

# Principali adempimenti, responsabilità e sanzioni nel Codice della Privacy: stato dell'arte

**Dott. Massimo Farina**

[massimo@massimofarina.it](mailto:massimo@massimofarina.it)

<http://www.massimofarina.it>

**E-Academy, Milano, 22 Ottobre 2005**

- Principali Adempimenti D.lgs. 196/03
- Responsabilità
- Sanzioni
- Tutela

# Gli Adempimenti

Una possibile classificazione sugli obblighi gravanti in capo al titolare del trattamento potrebbe essere la seguente:



PRINCIPIO DI FINALITA'  
(ART. 11, COMMA 1, LETTERA B)

PRINCIPIO DI NECESSITA'  
(ART. 3)

PRINCIPIO DI PROPORZIONALITA'  
(ART. 11, COMMA 1, LETTERA D)

PRINCIPIO DI INDISPENSABILITA'  
(ART. 22, COMMA 3)

**Il termine entro cui adeguarsi alle *nuove* misure di sicurezza fu originariamente previsto per il 30 giugno 2004**



**TALE TERMINE È STATO PIÙ VOLTE PROROGATO**



**Attualmente il termine previsto è il 31 dicembre 2005**



**Si tratta della terza proroga**

## ATTENZIONE!!!!!!

**Molti adempimenti non sono mai stati prorogati**

### **art. 34 codice privacy**

a) autenticazione  
informatica → già previsto

b) adozione di  
procedure di gestione  
delle credenziali di  
autenticazione → novità

## art. 34 codice privacy

c) utilizzazione di  
un sistema di  
autorizzazione



già previsto

d) aggiornamento periodico  
dell'individuazione dell'ambito  
del trattamento consentito ai  
singoli incaricati e addetti alla  
gestione o alla manutenzione  
degli strumenti elettronici



novità

## art. 34 codice privacy

- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici → già previsto
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi → già previsto

## art. 34 codice privacy

g) tenuta di un aggiornato  
documento programmatico  
sulla sicurezza



novità

h) adozione di tecniche di  
cifratura o di codici  
identificativi per determinati  
trattamenti di dati idonei a  
rivelare lo stato di salute o la  
vita sessuale effettuati da  
organismi sanitari



già previsto

Notificazione

Richiesta di  
"Autorizzazione"  
per i trattamenti  
effettuati

**La “notificazione” è una dichiarazione attraverso la quale il Titolare comunica al Garante l’esistenza di un’attività di trattamento di dati personali**

IERI



obbligo di notificazione quasi generalizzato

OGGI



notevolmente ridimensionato l’obbligo di notificazione:  
articolo 37  
D.lgs. 196/03

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**

## IN QUALE MOMENTO SI PRESENTA LA NOTIFICAZIONE?

Attività di  
trattamento già  
cominciate prima  
del 1° gennaio  
2004



entro il 30 aprile 2004

Attività di trattamento  
successive 1° gennaio  
2004



prima che inizi il  
trattamento  
medesimo

Quante volte si notifica?

Una sola volta



È irrilevante il numero di  
trattamenti effettuati

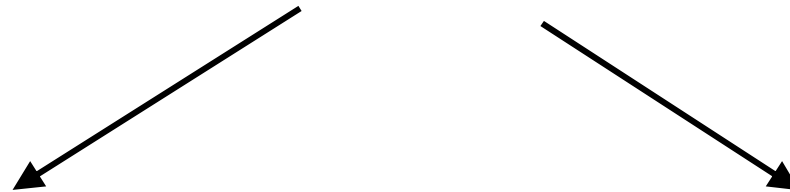
Come si notifica?

Esclusivamente per via  
telematica



Tramite il sito  
[www.garanteprivacy.it](http://www.garanteprivacy.it)

Quando va ripetuta?



