

Pillole di Privacy

Contenuti essenziali del D.Lgs. 196/03¹

Introduzione: Il D.Lgs. 196/03 (*Codice Privacy*) riunisce in un **testo unico** tutta le previgente normativa in materia, ad eccezione delle disposizioni di legge e di regolamento che stabiliscono divieti o limiti più restrittivi; inoltre riconosce a chiunque il **diritto alla protezione dei dati personali** che lo riguardano (*art. 1*), dove per chiunque si intende una persona fisica, una persona giuridica, un ente o un'associazione.

Per quanto detto la finalità del codice (*art. 2*) è quella di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla **riservatezza**, all'**identità personale** e al **diritto alla protezione dei dati personali**. Dunque il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà menzionate, nel rispetto dei **principi di semplificazione, armonizzazione ed efficacia** delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Un fondamentale principio espresso dal Codice Privacy è quello detto di **necessità nel trattamento dei dati** (*art. 3*): *“I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità”*.

Glossario (*art. 4*): Per comprendere meglio i termini e le definizioni adottati, è utile formalizzare alcuni concetti.

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

Per **trattamento** si intende qualunque operazione o complesso di operazioni, effettuati 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 di dati.

1 Le informazioni riportate in questo documento sono estratte dal testo consolidato vigente del D.Lgs. 196 del 30 giugno 2003 e dai suoi allegati, senza alcuna pretesa di esaustività. L'autore non si assume alcuna responsabilità relativamente ad eventuali imprecisioni, errori od omissioni contenuti nel presente documento.

Per **dato personale** si 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.

Per **dato identificativo** si intende quel particolare tipo di dato personale che permette l'identificazione diretta dell'interessato.

Per **dato sensibile** si intende quel particolare tipo di dato personale idoneo 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 il dato personale idoneo a rivelare lo stato di salute e la vita sessuale, ovvero i così detti dati *ultra-sensibili*.

Per **dato giudiziario** si intende quel particolare tipo di dato personale idoneo a rivelare provvedimenti 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.

Il **titolare** di un trattamento 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. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, il titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza (*art. 28*).

Il **responsabile** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposta dal titolare al trattamento di dati personali. Il responsabile è designato dal titolare facoltativamente (*art. 29*): se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni e istruzioni da lui stesso impartite.

Gli **incaricati** sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite (*art. 30*). La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata

preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

Informativa sulla privacy (art. 13): Per poter trattare dati personali è necessario **informare preventivamente l'interessato** o la persona presso la quale sono raccolti i dati personali, oralmente o per iscritto, tramite l'Informativa sulla privacy, circa:

1. le finalità e le modalità del trattamento cui sono destinati i dati
2. la natura obbligatoria o facoltativa del conferimento dei dati
3. le conseguenze di un eventuale rifiuto di rispondere
4. i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza e l'ambito di diffusione dei dati medesimi
5. gli estremi identificativi del titolare (*responsabile del trattamento*) e, se designati, del rappresentante nel territorio dello Stato
6. i diritti dei soggetti interessati (*es. accesso ai dati, opposizione al trattamento, aggiornamento o cancellazione, etc.*)

Per ogni tipologia di trattamento dovrà essere prevista una differente informativa.

Diritti dell'interessato (artt. da 8 a 10): Si riporta il testo integrale dell'art. 7 del Codice Privacy, così come andrebbe riportato in calce all'informativa, in modo da fornire all'interessato la possibilità di prendere atto di tutti i diritti che lo riguardano.

Art. 7. Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la **conferma dell'esistenza** o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
 - a. dell'**origine dei dati** personali;
 - b. delle **finalità e modalità del trattamento**;
 - c. della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
 - d. degli **estremi identificativi del titolare**, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
 - e. dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di

rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:
 - a. l'**aggiornamento**, la **rettificazione** ovvero, quando vi ha interesse, l'integrazione dei dati;
 - b. la **cancellazione**, la **trasformazione in forma anonima** o il **blocco** dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
 - c. l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di **opporsi**, in tutto o in parte:
 - a. per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorchè pertinenti allo scopo della raccolta;
 - b. al trattamento di dati personali che lo riguardano a fini di **invio di materiale pubblicitario** o di **vendita diretta** o per il compimento di ricerche di mercato o di comunicazione commerciale.

Consenso (artt. da 23 a 27): Il trattamento di dati personali effettuato da soggetti privati, ovvero da enti pubblici economici, è **ammesso solo dietro espresso consenso** dell'interessato. Poiché l'informativa può essere fornita sia oralmente che per iscritto, anche il consenso potrà essere espresso sia oralmente che per iscritto, purché venga espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato tramite l'informativa e sia documentato per iscritto. Tuttavia in caso di trattamento di dati sensibili il consenso dovrà essere necessariamente manifestato in forma scritta.

Esistono tuttavia dei casi in cui non è previsto il consenso da parte dell'interessato, che nella fattispecie sono (art. 24):

- a. è necessario per adempiere ad un **obbligo previsto dalla legge**, da un regolamento o dalla normativa comunitaria;
- b. è necessario 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;
- c. riguarda dati provenienti da **pubblici registri, elenchi, atti** o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i

- regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;
- d. riguarda dati relativi allo **svolgimento di attività economiche**, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
 - e. è necessario per la **salvaguardia della vita** o dell'incolumità fisica di un terzo;
 - f. con esclusione della diffusione, è necessario ai fini dello svolgimento delle **investigazioni difensive** o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
 - g. con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'**attività di gruppi bancari e di società controllate** o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;
 - h. con esclusione della comunicazione all'esterno e della diffusione, è effettuato 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, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;
 - i. è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi **scopi scientifici o statistici**, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

Comunicazione al Garante (artt. da 37 a 41): 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 diffuse, 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.

