

# Il nuovo Codice sulla protezione dei dati personali

Con la data del 1° gennaio 2004 è entrato in vigore il cosiddetto “Testo Unico sulla Privacy”, ovvero il Codice che raccoglie le disposizioni in materia di protezione dei dati personali (D.Lgs. 30 giugno 2003, n. 196). Il Codice, che contiene molte conferme, ma anche alcune importanti novità, trae origine dalla Legge 31 dicembre 1996, n. 675, che introdusse nel panorama nazionale la tutela della *privacy*, in attuazione di direttive comunitarie, per soddisfare l’esigenza di regolamentare il diritto alla riservatezza dei dati personali delle persone fisiche e giuridiche, di enti ed associazioni, con il riconoscimento giuridico che il trattamento dei dati personali è lecito nel rispetto di una serie di adempimenti formali volti a tutelare la persona rispetto all’intrusione di un terzo nella sua vita privata.

<p><b>Principi fondamentali</b></p>	<p><b>il diritto alla protezione:</b> viene affermato il principio per cui chiunque ha diritto alla tutela dei dati personali che lo riguardano;</p> <p><b>le finalità:</b> il Codice garantisce che il trattamento di dati si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell’interessato, assicurando un elevato livello di protezione, nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio;</p> <p><b>la necessità del trattamento dei dati:</b> viene sancito che i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l’utilizzo di dati personali ed identificativi, escludendone addirittura il trattamento laddove sia possibile l’utilizzo di dati anonimi o che permettano l’identificazione solo in caso di necessità.</p>
<p><b>Definizioni principali e soggetti interessati</b></p>	<p><b>trattamento:</b> è tale, secondo la norma, qualunque operazione o complesso di operazioni, svolte con o senza l’ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l’organizzazione, la conservazione, 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;</p> <p><b>dati:</b> possono essere “personali” (qualunque informazione relativa a persona fisica, giuridica, ente o associazione, identificati o identificabili anche indirettamente, compresi i numeri di identificazione personale), “identificativi” (sono i dati personali che consentono l’identificazione diretta dell’interessato, “sensibili” (quelli idonei a rivelare l’origine etnica e razziale, le convinzioni religiose, politiche, filosofiche, l’appartenenza a partiti e sindacati, nonché quelli idonei a rivelare lo stato di salute e la vita sessuale), e infine “giudiziari” (i dati personali in materia di casellario giudiziale, di anagrafe delle sanzioni dipendenti da reato e in genere le questioni attinenti alla giustizia civile e penale);</p>

	<p><b>Garante:</b> è l'autorità istituita per il controllo e la tutela della <i>privacy</i>, ed opera in piena autonomia e con indipendenza di giudizio e di valutazione.</p> <p>il <b>titolare</b> del trattamento, che è sempre indispensabile, è il soggetto su cui gravano tutti i principali obblighi previsti dalla normativa, tra cui gli obblighi relativi alla notificazione, se necessaria, al rilascio dell'informativa, alla richiesta del consenso, alla richiesta di autorizzazione preventiva al Garante per i dati sensibili, all'adozione delle misure di sicurezza. Solitamente si identifica nel titolare dello studio o dell'azienda;</p> <p>il <b>responsabile</b> del trattamento, ovvero il soggetto preposto dal titolare al trattamento dei dati personali. Può o meno esistere nell'ambito dell'azienda, e più grande è la dimensione della stessa, maggiore sarà la necessità di nominare uno o più responsabili. Il responsabile, se esiste, deve procedere al trattamento dei dati personali attenendosi alle istruzioni impartite per iscritto dal titolare. La nomina, sebbene sia facoltativa, risulta in realtà opportuna, se non necessaria, sotto il profilo organizzativo, costituendo tra l'altro presupposto per la corretta applicazione delle misure minime di sicurezza, come meglio evidenziato in seguito;</p> <p>gli <b>incaricati</b> del trattamento, che sono i soggetti che elaborano i dati personali cui hanno accesso, attenendosi alle istruzioni del titolare o del responsabile, sotto la loro diretta autorità.</p>
<p style="text-align: center;"><b>Informativa</b></p>	<p>L'informativa costituisce un elemento imprescindibile della tutela della <i>privacy</i>, nel senso che è sempre dovuta. Essa può anche essere fornita verbalmente, ma ciò comporta evidenti svantaggi al momento di dover eventualmente provare il corretto comportamento del titolare. Costui, tramite l'informativa, fornirà all'interessato le finalità e le modalità del trattamento, il fatto che il conferimento dei dati sia obbligatorio o facoltativo, le conseguenze del mancato conferimento, i soggetti cui i dati potranno essere comunicati o che possono venire a conoscenza in qualità di responsabili o incaricati, i diritti riconosciuti all'interessato, l'identificazione del titolare e, se nominato, del responsabile del trattamento.</p> <p>Si sottolinea che l'informativa è sempre dovuta, anche quando non è necessario il consenso espresso dell'interessato. Ciò avviene quando, per esempio, il titolare:</p> <ul style="list-style-type: none"> <li>tratta dati non sensibili per adempiere ad obblighi contrattuali;</li> <li>tratta dati non sensibili su specifiche richieste del cliente;</li> <li>tratta dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque.</li> </ul>
<p style="text-align: center;"><b>Consenso</b></p>	<p>Nel caso invece di trattamento di dati <b>sensibili</b>, il titolare deve sempre ottenere il consenso preventivo dell'interessato, oltre che l'autorizzazione del Garante, salvo particolari casi di esclusione disciplinati dalla norma.</p>
<p style="text-align: center;"><b>Autorizzazioni del</b></p>	<p>Al fine di agevolare gli adempimenti dei soggetti obbligati, il</p>