**In caso di definitiva  
cessazione dell'attività  
di trattamento**

**In caso di modifiche  
agli elementi da  
indicare nella  
notificazione**

## In cosa consiste?

è un adempimento previsto per tutti i titolari che trattano dati sensibili e giudiziari

## PRECISAZIONE

Tenuto conto dell'altissimo numero di soggetti interessati, il legislatore ha previsto le “**Autorizzazioni Generali**” concesse a determinate categorie di titolari o di trattamenti

## AUTORIZZAZIONI GENERALI AL TRATTAMENTO DATI SENSIBILI

.Trattamento dati nei rapporti di lavoro

.Trattamento dati da parte di liberi professionisti

.Trattamento dati da parte di diverse categorie di titolari ( p. es. attività bancarie, creditizie, assicurative)

.Trattamento dati da parte di investigatori privati

.Trattamento dati da parte di organismi di tipo associativo e delle fondazioni

.Trattamento dati a carattere giudiziario da parte di privati, enti pubblici economici e di soggetti pubblici

Informativa

richiesta di  
consenso per il  
trattamento dati

**Prevista all'articolo 13 del Codice Privacy**



## **DEFINIZIONE**

**Si tratta di una comunicazione finalizzata ad informare l'interessato su:**



I soggetti che effettueranno il trattamento



La finalità del trattamento



La modalità del trattamento



I diritti dell'interessato

# Prevista all'articolo 23 del Codice Privacy

**Consenso scritto  
nell'ipotesi di  
trattamento di dati  
sensibili e giudiziari**

**Cosa significa  
consenso  
espreso?**

**Per i dati comuni,  
si richiede il  
consenso  
espreso**

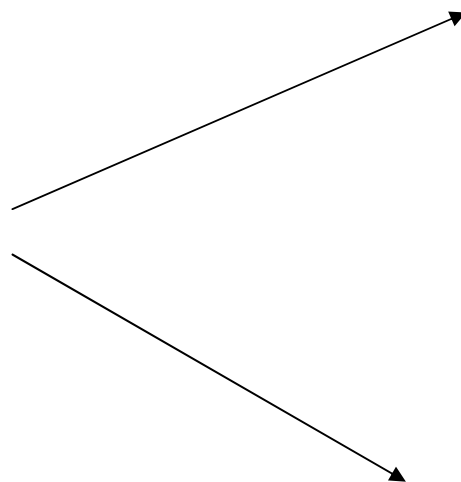
**Comma 3**

***“il consenso è  
validamente  
prestato solo se è  
[...] documentato  
per iscritto”;***

## Deroghe all'obbligo di consenso da parte dell'interessato

Artt. 24 e 26

**ALCUNI  
ESEMPI**



trattamento  
necessario per  
adempiere ad  
obblighi normativi

trattamento necessario  
per eseguire obblighi  
derivanti da un contratto  
del quale è parte  
l'interessato [...]

## Disciplinare Tecnico in materia di "Misure Minime di Sicurezza".

Previsti nell'Allegato B al D.lgs. 196/03



<b>Credenziali di autenticazione</b>	<ul style="list-style-type: none"><li>- USER ID</li><li>- PASSWORD</li></ul> <ol style="list-style-type: none"><li>1. almeno 8 caratteri,</li><li>2. non riconducibile al soggetto,</li><li>3. modificata dopo il primo utilizzo, ogni 6 o 3 mesi a seconda dei dati trattati</li></ol>	<p><b>NOVITA':</b></p> <p>↓</p> <p>caratteristiche della password</p>
--------------------------------------	---	---

## Gestione delle credenziali

### DISATTIVAZIONE PER:

1. non uso per almeno 6 mesi
2. perdita della qualità che permette l'accesso ai dati

### GARANTIRE

la disponibilità dei dati o degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che goda delle credenziali di autenticazione

### NOVITA':



*tali procedure sono previste indipendentemente dal tipo di dati trattati e dal tipo di accesso previsto per lo strumento elettronico*

