
PRIVACY
D.Lgs 196/2003

**INCONTRO DI PRESENTAZIONE
DEL CODICE SULLA PRIVACY
D.Lgs 30 giugno 2003, n. 196**

19 maggio 2005

**Sala Vitali
Credito Valtellinese
SONDRIO**

INDICE

1. Il Codice sulla privacy
2. I dati e il trattamento: dati personali, sensibili, giudiziari, comuni
3. I soggetti: titolare, responsabile, incaricato, interessato
4. Informativa e consenso
5. Notifica al garante
6. Misure minime e misure idonee di sicurezza
7. Scadenze
8. Sanzioni

Appendice: tabella riassuntiva dei principali adempimenti

1 CODICE SULLA PRIVACY

Il decreto legislativo n. 196 del 30 giugno 2003, noto come "Codice in materia di protezione *dei dati personali*" o Testo Unico sulla Privacy, entra in vigore il 1 gennaio 2004 abrogando la precedente normativa (Legge 675/96).

Il Codice rappresenta il tentativo di comporre in maniera organica le innumerevoli disposizioni relative alla privacy (Legge 675/1996, gli altri decreti, regolamenti e codici), tenendo conto della "giurisprudenza" del Garante e della direttiva CEE 2000/58 sulla riservatezza nelle comunicazioni elettroniche.

Si precisa che i soggetti che effettuavano trattamento di dati prima dell'entrata in vigore del D.lgs 196/03 devono poter dimostrare di aver ottemperato agli obblighi previsti dalla precedente legge 675/96, ora abrogata (informative, nomine incaricati, previgenti misure minime di sicurezza) e di essersi aggiornati in base al nuovo testo normativo.

Le decisioni sull'applicazione concreta alla realtà dei diversi soggetti dovrà essere effettuata in base alle caratteristiche proprie di ciascun titolare in quanto la complessità della normativa non consente di fornire indicazioni di carattere generale o standardizzato.

Finalità

Il decreto legislativo n. 196 del 30 giugno 2003 si propone di garantire che il **trattamento** dei **dati personali** (per le definizioni vedasi in seguito) si svolga nel rispetto dei diritti fondamentali e della dignità dell'interessato, con particolare riferimento alla riservatezza e al diritto alla protezione dei dati personali.

In caso di controversie o di danni cagionati per effetto del trattamento è il soggetto che tratta i dati che deve dimostrare di avere messo in atto un sistema di protezione adeguato al livello di rischio presente nell'ambiente in cui sono stati trattati i dati stessi.

Questa inversione dell'onere delle prova è una delle più importanti novità del Codice.

Solitamente chi si ritiene danneggiato da un fatto illecito, deve provare la responsabilità di colui che ha commesso il fatto. Nel nostro caso, invece, il danneggiato deve provare solo il fatto storico, mentre colui che effettua il trattamento, e che quindi ha causato il fatto dannoso, a fini liberatori, deve dimostrare di aver adottato tutte le misure idonee (attenzione: non minime!) ad evitarlo.

Non è pertanto sufficiente la sola dimostrazione, in negativo, di non aver commesso alcuna violazione della legge o delle regole di comune prudenza, ma è necessaria la prova positiva di aver impiegato ogni cura o misura atta ad impedire l'evento dannoso.

Il Codice si suddivide in diverse parti: in questa dispensa verranno presentate, in forma sintetica e non esaustiva, le disposizioni generali (fino all'art. 45), il sistema sanzionatorio e l'Allegato B "disciplinare tecnico in materia di misure minime di sicurezza".

Quest'ultimo rappresenta il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito.

Un ulteriore principio del nuovo Codice è il cosiddetto principio di necessità (art. 3) in base al quale i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali quando le finalità perseguite possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Questo significa, nel concreto, che il titolare dovrà preventivamente adottare delle procedure organizzative/informatiche che permettano all'utente l'accesso ai soli dati necessari alla propria attività lavorativa e dovrà escludere la possibilità di trattamento di dati identificativi a quelle persone che non abbiano necessità di vederle in chiaro.

Fattivamente, essendo inopportuno conservare i dati se non se ne ha la necessità, è necessario eliminare tutti quei dati personali di cui il titolare sa di non avere più bisogno.

2 LA NATURA DEI DATI PERSONALI

La legge definisce **dato personale** "qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale" (Art. 4 comma b)

Il «dato personale» è pertanto qualsiasi informazione relativa a una persona fisica o giuridica, ente o associazione purché identificata o identificabile (ad esempio, attraverso codici o numeri identificativi); se non fosse identificato il dato sarebbe anonimo, per cui non rientrante nell'applicazione della legge.