<p><b>Garante</b></p>	<p>Garante nel passato ha fornito delle autorizzazioni di carattere generale, tra cui una specifica per i professionisti (la n. 4), secondo lo schema che segue:</p> <ol style="list-style-type: none"> <li>1 – Datori di lavoro</li> <li>2 – Operatori che trattano dati sulla salute</li> <li>3 – Organismi di tipo associativo e fondazioni</li> <li>4 – Liberi professionisti</li> <li>5 – Banche, assicurazioni, chi svolge attività di ricerche personale, sondaggi, elaborazione dati</li> <li>6 – Investigatori privati</li> <li>7 – Soggetti che trattano dati di carattere giudiziario</li> </ol>
<p><b>Notificazione</b></p>	<p>La notificazione consiste in un modello, contenente tutta una serie di dati, tra cui quelli relativi ai trattamenti effettuati, alle modalità e alle finalità del trattamento, alle misure di sicurezza adottate, da inviare telematicamente al Garante prima dell’inizio del trattamento, ed una sola volta a prescindere dal numero delle operazioni e della durata del trattamento. Per i trattamenti già iniziati alla data di entrata in vigore del Codice, la scadenza è stata fissata al 30 aprile.</p> <p>Contrariamente a quanto avveniva in passato, il titolare deve ora procedere ad inviare la notificazione solo nei casi previsti dalla norma (art. 37), vale a dire quando il trattamento riguarda, principalmente, dati relativi alla salute, alla sfera sessuale o psichica, dati volti a definire il profilo o la personalità, dati a fini della selezione del personale per conto terzi, dati relativi a sondaggi di opinione e ricerche di mercato, dati relativi alla solvibilità economica o alla situazione patrimoniale degli interessati. In sostanza, ora sono ben più rari i casi in cui è necessario provvedere a tale adempimento.</p>
<p><b>Misure minime di sicurezza</b></p>	<p>Il nuovo Codice riscrive (artt. 33-36 e Allegato B) integralmente le disposizioni in tema di sicurezza, in sostituzione di quanto in precedenza previsto dal Dpr 318/99.</p> <p>Le misure minime di sicurezza, si ricorda, riguardano tanto i trattamenti effettuati con mezzi elettronici tanto quelli non elettronici.</p> <p>La logica di fondo della norma, per quanto attiene alla sicurezza, è quella secondo cui i dati personali devono essere custoditi e controllati in modo da ridurre ad un ragionevole margine il rischio di sottrazione o perdita degli stessi, nonché di accessi non autorizzati da parte di terzi, evitando inoltre il trattamento di dati consentito e conforme.</p> <p>Per fare ciò, quando il trattamento è effettuato con mezzi elettronici, è richiesto un sistema di autenticazione informatica: in pratica ciascun incaricato deve essere dotato di “credenziali di autenticazione” che consentano il superamento di una procedura di autenticazione attraverso l’identificazione dell’incaricato medesimo. Le credenziali possono consistere in strumenti quali</p>