<b>Sistema di autorizzazione</b> (se necessarie autorizzazioni diverse)	Verifica almeno annuale delle condizioni per l'autorizzazione	<b>NOVITA':</b> <i>Nella precedente disciplina era previsto solo per dati sensibili o giudiziari trattati con determinati strumenti elettronici</i>
<b>Protezione contro intrusioni esterne</b> ( p.es. antivirus)	Almeno ogni 6 mesi	

<b>Protezione interna del sistema</b>	<ul style="list-style-type: none"><li>•Annuale per i dati comuni</li><li>•Semestrale per i dati sensibili e giudiziari</li></ul>	<b>NOVITA':</b> <i>protezione interna da eventuali errori del sistema</i>
<b>Salvataggio dati e Ripristino all'accesso dati</b>	Back up (o disaster recovery) almeno settimanale  Ripartenza entro max 1 settimana	<b>NOVITA'</b>

**L'ADEMPIMENTO PIU' IMPORTANTE  
PREVISTO NEL  
CODICE E' IL D.P.S.  
(DOCUMENTO PROGRAMMATICO PER  
LA SICUREZZA)**

**Il DPS deve essere redatto o aggiornato, entro il 31 marzo di ogni anno, dal titolare del trattamento di dati sensibili o giudiziari, effettuato con strumenti elettronici.**

## QUALI INFORMAZIONI DEVE CONTENERE IL DPS?

➤ l'elenco dei trattamenti

➤ i compiti e le responsabilità dei soggetti incaricati al trattamento

➤ l'analisi dei rischi con l'indicazione delle misure che sono adottate al fine di garantire l'integrità e la disponibilità dei dati

➤ la protezione delle aree e dei locali in relazione alla loro custodia ed accessibilità

➤ l'analisi dei rischi con l'individuazione delle modalità che possono essere poste a favore del ripristino della disponibilità dei dati qualora si verificano episodi di distruzione o danneggiamento

➤ gli interventi formativi in tema di analisi dei rischi che incombono sui dati

➤ i criteri per l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura (outsourcing)

➤ criteri adottati per la separazione dei dati sensibili da quelli comuni.

## ULTERIORI MISURE IN CASO DI TRATTAMENTO DI DATI SENSIBILI O GIUDIZIARI

➤ Protezione contro l'accesso abusivo con strumenti hardware e software

➤ Ripristino della disponibilità dei dati entro sette giorni

➤ Attenta gestione dei supporti magnetici rimovibili

➤ Particolari misure fisiche e logiche di protezione per i dati genetici – cifratura –

**AVVISO!!!!!!**

**LA SICUREZZA  
TOTALE NON  
ESISTE:**

**INFORMAZIONE,  
AGGIORNAMENTO,  
PREVENZIONE**

## LE MISURE MINIME DISICUREZZA SONO PREVISTE ANCHE PER TRATTAMENTI EFFETTUATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

### Novità

➤ aggiornamento almeno annuale dell'ambito consentito all'incaricato per il trattamento

➤ i controllo e custodia di atti e documenti contenenti i dati personali fino al termine del trattamento e conseguente restituzione

➤ accesso controllato agli archivi per i dati sensibili o giudiziari

➤ fuori dall'orario di chiusura, individuazione e registrazione delle persone ammesse negli archivi

### Novità

➤ in caso di mancanza di vigilanza agli archivi, necessaria preventiva autorizzazione all'accesso

## Altri adempimenti interni (modulistica)

- **ATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO DATI**
- **ATTO DI NOMINA DELL'INCARICATO DEL TRATTAMENTO DATI**
- **ATTO DI NOMINA DELL'AMMINISTRATORE DEL SISTEMA INFORMATIVO**
- **ATTO DI NOMINA CUSTODE PAROLE CHIAVE**
- **MODULO COMUNICAZIONE PASSWORD**
- **DOCUMENTO PROGRAMMATICO PER LA SICUREZZA**