Trattamento dei dati personali

L'ambito di applicazione della normativa è il trattamento dei dati personali, inteso come "qualunque operazione o complesso di operazioni, effettuate 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 dati" (Art. 4 comma a)

Non importa quale sia il mezzo con cui vengono svolte le operazioni sui dati: sia quelle con l'ausilio di mezzi elettronici che quelle effettuate mediante supporto cartaceo sono assoggettate alla normativa sulla tutela della privacy.

Ne consegue che:

- il dato non deve essere necessariamente organizzato
- il dato non deve venir necessariamente utilizzato (la sola conservazione è trattamento)

Le operazioni di utilizzo cui la legge dedica le maggiori attenzioni, in quanto si tratta di quelle potenzialmente più lesive della privacy, sono quelle con cui si mettono a disposizione di terzi i dati personali e sono:

- la comunicazione, cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- la diffusione, cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (es. pubblicazione in un sito).

Il Codice ha stabilito che i dati personali possono essere:

- **sensibili**: quelli che risultano 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 (art. 4 comma d)

- **giudiziari**: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, 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 ai sensi degli articoli 60 e 61 del codice di procedura penale (art. 4 comma e)

- **cosiddetti "semi-sensibili"**: dati il cui trattamento presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

E' il caso tipico dei nominativi inseriti nelle centrali dei rischi a cui fanno riferimento gli istituti di credito, dati diversi dal semplice indirizzo o nominativo, ma meno riservati dei dati sulla salute.

- **comuni**: tutti i dati personali che non rientrano nelle categorie precedenti.

Ai dati considerati sensibili o giudiziari occorre garantire una tutela più intensa, per cui sono imposti maggiori obblighi ed oneri nell'effettuare il loro trattamento e nella loro custodia.

3 I SOGGETTI (Art. 4 commi f-i)

Titolare

E' 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.

Pertanto, se il Professionista ha uno studio individuale, sarà lui stesso Titolare. Diversamente, se si tratta di uno Studio associato, è lo studio stesso ad essere Titolare qualunque sia la sua natura giuridica.

Responsabile

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

Il Responsabile può coincidere con il Titolare del trattamento (per cui la nomina è facoltativa).

In caso di nomina, il Responsabile va individuato in una figura di ruolo significativo (es. Responsabile dell'Amministrazione o del Personale, ecc.), che vanti una buona conoscenza dei processi aziendali in materia di trattamento dei dati personali e degli strumenti utilizzati (sia cartacei che elettronici).

I compiti affidati al responsabile sono specificati per iscritto dal titolare.

Possono essere nominati più Responsabili del trattamento.

In uno Studio individuale Responsabile del trattamento è lo stesso professionista mentre in uno Studio Associato possono esserlo tutti i professionisti costituenti l'associazione professionale.

In ogni caso il Titolare può nominare responsabile anche un dipendente o altri soggetti all'interno (o addirittura all'esterno) della struttura.

Incaricati

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

Si tratta in pratica tutti o quasi i dipendenti / collaboratori / praticanti, ecc. dello Studio.

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

Le lettere vengono controfirmate per accettazione.

Interessato

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

4 INFORMATIVA E CONSENSO

INFORMATIVA (Art. 13)

L'interessato è previamente informato oralmente o per iscritto circa le finalità e le modalità del trattamento cui sono destinati i dati.

Per ragioni di certezza giuridica è opportuno consegnare l'informativa in forma scritta o attraverso un apposito modello o inserendolo nella modulistica dello studio (lettere di incarico, parcelle, ecc.). E' chiaro che in questa seconda ipotesi non ho la certezza di aver informato tutti gli interessati.

Gli interessati sono tutti coloro di cui abbiamo raccolto dati personali, ossia clienti, fornitori, consumatori, utenti e dipendenti.

Per l'informativa non sono previste ipotesi di esenzione.

CONSENSO (Art. 23)

Sul consenso la norma è molto complessa, presenta diverse distinzioni ed eccezioni, e pertanto lascia adito ad una serie disparata di letture ed interpretazioni.

In generale: il trattamento di dati personali è ammesso solo con il consenso espresso dell'interessato (Art. 23)

Va distinto il consenso **per i dati comuni** e quello per i **dati sensibili**.

Per i dati sensibili il consenso deve essere manifestato per iscritto (attraverso l'apposizione della firma dell'interessato).

