

Infoserv Flegrea s.a.s.

Sintesi D.Lgs. 30 giugno 2003 n. 196 (ex 675/96)
(Sicurezza dei dati e Tutela della privacy)

1. Codice della privacy	2
2. Finalita	2
3. Soggetti tutelati	2
4. Oggetto di tutela	2
5. Ambito di applicazione	3
6. Esclusioni	3
7. Modalità del trattamento	3
8. Soggetti coinvolti	4
9. Principio della trasparenza	5
10. Notificazione	6
11. Trasferimento di dati all'estero	7
12. Sanzioni	7

1. Codice della privacy

Lo scorso giugno 2003 è stato approvato dal Consiglio dei Ministri il testo unico in materia di protezione dei dati personali, denominato “Codice” della privacy. Il provvedimento, D.Lgs. 30 giugno 2003 n. 196 , è stato pubblicato sulla Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento ordinario n. 123.

Il Codice entrerà in vigore, pressochè integralmente, il primo gennaio 2004 e sostituisce la precedente legge 675/96 nonchè i vari provvedimenti che si sono succeduti in materia.

2. Finalità

Il Codice, in aderenza alla direttiva europea di riferimento n. 95/46 Ce del 24 ottobre 1995 , intende **garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti**, delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale e al **diritto alla protezione dei dati** (art. 2).

3. Soggetti tutelati

La protezione è garantita non solo ai dati riguardanti le **persone fisiche**, vale a dire gli individui, ma anche a quelli riguardanti le **persone giuridiche, gli enti e le associazioni** (4, comma 1, lettera i). **E' questa una delle più rilevanti differenze nei confronti della direttiva europea, che limita l'ambito di tutela alle sole persone fisiche.**

4. Oggetto di tutela

4.1. Trattamento

Per trattamento la legge intende: “(...) qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, 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 1, lett. a). La definizione, coprendo l'intero arco delle operazioni che vanno dalla raccolta alla distruzione di un dato, termini inclusi, è di ampiezza tale **da riguardare tutte le operazioni che normalmente coinvolgono l'utilizzo di un dato personale.**

4.2. Dati personali

Per “dato personale”, il codice intende: **“(...) qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale”** (art. 4, comma 1, lett. b). La definizione include qualsiasi informazione che consenta di individuare con certezza in modo diretto o indiretto una persona fisica o giuridica. Sono tali, solo a titolo di esempio, i dati anagrafici, i recapiti telefonici o telematici, i codici identificativi delle carte di credito, del conto corrente etc; ma anche la registrazione della voce, delle immagini; e ancora, le caratteristiche biometriche quali le impronte digitali, la geometria del viso, della mano, il disegno dell'iride. In una parola, tutto quanto permetta di identificare un soggetto sia in

via diretta sia in via indiretta, vale a dire attraverso il collegamento di più informazioni anche di per sé non significative se singolarmente considerate. La legge individua **tre categorie di dati personali**, in funzione della diversa rilevanza loro attribuita dalla legge, delle diverse precauzioni richieste per il loro utilizzo e la loro custodia, e della oggettiva diversa pericolosità per l'individuo derivante da un eventuale illecito trattamento.

Dati sensibili

Sono i dati personali 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 1, lett. d).

Dati giudiziari

Sono i dati personali "idonei a rivelare i provvedimenti di cui all'art. 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 o 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 1, lett. e).

Dati comuni

Sono tutti i restanti dati personali, non compresi nelle due precedenti categorie. A questo punto va sottolineato e ribadito che la legge sulla privacy tutela tutti i dati personali, inclusi quelli cosiddetti "comuni". **Semmai la legge prevede norme più restrittive e detta cautele maggiori per i dati sensibili o giudiziari, ma non esclude affatto la protezione anche dei dati comuni.**

5. Ambito di applicazione

La legge si applica al trattamento dei dati personali da chiunque effettuato nel territorio dello Stato; anche se i dati riguardano una persona fisica o giuridica estera e anche nel caso in cui i dati personali siano detenuti all'estero (art. 5).