La notificazione relativa al trattamento dei dati di cui sopra non è dovuta se relativa all'attività dei medici di famiglia e dei pediatri di libera scelta, in quanto tale funzione è tipica del loro rapporto professionale con il Servizio sanitario nazionale.

Modalità di trattamento (art. 11): I dati personali oggetto di trattamento sono:

- a. trattati in modo **lecito** e secondo **correttezza**;
- b. raccolti e registrati per **scopi determinati, espliciti e legittimi**, ed utilizzati in altre operazioni del trattamento intermini compatibili con tali scopi;
- c. esatti e, se necessario, **aggiornati**;
- d. **pertinenti, completi e non eccedenti** rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- e. conservati in una forma che consenta l'**identificazione dell'interessato per un periodo di tempo non superiore a quello necessario** agli scopi per i quali essi sono stati raccolti o successivamente trattati.

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Cessazione del trattamento (art. 16): In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:

- a. **distrutti**;
- b. **ceduti ad altro titolare**, purchè destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
- c. **conservati per fini esclusivamente personali** e non destinati ad una comunicazione sistematica o alla diffusione;
- d. conservati o ceduti ad altro titolare, per **scopi storici, statistici o scientifici**, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12.

La cessione dei dati in violazione di quanto previsto dal Codice Privacy, o di altre disposizioni rilevanti in materia di trattamento dei dati personali è priva di effetti.

Danni cagionati per effetto del trattamento (art. 15): Chiunque **cagiona danno** ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile (*Responsabilità per l'esercizio di attività pericolose*), il quale recita: "Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno".

In sintesi l'**inversione dell'onere della prova a carico del titolare** del trattamento fa sì che sarà quest'ultimo a dover dimostrare di avere adottato tutte le misure idonee ad evitare il danno.

Obblighi di Sicurezza (artt. 31 e 32): Il Codice Privacy sancisce l'obbligo di custodire e controllare i dati personali oggetto di trattamento, anche in relazione alle conoscenze acquisite in base al **progresso tecnico**, alla **natura dei dati** e alle specifiche **caratteristiche del trattamento**, in modo da **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.

Misure minime di Sicurezza (artt. da 33 a 35): I titolari del trattamento sono comunque tenuti ad adottare le misure di sicurezza volte ad assicurare un **livello minimo di protezione** dei dati personali.

In particolare il **trattamento di dati personali effettuato con strumenti elettronici** è consentito solo se sono adottate 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 (DPS)**;
- 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.

Disciplinare tecnico in materia di misure minime di sicurezza (allegato B): L'allegato B del Codice Privacy individua le **modalità tecniche** da implementare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici, affinché si realizzi l'adozione delle **misure minime** di sicurezza di cui al precedente punto.

Documento Programmatico sulla Sicurezza (DPS) (allegato B, reg. 19): La regola 19 dell'allegato B dettaglia le informazioni che vanno riportate nel **Documento Programmatico sulla Sicurezza (DPS)**. In particolare esse sono:

- a. **elenco dei trattamenti** di dati personali;
- b. la **distribuzione dei compiti e delle responsabilità** nell'ambito delle strutture preposte al trattamento dei dati;
- c. l'**analisi dei rischi** che incombono sui dati;
- d. 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;
- e. la descrizione dei **criteri e delle modalità per il ripristino della disponibilità dei dati** in seguito a distruzione o danneggiamento;
- f. 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

$$\Delta x \Delta p_x \geq \frac{\hbar}{2}$$

- ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare;
- g. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di **trattamenti di dati personali affidati all'esterno** della struttura del titolare, purché in conformità al codice;
 - h. per i dati personali idonei a rivelare lo **stato di salute e la vita sessuale**, trattati da parte di **organismi sanitari** e/o esercenti professioni sanitarie, l'individuazione dei criteri da adottare per la **cifratura** o per la separazione di tali dati dagli altri dati personali dell'interessato.

Riguardo l'**obbligo di redazione** del Documento Programmatico sulla Sicurezza, la posizione dall'autore prevede che il **DPS vada redatto comunque da tutti coloro che effettuano un trattamento di dati personali**, in quanto esso è un utilissimo **strumento di autoanalisi**, la cui utilità va ben oltre il mero obbligo normativo.

Se, ad ogni modo, si vuole individuare un obbligo è possibile ragionevolmente pensare che il **DPS debba essere redatto soltanto da coloro che trattano dati sensibili e giudiziari tramite strumenti elettronici**.

Tuttavia si ribadisce come la redazione del Documento Programmatico sulla Sicurezza vada inquadrata nell'ottica di una **gestione efficiente del proprio sistema informativo**, al fine di ridurre la minimo il rischio di cagionare danni per effetto del trattamento di dati personali. Per ulteriori approfondimenti sull'argomento vedasi sul Journal on-line dell'autore <http://www.ingamendola.com/journal> l'articolo "*Obbligo di redazione del Documento Programmatico sulla Sicurezza (DPS)*".

Le misure minime di sicurezza di cui agli articoli da 33 a 35 del D.Lgs. 196/03, e all'allegato B) al medesimo, che non erano previste dal decreto del Presidente della Repubblica 28 luglio 1999, n. 318, sono adottate entro il 31 dicembre 2005.

Per maggiori informazioni sulla normativa vigente in materia di protezione dei dati personali è possibile far riferimento al sito web del Garante Privacy su <http://www.garanteprivacy.it>