Per quelli comuni deve essere documentato per iscritto; questo significa, secondo alcune interpretazioni, che il consenso può essere manifestato dall'interessato anche in forma orale, ma ai fini dell'efficacia deve essere necessariamente documentato. Vista la sottigliezza interpretativa si consiglia comunque di farsi sempre rilasciare il consenso per iscritto.

Per i dati comuni (art. 24) vi è una serie di eccezioni che escludono il consenso.

Lo stesso non è richiesto, ad esempio, quando il trattamento:

- è necessario per adempiere ad un obbligo previsto dalla legge ...
- è necessario per eseguire obblighi derivanti da un contratto ...
- riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque ...
-

Non è pertanto infrequente che si rientri in una delle suddette eccezioni.

Per i dati sensibili (art. 26) una delle eccezioni più significative, che esonera dalla richiesta di consenso, si ha quando il trattamento è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro. Dunque, il consenso non è necessario per il trattamento dei dati sensibili dei dipendenti da parte del datore di lavoro.

Va detto in aggiunta che per i dati sensibili, oltre al consenso, è necessaria preventiva autorizzazione del Garante.

Per i dati giudiziari sembrerebbe invece servire solo l'autorizzazione (e non il consenso!)

In termini di autorizzazione, va aggiunto che sono state concesse due autorizzazioni generali del Garante che evitano la richiesta specifica di un'autorizzazione da parte del singolo Studio:

- la prima (4/2002) consente a tutti i professionisti di trattare dati sensibili
- la seconda (7/2002) consente il trattamento di dati giudiziari

La validità di queste autorizzazioni è stata prorogata al 31.12.05, ma non si ha la certezza che verranno rese definitive.

In conclusione

Secondo una diffusa interpretazione, per quanto concerne i dati comuni, il Professionista è generalmente esente dall'obbligo di consenso in quanto agisce, per definizione, nell'esecuzione di un contratto di mandato da parte del cliente (clausola di esclusione).

Tuttavia, stante la complessità dell'incarico, è sempre opportuno, prudenzialmente, acquisirne il consenso.

Un'ultima precisazione: il consenso deve essere informato (ossia non ha validità se non accompagnato da informativa)

5 NOTIFICA / NOTIFICAZIONE

La notifica si rende necessaria solo per i titolari dei trattamenti di cui all'art. 37: casi che, per la delicatezza dei dati e altre peculiarità, presentano rischi per i diritti e le libertà dell'interessato.

Rientrano in questa fattispecie, a titolo di esempio, i dati genetici, i dati che indicano la posizione geografica di persone mediante una rete di comunicazione elettronica, i dati idonei a rivelare lo stato di salute e la vita sessuale, i dati volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, i dati registrati in banche di dati relative al rischio sulla solvibilità.

La notifica è normalmente necessaria quando il trattamento è sistematico, rientra cioè pienamente nell'attività specifica del soggetto interessato. Nel caso di trattamenti occasionali di tali dati si è generalmente esonerati dall'obbligo di notifica.

La notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta.

La notificazione è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante

6 MISURE MINIME E MISURE IDONEE DI SICUREZZA

Nel codice della privacy sono menzionate ed evidenziate due differenti categorie di misure: le misure idonee (art. 31) e le misure minime (artt. 33, 34 e 35+allegato B).

Il codice ripropone la distinzione tra misure di sicurezza idonee e misure di sicurezza minime con le medesime conseguenze previste dalla normativa precedente: responsabilità civile (e pertanto sanzioni pecuniarie) in caso di violazione delle misure idonee; responsabilità penali (art. 169) nel caso delle minime.

Lo scopo che tale norma si propone è quello di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31).

Questo impone un'analisi approfondita del proprio ambiente di lavoro, nonché un'attenzione particolare al continuo sviluppo tecnologico.

Proprio in relazione all'utilizzo o meno di strumentazione elettronica la legge prevede delle misure di sicurezza differenti, imponendone di più severe e rigorose a chi usufruisce di dispositivi informatici.

Trattamento con strumenti elettronici (art. 34 e allegato B)

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B, le seguenti misure minime:

- a) autenticazione informatica;
- b) adozione di procedure di gestione delle credenziali di autenticazione;
- c) utilizzazione di un sistema di autorizzazione;
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- g) tenuta di un aggiornato documento programmatico sulla sicurezza; esso diventa obbligatorio per tutti i titolari che trattino dati sensibili e giudiziari tramite elaboratori, a differenza della norma precedente in cui era necessario solo per i trattamenti svolti mediante una rete disponibile al pubblico.

Pertanto, entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

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.

Trattamento senza strumenti elettronici (art. 35)

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B, le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) 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.