6. Esclusioni

La legge, in generale, non si applica al trattamento di dati effettuato da persone fisiche **per fini esclusivamente personali, privati**, purché essi non siano destinati ad una comunicazione sistematica o alla diffusione ad un pubblico indeterminato (art. 5). **Tuttavia**, anche al trattamento per fini esclusivamente personali si applicano **le disposizioni relative all'obbligo di custodia dei dati con idonee e preventive misure di sicurezza** (richieste dall' art. 31), al risarcimento del danno per effetto del trattamento di dati personali (stabilito dall' art. 15)

7. Modalità del trattamento

In base a quanto previsto dall'art. 11, i dati personali devono essere:

- trattati in modo lecito e con correttezza;
- raccolti e utilizzati per scopi determinati, espliciti e legittimi;
- esatti e mantenuti aggiornati;

- pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti;
- conservati solo per il tempo necessario agli scopi per i quali sono stati raccolti.

I comportamenti tenuti in violazione di questo articolo possono comportare una richiesta di risarcimento del danno, anche non patrimoniale (art. 15).

8. Soggetti coinvolti

La legge individua cinque figure principali a ciascuna delle quali associa uno specifico ruolo nell'ambito della tutela della riservatezza: l'interessato, il titolare, il responsabile, gli incaricati del trattamento e l'Autorità Garante. Ad esse si aggiunge, quale naturale organo di tutela dei diritti, l'autorità giudiziaria

8.1. interessato

E' "**la persona fisica, la persona giuridica, l'ente o l'associazione** cui si riferiscono i dati personali" (art. 4, comma 1, lett. i). Sono tali, per una azienda, tutti i soggetti dei quali vengono raccolti e trattati dati personali, sia che si tratti di persona fisica sia che si tratti di persona giuridica. Tra gli altri, quindi, i dipendenti, i clienti, i fornitori, i consulenti, i partners, ecc... Trattamento, comunicazione e diffusione di dati personali si possono effettuare solo previo consenso dell'interessato; consenso che deve essere: informato, libero, esplicito, espresso in forma specifica e documentato per iscritto (art. 23). All'interessato è assicurato il cosiddetto "diritto di accesso" ai dati (art. 7). Ha inoltre diritto a ricevere risposta, dal titolare! responsabile, entro 15 giorni dalla richiesta (146, comma 2). I diritti dell'interessato vengono analizzati dettagliatamente nel paragrafo "Principio della trasparenza".

8.2. Titolare

Può essere una **persona fisica, una persona giuridica, la pubblica amministrazione, gli enti pubblici economici e qualsiasi altro ente, associazione od organismo** cui competono le decisioni in ordine alle finalità e alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza(art. 4, comma 1, lettera f). Il titolare è responsabile di notificare al Garante che "intende procedere a un trattamento di dati personali" (art. 37). E' inoltre responsabile di inoltrare le richieste di autorizzazione al trattamento quando previste dalla legge, ad esempio nel caso di dati sensibili (cfr. in questo stesso paragrafo "Garante"); di nominare i responsabili; dare loro disposizioni scritte in merito al trattamento e alle misure di sicurezza; vigilare sulla loro attività con verifiche periodiche (art. 29).

Risponde, inoltre, del trattamento illecito dei dati personali (cfr. Sanzioni).

8.3. Responsabile

Viene designato, facoltativamente, dal titolare tra coloro che "per esperienza, capacità e affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza". Per esigenze organizzative può essere designato più di un responsabile, "anche mediante suddivisione di compiti" (art. 29). Il responsabile può nominare gli incaricati del trattamento fornendo loro le istruzioni a cui debbono attenersi nell'elaborare i dati ai quali hanno accesso (art. 29).

8.4. Incaricati

Gli incaricati del trattamento sono gli individui che agiscono sotto la diretta autorità del titolare o del responsabile e che ricevono, per iscritto, da questi ultimi, disposizioni in merito alle operazioni da compiere per il trattamento dei dati personali (art. 30). Possono

essere designati incaricati del trattamento solo e soltanto persone fisiche (art. 4, comma 1, lett. h).

