifica trattamenti
- Mantenere le registrazioni di tutte le richieste utente, i backup

II DPS - *Aspetti generali e Contenuti*

Documento Programmatico sulla Sicurezza (DPS)

- Deve essere redatto da chi tratti dati sensibili e giudiziari con l'ausilio di strumenti informatici
- Elenca i rischi in materia di sicurezza e le contromisure da adottare
- Deve essere redatto entro il 31 marzo 2006
- Dovrà essere aggiornato dal Titolare, anche attraverso l'ausilio dei responsabili, entro il 31 marzo di ogni anno

Contenuto del DPS

- Elenco dei trattamenti dei dati personali
- Distribuzione dei compiti e responsabilità
- Misure per garantire integrità e disponibilità dei dati, protezione delle aree e locali
- Criteri e modalità per il recupero dei dati distrutti o danneggiati
- Previsione di interventi formativi per gli incaricati
- Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamento dati affidato all'esterno

Illeciti e Sanzioni - (Titolo III)

Le sanzioni previste dal D.lgs. 196/2003 sono distinte a seconda della tipologia di illecito:

Violazioni amministrative

- *Art. 161. Omessa o inidonea informativa all'interessato*
- *Art. 162. Altre fattispecie*
- *Art. 163. Omessa o incompleta notificazione*
- *Art. 164. Omessa informazione o esibizione al Garante*
- *Art. 165. Pubblicazione del provvedimento del Garante*

Illeciti penali

- *Art. 167. Trattamento illecito di dati*
- *Art. 168. Falsità nelle dichiarazioni e notificazioni al Garante*
- *Art. 169. Misure di sicurezza*
- *Art. 170. Inosservanza di provvedimenti del Garante*
- *Art. 171. Altre fattispecie*
- *Art. 172. Pene accessorie*

Illeciti e Sanzioni

A titolo esemplificativo si riportano di seguito le principali sanzioni per inadempimenti in materia di privacy:

TIPOLOGIA SANZIONE		SPECIFICHE
SANZIONI AdS	Codice Privacy	- Art. 162.2ter: Sanzione amministrativa introdotta a gennaio 2009 da 30 mila a 180 mila euro per semplice inosservanza. Riducibile 2/5; aumentabile x4 .Reato di omissione. - Art.167: <u>reclusione da 1 a 3 anni</u> se provocati danni per recare a sé profitto - Art 15: risarcimento danni, anche non patrimoniali, ai sensi dell’ art 2050 cc
	D.Lgs. 231/2001	Art 24 bis ha inserito i delitti informatici e il trattamento illecito dei dati tra i reati contemplati
	Sanzioni Accessorie	Esclusione gare/pubblicazione/immagine
SANZIONI PER INOSSERVANZA DEI PROVVEDIMENTI DEL GARANTE	Amministrativa pecuniaria	Sanzione da 30K a 180K€ per la semplice inosservanza di un Provvedimento Generale adottato ai sensi dell’art. 154 comma 1 – riducibile a 2/5, aumentabile x 4 – reato di omissione
	Penale	Reclusione da 3 mesi a 2 anni per inosservanza dei Provvedimenti dati sensibili o Provvedimento specifico adottato dal Garante ai sensi dell’art. 143; reclusione da 1 a 3 anni per trattamenti in violazione di quanto disposto ex. Art. 17, se provocati danni con dolo specifico
	Civile	Risarcimento danni, anche non patrimoniali, ai sensi dell’art. 2050 cc
SANZIONI RELATIVE ALLA SICUREZZA	Mancata adozione di misure minime (allegato B del Codice Privacy)	Sanzione penale/reato di omissione; risarcimento danno patrimoniale e non ex. Art. 2050 cc
	Mancata adozione misure idonee (non predefinite, a discrezione del Garante)	Risarcimento danno patrimoniale e non ex. Art. 2050 cc
	Mancata adozione misure “specifiche” richieste dal Garante	Sanzione amministrativa pecuniaria/ altro
ALTRE SANZIONI	PER OMESSA O INIDONEA INFORMATIVA – Sanzione Amministrativa	Pecuniaria da 6K a 36K€
	Per Trattamento di dati personali effettuato in violazione	- Sanzioni previste per violazione delle misure minime di sicurezza - Sanzioni previste per trattamento illecito - È altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento ad una somma da 10K a 120K€

Allegato: Presa Visione

(Deve essere fornita come ricevuta dall'incaricato, al Responsabile)

ALLEGATO 2

Ricevuta di avvenuta consegna della documentazione Privacy agli Incaricati del trattamento dei dati personali.

Io sottoscritto, in relazione alla mia nomina ad Incaricato del trattamento dei dati personali ai sensi del Codice Privacy (D.Lgs 196/03), dichiaro di aver ricevuto in data odierna la seguente documentazione:

- Lettera collettiva di nomina ad Incaricato;
- Informativa Privacy AM;
- Istruzioni per gli incaricati al Trattamento dei dati personali.

Luogo e data

.....

(firma dell'incaricato)

Il presente allegato dovrà essere compilato e fatto pervenire presso la sede centrale di Alliance Medical.