

## La nuova disciplina in materia di tutela della privacy (D.Lgs. 30.6.2003 n. 196)

### Principali novità

#### INDICE

1	<b>Il nuovo Codice sulla privacy</b> .....	2
2	<b>Ambito di applicazione</b> .....	2
3	<b>Soggetti coinvolti dal trattamento dei dati personali</b> .....	2
3.1	<i>L'interessato</i> .....	2
3.2	<i>Il titolare</i> .....	2
3.3	<i>Il responsabile</i> .....	2
3.4	<i>Gli incaricati</i> .....	2
4	<b>La notificazione al Garante</b> .....	3
4.1	<i>Le modalità di effettuazione della notificazione</i> .....	3
4.2	<i>Il termine di effettuazione della notificazione</i> .....	3
4.3	<i>La variazione dei dati e la cessazione del trattamento</i> .....	3
4.4	<i>Disciplina transitoria</i> .....	3
5	<b>Gli obblighi relativi alla raccolta e al trattamento dei dati personali</b> .....	3
5.1	<i>L'informativa all'interessato</i> .....	3
5.2	<i>Il consenso dell'interessato</i> .....	4
5.3	<i>Il trattamento dei "dati sensibili" e giudiziari</i> .....	4
6	<b>Le misure di sicurezza nel trattamento dei dati personali</b> .....	5
6.1	<i>Le misure "minime" di sicurezza per i trattamenti di dati personali mediante strumenti elettronici</i> .....	5
6.2	<i>Le misure "minime" di sicurezza per i trattamenti di dati personali senza strumenti elettronici</i> .....	5

10.06.2004



## **1 IL NUOVO CODICE SULLA PRIVACY**

L'**1.1.2004** è entrato in vigore il DLgs. 30.6.2003 n. 196, che costituisce il nuovo Codice in materia di protezione dei dati personali (c.d. "Codice della privacy").

Il Codice raccoglie e riorganizza la disciplina in materia di tutela della privacy emanata a partire dalla L. 31.12.96 n. 675, entrata in vigore l'8.5.97.

Di seguito si riepilogano sinteticamente i principali aspetti della nuova disciplina.

## **2 AMBITO DI APPLICAZIONE**

La disciplina di tutela della privacy si applica al trattamento di dati personali effettuati:

- **da chiunque** (es. società di persone o di capitali, imprenditori individuali, professionisti, enti e associazioni no-profit, altri soggetti sia privati che pubblici);
- **con qualunque mezzo**, quindi sia con strumenti elettronici (es. computer) che in modo manuale con riferimento ad archivi cartacei;
- **nel territorio italiano**, o in un luogo comunque soggetto alla sovranità italiana (es. navi e aerei), anche se i dati personali sono detenuti all'estero;
- da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea ed impiega, per il trattamento dei dati, **strumenti situati nel territorio italiano** anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito dei dati nel territorio dell'Unione europea; in tal caso occorre designare un rappresentante in Italia.

## **3 SOGGETTI COINVOLTI DAL TRATTAMENTO DEI DATI PERSONALI**

Il Codice della privacy definisce e disciplina i soggetti coinvolti nel trattamento di dati personali.

### **3.1 L'INTERESSATO**

L'**interessato** è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

### **3.2 IL TITOLARE**

Il **titolare** è 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.

In caso di società o enti, "titolare del trattamento" è la società o ente nel suo complesso, il quale ovviamente opererà mediante le persone fisiche che rivestono le funzioni di amministrazione e rappresentanza.

### **3.3 IL RESPONSABILE**

Il **responsabile** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

I responsabili possono essere più di uno e devono essere individuati tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia, compreso il profilo relativo alla sicurezza.

I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare, il quale vigila sulla puntuale osservanza delle disposizioni di legge e delle istruzioni impartite, anche tramite verifiche periodiche.

### **3.4 GLI INCARICATI**

Gli **incaricati** sono le persone fisiche autorizzate dal titolare o dal responsabile a compiere operazioni di trattamento di dati personali.

In pratica, si tratta delle persone fisiche addette ai terminali e agli archivi che, materialmente, si occupano delle fasi di raccolta, gestione, elaborazione e conservazione dei dati personali, le quali operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

La designazione degli incaricati è effettuata per iscritto, individuando puntualmente l'ambito del trattamento di dati consentito.