8.5. Garante

E' la struttura pubblica che deve vigilare sull'esatto adempimento degli obblighi di legge. Si tratta di un organo collegiale composto da quattro membri elettivi, tra i quali viene eletto un Presidente, alle cui dipendenze è posto un ufficio composto da dipendenti dello Stato. Il titolo del II codice elenca dettagliatamente la composizione dell'ufficio del Garante, i suoi compiti, l'organizzazione e il funzionamento dell'ufficio nonché le norme relative allo svolgimento dei procedimenti in base a principi di trasparenza partecipazione e contraddittorio. Tra i compiti assegnatigli, il Garante:

- istituisce e tiene un registro generale dei trattamenti in finzione delle notifiche ricevute dai titolari;
- controlla se i trattamenti avvengono nel rispetto della legge;
- diffonde la conoscenza tra il pubblico della normativa;
- ha la facoltà di richiedere al titolare o al responsabile, all'interessato o a terzi, documenti e informazioni sul trattamento dei dati personali e può disporre accessi ispezioni e verifiche nei luoghi nei quali si svolge il trattamento dei dati o ove ritiene di poter effettuare rilevazioni comunque utili al controllo del trattamento dei dati. In ciò avvalendosi, se necessario, della collaborazione di altri organi dello Stato.

Il Garante è inoltre l'organo competente a irrogare sanzioni amministrative qualora, ad esempio, non gli siano stati forniti i documenti e le informazioni richiesti o nel caso in cui non siano state rese all'interessato le informazioni previste dalla legge, al momento della raccolta dei dati.

9. Principio della trasparenza

I diritti alla riservatezza, garantiti dal codice, comportano per contro precisi obblighi e precise limitazioni alla libertà di azione.

Diritti e obblighi si possono riassumere come segue.

9.1. Informativa

Chi vuole utilizzare i dati personali di un terzo (definito dal codice col termine di "interessato"), deve informarlo preventivamente secondo le modalità previste all'art. 13, al fine di assicurare che egli comprenda, prima di fornire i dati richiesti, quali effetti concreti comporterà il conferimento degli stessi.

Le informazioni preventive devono essere fornite per iscritto o oralmente all'interessato stesso o alla persona presso la quale i dati personali sono raccolti. L'informativa va sempre data.

L'interessato deve essere sempre nella condizione, di poter controllare che i dati vengano effettivamente utilizzati in conformità con quanto originariamente dichiaratogli e non per differenti finalità, modalità od altro.

9.2. Consenso

Se un privato o un ente pubblico economico vuole utilizzare i dati personali di un terzo ("interessato") deve richiedere e ottenere la sua autorizzazione. Il trattamento dei dati è infatti consentito (fatti salvi i casi di esclusione previsti dal codice), solo dopo che l'interessato ha espresso il proprio consenso. Per essere valido, il consenso deve essere raccolto nel rispetto delle condizioni previste dall'art. 23 e di seguito riportate.

- *Informato*
- *Libero*

- *Espresso informa specifica*
- *Documentato per iscritto*
- *Scritto*

9.3. Esclusione del consenso

Alla regola generale della necessità di disporre del consenso per poter trattare dati personali, sono previste eccezioni. **Il codice identifica con precisione i casi in cui il consenso dell'interessato non è richiesto (art. 24).**

Le ipotesi più frequenti. Il consenso non è richiesto quando, fra gli altri, i dati personali sono stati raccolti in base ad un obbligo previsto dalla legge; sono utilizzati nell'ambito di un di cui è parte l'interessato; provengono da pubblici registri, elenchi, atti o documenti conoscibili da chiunque (es. elenco telefonico); riguardano lo svolgimento di attività economiche proprie dell'interessato; quando i dati sono utilizzati nell'esercizio della professione giornalistica, quando la raccolta è necessaria per la salvaguardia della vita o dell'incolumità fisica dell'interessato o per lo svolgimento di investigazioni.

Il consenso risulta necessario in una o più delle seguenti situazioni:

- i dati sono ceduti a terzi;
- dati sono utilizzati per studi e ricerche di mercato;
- si intende inviare nel tempo, su base discrezionale, materiale pubblicitario, promozionale, mediante l'utilizzo di strumenti automatizzati come ad esempio il fax; vengono richiesti dati "sensibili".

9.4. Diritto di accesso ai dati

Il codice riconosce all'interessato il cosiddetto "diritto di accesso" ai propri dati. Consiste nel diritto ad ottenere dal titolare o dal responsabile, senza ritardo, conferma dell'esistenza o meno di dati che lo riguardano, a conoscere l'origine e le finalità su cui si basa il trattamento ed eventualmente ad ottenere la cancellazione, l'aggiornamento e la rettifica dei dati. L'interessato può inoltre opporsi in tutto o in parte al trattamento dei dati personali che lo riguardano per fini di informazione commerciale, pubblicitari o di vendita diretta (art. 7).