7 SCADENZE

Non tutte le disposizioni (adempimenti) prevedono la stessa scadenza. Nello specifico:

Notificazione (comunicazione formale al garante per alcune tipologie di dati)	30 aprile 2004
Adozione misure minime di sicurezza (allegato B)	31 dicembre 2005
Redazione del Documento Programmatico sulla sicurezza (DPS)	31 dicembre 2005
Aggiornamento del DPS (redatto in anni precedenti)	31 marzo 2006
Predisposizione di un documento, con data certa, con il quale si comunica che il soggetto dispone di strumenti elettronici che, per ragioni tecniche, non consentono di adottare le misure minime	31 dic. 2005
Adeguamento degli strumenti elettronici di cui al punto precedente	31 marzo 2006

È bene precisare che la proroga al 31/12/2005 riguarda soltanto l'adozione delle nuove misure minime di sicurezza richieste dal Codice e dal già citato Allegato B, non previste dalla precedente normativa.

8 SANZIONI (artt. 161-172)

Illeciti civili	Sanzioni
Art. 161 Assenza o inidoneità informativa - dati comuni - dati sensibili o giudiziari o trattamenti che presentano rischi specifici o di maggiore rilevanza del pregiudizio	Sanzione da 3.000 a 18.000 euro Sanzione da 5.000 a 30.000 euro (moltiplicabile per 3 quando risulta inefficace in ragione delle condizioni economiche del contravventore)
Art. 163 Omessa o incompleta notificazione al Garante	Sanzione da 10.000 a 60.000 euro + pubblicazione su quotidiani
Art. 164 Omissione di fornire informazioni o esibire documenti richiesti dal Garante	Sanzione da 4.000 a 24.000 euro.
Illeciti penali	Sanzioni
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
Art. 169 Omessa adozione di misure necessarie alla sicurezza dei dati	Arresto fino a 2 anni o ammenda da 10.000 a 50.000 euro
Art. 170 Inosservanza dei provvedimenti del Garante	Arresto da 3 mesi a 2 anni

Alcuni dei principali adempimenti ai sensi del D.Lgs. 196/03

PROVVEDIMENTO	NOTE
Lettere di nomina del/dei responsabile/i del trattamento	Facoltativa
Lettere di nomina degli incaricati	Considerare anche gli eventuali collaboratori, praticanti, ecc.
Lettera di nomina per gli esterni che trattano i dati	Trasferimento delle responsabilità (società di software, commercialista, legale, studio paghe, ecc.)
Informativa e consenso agli interessati	Clienti, fornitori, altri interessati
Informativa e consenso ai dipendenti	Considerare anche gli eventuali collaboratori, praticanti, ecc.
Attivare username e password	<ul style="list-style-type: none"> - Ai diversi livelli server / PC / programmi - Sistema sicuro (consigliato) a partire da Windows 2000 - Cambiare password ogni 3 mesi (dati sensibili) o 6 mesi (dati comuni) - Password alfanumerica - Password non riconducibile in nessun modo alla persona - Password di almeno 8 caratteri (o il massimo consentito dal programma) - In caso di abbandono del posto di lavoro attivare screen-saver con password o funzione "disconnetti"
Attivare profili utente diversi per diversi PC	<ul style="list-style-type: none"> - solo in caso di più PC con accessi diversificati - rivedere periodicamente (almeno 1 volta all'anno) le autorizzazioni
Custode delle password	Trascrivere password in busta chiusa e consegna al custode
Antivirus / Firewall	<ul style="list-style-type: none"> - Antivirus su tutte le macchine / banche dati - Valutare l'opportunità di antispam - Aggiornamento minimo annuale del software (almeno relativamente agli aspetti della sicurezza) - Firewall per la protezione da intrusioni esterne (prevedere un'analisi periodica del funzionamento dell'attività del firewall)
Back-up	<ul style="list-style-type: none"> - custodia delle registrazioni in luogo non accessibile e protetto - back-up completo con cadenza almeno settimanale con verifica del ripristino dei dati (per i dati sensibili entro sette giorni).
Documento Programmatico sulla Sicurezza (DPS)	In caso di trattamento <u>dati sensibili</u> /giudiziari in forma elettronica
Dati sensibili / giudiziari	<ul style="list-style-type: none"> - Indicati nelle lettere di incarico - Custoditi da personale autorizzato / non lasciati sulla scrivania ma conservati in cassettiere / armadi con serratura - Avvalersi di dispositivi distruggi-documenti.
Nomina dell'incaricato all'accesso ai locali	Valutare l'istituzione di un registro di rilevazione ingressi / presenze dopo l'orario di lavoro (es. impresa di pulizia)