#### **4 LA NOTIFICAZIONE AL GARANTE**

Il nuovo Codice prevede che l'obbligo di notificazione al Garante ricorra solo più se il trattamento riguarda:

- dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- 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;
- 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;
- 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;
- 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;
- 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.

Il Garante ha annunciato chiarimenti in relazione alla nuova disciplina della notificazione.

##### **4.1 LE MODALITÀ DI EFFETTUAZIONE DELLA NOTIFICAZIONE**

La notificazione deve essere effettuata esclusivamente mediante trasmissione in via telematica, con utilizzo della firma digitale e dei modelli approvati dal Garante.

Se il titolare non possiede una firma digitale, è possibile avvalersi di intermediari autorizzati dal Garante (es. uffici postali).

Per ulteriori informazioni si consiglia di consultare il sito internet del Garante ([www.garanteprivacy.it](http://www.garanteprivacy.it)).

##### **4.2 IL TERMINE DI EFFETTUAZIONE DELLA NOTIFICAZIONE**

La notificazione del trattamento deve essere effettuata al Garante **prima dell'inizio** del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate.

##### **4.3 LA VARIAZIONE DEI DATI E LA CESSAZIONE DEL TRATTAMENTO**

Una nuova notificazione al Garante deve essere effettuata in caso di:

- mutamento di taluno degli elementi da indicare nella notificazione medesima (es. ragione o denominazione sociale del titolare o della relativa sede, nomina, revoca o variazione del responsabile precedentemente indicato, ecc.);
- cessazione del trattamento.

La notificazione deve avvenire **anteriamente** alla variazione o alla cessazione del trattamento.

##### **4.4 DISCIPLINA TRANSITORIA**

In via transitoria, per i trattamenti di dati personali iniziati prima dell'1.1.2004 e che rientrano nelle suddette categorie per le quali è rimasto l'obbligo di notificazione, la notificazione stessa deve essere effettuata entro il **30.4.2004**, utilizzando i nuovi modelli e le nuove modalità.

#### **5 GLI OBBLIGHI RELATIVI ALLA RACCOLTA E AL TRATTAMENTO DEI DATI PERSONALI**

Il Codice conferma gli obblighi che erano previsti in relazione alla raccolta e al trattamento dei dati personali.

##### **5.1 L'INFORMATIVA ALL'INTERESSATO**

L'interessato o la persona presso la quale sono raccolti i dati personali devono continuare ad essere preventivamente informati, oralmente o per iscritto, circa:

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- i diritti spettanti all'interessato (es. ottenere l'aggiornamento, la rettifica o la cancellazione dei dati, di opporsi al loro trattamento, specie a fini pubblicitari, di vendita o di ricerche di mercato);
- gli estremi identificativi del titolare e, se designati, del suo rappresentante in Italia e di almeno un responsabile.

## **5.2 IL CONSENSO DELL'INTERESSATO**

Il trattamento di dati personali richiede il consenso espresso dell'interessato, documentato per iscritto, ad eccezione, ad esempio:

- dei dati raccolti e detenuti in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- dei trattamenti necessari per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
- dei dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;
- dei dati relativi allo svolgimento di attività economiche, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
- dei trattamenti necessari per far valere o difendere un diritto in sede giudiziaria;
- dei trattamenti effettuati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, con esclusione della comunicazione all'esterno e della diffusione.

## **5.3 IL TRATTAMENTO DEI "DATI SENSIBILI" E GIUDIZIARI**

Per il trattamento dei "dati sensibili" (es. relativi alla salute, alla vita sessuale, alle opinioni religiose, politiche, sindacali o filosofiche, all'origine etnica, ecc.) continuano ad essere necessari:

- il consenso scritto dell'interessato;
- l'autorizzazione del Garante.

I dati giudiziari (es. atti relativi alle indagini, richieste di rinvio a giudizio, sentenze definitive di condanna, "patteggiamenti", provvedimenti di sospensione condizionale della pena, di non menzione, di applicazione di pene accessorie, di misure alternative alla detenzione, di misure di sicurezza personali e patrimoniali, ecc.) possono essere trattati solo se autorizzati da un'espressa disposizione di legge o da un provvedimento del Garante.