10. Notificazione

Il principale obbligo del titolare, nei confronti dell'Autorità Garante, consiste nella notificazione dei trattamenti secondo quanto di seguito indicato.

Notificazione iniziale

Il Titolare del trattamento è tenuto a notificare al Garante l'intenzione di procedere al trattamento dei dati solo in determinate ipotesi, specificamente indicate nell'art. 37 . In tal caso la notifica deve essere effettuata "preventivamente e una sola volta utilizzando l'apposito modello predisposto dal Garante e secondo le modalità indicate all'art. 37.

Notifica delle modificazioni

La notificazione, una volta effettuata, non è soggetta a limiti temporali. Tuttavia se una delle informazioni già notificate muta, è necessario procedere ad una nuova notificazione che deve precedere l'effettuazione della variazione (art. 38).

Notifica della cessazione

Allo stesso modo, in caso di cessazione del trattamento di dati dovuta a qualsivoglia ragione, quale ad esempio la cessazione dell'attività, la fusione, l'incorporazione ecc., il titolare è tenuto a notificare preventivamente al Garante la destinazione dei dati. Può consistere nella loro distruzione, o nella loro cessione ad altro titolare per un utilizzo analogo, oppure nella loro conservazione per un utilizzo esclusivamente privato (art. 38).

Esoneri

I titolari che non effettuano trattamenti inclusi nella ridotta casistica di cui all' art. 37 sono esonerati dall' onere della Notifica al Garante. L' esonero riguarda una quantità rilevante di titolari, ulteriormente arricchita dalla deliberazione del Garante n. 1 del 31 marzo 2004

Termini di presentazione

La notificazione deve essere effettuata prima dell' inizio del trattamento.

11. Trasferimento di dati all'estero

Gli articoli dal 42 al 45 del Codice contengono le norme relative al trasferimento dei dati all'estero. La disciplina è diversa in funzione del Paese di destinazione dei dati.

12. Sanzioni

L' importanza attribuita dal legislatore alla legge in questione è rilevabile anche dal **considerevole apparato sanzionatorio** da cui il codice è assistito. In caso di violazione della legge, sono previste **sanzioni di tipo penale, civile e amministrativo**. Il titolare ed il responsabile sono i principali soggetti chiamati a rispondere personalmente sotto il profilo sanzionatorio e penale.

Sanzioni penali

Per quanto riguarda le sanzioni penali il codice stabilisce:

- per falsità nelle dichiarazioni e notificazioni al Garante la reclusione da 6 mesi a 3anni - (art. 168);
- per trattamento illecito di dati personali la reclusione da 6 a 24 mesi a seconda dei casi (art. 167);
- per omessa adozione di misure "minime" necessarie alla sicurezza dei dati l' arresto sino a 2 anni o l' ammenda da diecimila a cinquantamila Euro (art. 169);
- per inosservanza dei provvedimenti del Garante la reclusione da 3 mesi a 2 anni (art. 170).

Risarcimento del danno

L' articolo art. 15 stabilisce che "Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell' art. 2050 del codice civile". Si tratta di una responsabilità molto ampia parificata a quella relativa allo svolgimento di una qualsiasi attività pericolosa (art. 2050 c.c.) per cui spetta al danneggiante dimostrare che il danno arrecato non gli è imputabile in quanto aveva adottato tutti i mezzi organizzativi e tecnici per evitarlo. Sono risarcibili sia i danni patrimoniali sia quelli non patrimoniali.

Sanzioni amministrative

Per quanto riguarda le sanzioni amministrative l' art. 161 stabilisce che:

- l' omissione o l' incompleta notificazione al Garante è punita col pagamento di una somma da diecimila a sessantamila Euro;
- la violazione delle disposizioni previste per le informazioni da rendere all' interessato al momento della raccolta dei dati di cui all' art. 13 , è punita con la sanzione del pagamento da tremila a diciottomila Euro o, nei casi di dati sensibili e giudiziari, da cinquemila a trentamila Euro (art. 161).