	<p>smart card o dispositivi biometrici, ma molto più comunemente consisteranno in codici identificativi associati a password, aventi le caratteristiche illustrate nel riquadro che segue.</p> <p>Altre misure di sicurezza riguardano:</p> <p>la necessità di impartire adeguate istruzioni sull'utilizzo degli strumenti informatici, a cura del titolare o del responsabile, che hanno anche l'obbligo di controllare e gestire le credenziali di autenticazione;</p> <p>l'adozione di strumenti anti-virus, da aggiornare almeno semestralmente;</p> <p>l'effettuazione degli aggiornamenti dei programmi, per prevenire la vulnerabilità degli strumenti elettronici e correggerne i difetti, da effettuarsi almeno annualmente (semestralmente per i trattamenti di dati sensibili);</p> <p>la necessità di effettuare il salvataggio dei dati almeno settimanalmente, impartendo le relative istruzioni organizzative e tecniche;</p> <p>l'obbligo di redigere il "documento programmatico sulla sicurezza" annualmente (entro il 31 marzo di ogni anno) se si trattano dati sensibili o giudiziari, secondo lo standard illustrato nell'allegato B del Codice.</p> <p>L'adeguamento alle nuove misure minime di sicurezza, è opportuno sottolinearlo, deve avvenire entro il prossimo 31 dicembre 2004.</p>	
<p><b>Gestione delle password</b></p>	<p><b>Composizione:</b> la password deve essere composta da almeno otto caratteri, non contenenti riferimenti agevolmente riconducibili all'incaricato (per esempio il suo nome, cognome, ecc.)</p> <p><b>Modifica:</b> Al primo utilizzo l'incaricato deve modificare la password, e successivamente almeno ogni sei mesi. Se il trattamento riguarda dati sensibili la password deve essere modificata almeno ogni tre mesi.</p> <p><b>Custodia e riservatezza:</b> L'incaricato deve adottare le necessarie cautele per assicurare la segretezza della password, e la diligente custodia della stessa (come degli eventuali dispositivi) in suo possesso e a suo uso esclusivo.</p>	
<p><b>Sanzioni amministrative</b></p>	<p><b>Informativa all'interessato omessa o non idonea</b></p>	<p>Da 3.000 a 18.000 Euro (ovvero da 5.000 a 30.000 Euro nei casi di dati sensibili o giudiziari o che presentano rischi specifici), aumentabile sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.</p>

	<b>Notificazione omessa o incompleta</b>	Da 10.000 a 60.000 Euro, oltre alla sanzione accessoria della pubblicazione dell'ordinanza-ingiunzione su uno o più giornali.
	<b>Omessa informazione o esibizione al Garante</b>	Da 4.000 a 24.000 Euro.
<b>Sanzioni penali</b>	<b>Trattamento illecito di dati</b>	Se dal fatto deriva documento, reclusione da sei a diciotto mesi; se il fatto consiste nella comunicazione o diffusione, reclusione da sei a ventiquattro mesi.  Se l'illecito è commesso al fine di trarne un profitto o recare un danno, se dal fatto deriva documento, reclusione da uno a tre anni.
	<b>False dichiarazioni o comunicazioni al Garante</b>	Reclusione da sei mesi a tre anni.
	<b>Omessa adozione delle misure minime di sicurezza</b>	Reclusione sino a due anni o ammenda da 10.000 a 20.000 Euro.
	<b>Inosservanza dei provvedimenti del Garante</b>	Reclusione da tre mesi a due anni.
<b>Scadenziario adempimenti</b>	<p style="text-align: center;"><b>30 aprile 2004</b></p> <p>Nei soli casi previsti dalla normativa (art. 37) entro tale data è necessario inviare le <b>Notificazioni al Garante</b> relativamente ai trattamenti già iniziati; si ricorda che per i nuovi trattamenti la Notificazione va effettuata prima dell'inizio del trattamento.</p> <p style="text-align: center;"><b>31 dicembre 2004</b></p> <p>Entro tale termine devono essere adottate le nuove <b>misure minime di sicurezza (ivi compreso il documento programmatico della sicurezza)</b>. Chi utilizza strumenti elettronici che, per obiettive ragioni tecniche, non consentono l'immediata applicazione delle misure minime, ha a disposizione un termine più ampio per l'adeguamento ossia il 31 marzo 2005, previa redazione di un documento con data certa da conservare presso la propria struttura.</p>	

**Prelevato dal sito:**

**[www.counselingpsicologico.it](http://www.counselingpsicologico.it)**

**Dottoressa Psicologa Jeny Meregaglia**

**Viale Libertà 16 a 27100 Pavia**

**Cell: 331/9741064**

**Iscrizione Albo psicologi della Lombardia numero 11351**