### **Le "autorizzazioni standard" del Garante**

Fino al **30.6.2004** continuano ad applicarsi le seguenti "autorizzazioni standard" del Garante relative al trattamento dei:

- "dati sensibili" nell'ambito di rapporti di lavoro;
- dati relativi allo stato di salute e alla vita sessuale;
- "dati sensibili" da parte degli organismi di tipo associativo e delle fondazioni;
- "dati sensibili" da parte dei liberi professionisti;
- "dati sensibili" da parte di banche, assicurazioni, SIM, imprese turistiche, di elaborazione dati, di sondaggi di opinione e ricerche di mercato, di ricerca e selezione del personale, di agenzie matrimoniali, ecc.;
- "dati sensibili" da parte degli investigatori privati;
- dati di carattere giudiziario.

I soggetti che trattano i "dati sensibili" nel rispetto di quanto indicato nelle "autorizzazioni standard" sono esonerati dal richiedere al Garante un'autorizzazione individuale.



## **6 LE MISURE DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI**

L'aspetto che ha subito le maggiori innovazioni a seguito dell'entrata in vigore del Codice della privacy riguarda la disciplina delle misure minime di sicurezza, la cui mancata adozione è sanzionata penalmente.

Le misure di sicurezza perseguono l'obiettivo di ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale, dei dati;
- accesso non autorizzato;
- trattamento non consentito o non conforme alle finalità della raccolta.

Le nuove misure minime di sicurezza sono differenziate solo più a seconda che il trattamento dei dati personali avvenga o meno mediante strumenti elettronici (es. computer).

### **6.1 LE MISURE "MINIME" DI SICUREZZA PER I TRATTAMENTI DI DATI PERSONALI MEDIANTE STRUMENTI ELETTRONICI**

In estrema sintesi, il trattamento di dati personali effettuato con strumenti elettronici richiede l'adozione delle seguenti misure minime di sicurezza:

- individuare per ciascun incaricato, o addetto alla gestione o manutenzione degli elaboratori, i dati e i trattamenti cui possono accedere; tali procedure devono essere aggiornate almeno una volta all'anno;
- attribuire ad ogni incaricato un codice identificativo (es. login, PIN, username) e una password con almeno otto caratteri (o, se inferiore, con il numero massimo consentito dallo strumento elettronico); la password non deve contenere riferimenti agevolmente riconducibili all'incaricato e deve essere sostituita ogni sei mesi;
- disattivare gli accessi ai dati personali nei confronti dei soggetti non più incaricati;
- proteggere gli strumenti elettronici e i dati rispetto ad accessi non consentiti e a trattamenti illeciti;
- aggiornare i programmi informatici ogni anno
- aggiornare i programmi antivirus ogni sei mesi;
- procedere al back-up dei dati almeno settimanalmente e stabilire procedure per la custodia delle copie di sicurezza;
- farsi rilasciare la certificazione di conformità, per gli interventi di adozione delle misure minime di sicurezza effettuati da soggetti esterni.

#### *Trattamenti di dati "sensibili" o giudiziari*

In caso di trattamenti di dati "sensibili" o giudiziari occorre altresì:

- aggiornare la password ogni tre mesi;
- aggiornare i programmi informatici ogni sei mesi;
- proteggere i dati contro l'accesso abusivo mediante idonei strumenti elettronici;
- dare istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili (es. floppy, cartucce, ecc.) su cui sono memorizzati i dati;
- adottare misure in caso di danneggiamento dei dati e degli strumenti elettronici;
- predisporre annualmente il documento programmatico sulla sicurezza (DPS).

### **6.2 LE MISURE "MINIME" DI SICUREZZA PER I TRATTAMENTI DI DATI PERSONALI SENZA STRUMENTI ELETTRONICI**

Qualora il trattamento di dati personali sia effettuato senza l'ausilio di strumenti elettronici (es. archivi cartacei), occorre adottare le seguenti misure minime di sicurezza:

- individuare i trattamenti consentiti ai singoli incaricati e procedere al loro aggiornamento almeno una volta all'anno;
- dare istruzioni scritte per il controllo e la custodia degli atti e dei documenti contenenti dati personali; gli atti e i documenti contenenti dati personali "sensibili" o giudiziari devono essere custoditi in modo tale che ad essi non accedano persone prive di autorizzazione;
- controllare l'accesso agli archivi contenenti dati personali "sensibili" o giudiziari; le persone ammesse a qualunque titolo dopo l'orario di chiusura devono essere identificate e registrate; se gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati di vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.