## IL CODICE PREVEDE TRE TIPI DI RESPONSABILITÀ:

➤ AMMINISTRATIVA

➤ CIVILE

➤ PENALE

## L'ORGANO COMPETENTE AD IRROGARE LE SANZIONI AMMINISTRATIVE È IL GARANTE

**art. 161 – OMESSA O INIDONEA  
INFORMATIVA ALL'INTERESSATO**

da 3.000 a  
18.000 euro  
SE  
RIGUARDA  
DATI  
COMUNI

SE RIGUARDA DATI SENSIBILI O  
GIUDIZIARI  
DA 5.000 A 30.000 EURO,  
MOLTIPLICABILE PER TRE IN  
RELAZIONE ALLE CONDIZIONI  
ECONOMICHE DEL  
CONTRAVVENTORE

da 5.000 a 30.000 euro se la cessione è verso altro titolare, purchè i dati siano destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti

**art. 162 – CESSIONE DI DATI  
IN VIOLAZIONE DEL CODICE**

da 500 a 3.000 euro se la cessione riguarda dati sanitari da parte di un esercente la professione sanitaria

art. 163 – Omessa o  
incompleta  
notificazione al  
garante



da 10.000 a 60.000 euro

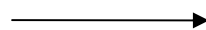
Art. 164 – Omesso invio  
di informazioni o  
documenti richiesti dal  
garante



da 4.000 a 24.000  
euro

L'illecito civile è disciplinato nell'art. 15 che assimila l'attività di trattamento di dati tra quelle pericolose ai sensi dell'art. 2050 c.c.

**Art. 167 –  
TRATTAMENTO  
ILLECITO DI DATI  
PERSONALI**



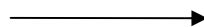
reclusione da 6 mesi  
a 3 anni

**Art. 168 – FALSITÀ NELLE  
DICHIARAZIONI E  
NOTIFICAZIONI AL  
GARANTE**



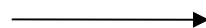
reclusione da 6 mesi  
a 3 anni

**OMISSIONE DI ADOZIONE  
DELLE MISURE MINIME DI  
SICUREZZA, SALVO IL  
C.D. RAVVEDIMENTO  
OPEROSO DI CUI  
ALL'ART. 169, COMMA 2**



arresto fino a 2 anni o  
ammenda da 10.000  
a 50.000 euro

**Art. 170 –  
INOSSERVANZA DEI  
PROVVEDIMENTI DEL  
GARANTE**



reclusione da 3 mesi  
a 2 anni

# Forme di tutela per l'interessato

TUTELA GIURISDIZIONALE

TUTELA AMMINISTRATIVA

GIUDICE ORDINARIO

GARANTE

**PRECISAZIONE**



**Per il risarcimento dei  
danni l'unica forma di tutela  
ammessa è quella davanti  
al Giudice Ordinario**

*Grazie per l'attenzione*

massimo@massimofarina.it

<http://www.massimofarina.it>

**E-Academy, Milano, 22 Ottobre 2005**

## Attribuzione - Non Commerciale - Condividi allo stesso modo 2.5

Tu sei libero:

- di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire o recitare l'opera
- di creare opere derivate
- Alle seguenti condizioni:
  - Attribuzione. Devi riconoscere il contributo dell'autore originario.
  - Non commerciale. Non puoi usare quest'opera per scopi commerciali.
  - Condividi allo stesso modo. Se alteri, trasformi o sviluppi quest'opera, puoi distribuire l'opera risultante solo per mezzo di una licenza identica a questa.
- In occasione di ogni atto di riutilizzo o distribuzione, devi chiarire agli altri i termini della licenza di quest'opera.
- Se ottieni il permesso dal titolare del diritto d'autore, è possibile rinunciare ad ognuna di queste condizioni.
- Le tue utilizzazioni libere e gli altri diritti non sono in nessun modo limitati da quanto sopra