

## PRIVACY in Pillole

<i>Cosa si intende per privacy?</i>	<p>La protezione dei dati si concretizza nei poteri di intervento, spettanti ad ogni soggetto nei confronti di chiunque gestisca informazioni personali che possono comportare impatto sociale.</p> <p>La tutela consente di seguire e controllare la circolazione dei dati personali e la loro protezione nei diversi circuiti in cui possono venire inseriti</p>
<i>Chi sono i soggetti tutelati?</i>	<p>Le persone fisiche e le persone giuridiche</p>
<i>Che tipo di diritto è la privacy?</i>	<p>Il diritto alla privacy è posto accanto ai diritti e alle libertà fondamentali come garanzia per il trattamento dei dati personali. Il diritto alla privacy è stato definito non soltanto quale diritto fondamentale della persona umana, ma anche come un presupposto necessario per il godimento delle altre libertà garantite dalla nostra Costituzione. È per questa ragione che il legislatore ha adottato con il nuovo Codice una regolamentazione stringente; questa deve bilanciarsi tra: a) la necessità di acquisire le informazioni indispensabili allo svolgimento delle varie attività; b) la garanzia di tutela della persona, in particolare con riferimento a determinate caratteristiche dell'individuo la cui pubblicità potrebbe ledere la sensibilità, limitarne la libertà o anche determinare una diversità di trattamento, nel senso discriminatorio del termine</p> <ul style="list-style-type: none"><li>• <i>Dati personali</i>: qualunque informazione relativa a persona fisica, giuridica, ente o associazione, identificati o identificabili anche indirettamente, compresi i numeri di identificazione personale;</li><li>• <i>Dati identificativi</i>: sono i dati personali che consentono l'identificazione diretta dell'interessato;</li></ul>
<i>Alcune definizioni</i>	<ul style="list-style-type: none"><li>• <i>Dati sensibili</i>: dati personali 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;</li><li>• <i>Dati 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</li></ul>
<i>Il diritto di accesso ai dati personali</i>	<p>L'art. 7 del codice della privacy consente all'interessato di ottenere la conferma dell'esistenza di dati personali che lo riguardano. D'altra parte l'interessato ha il diritto d'opporvi, in tutto o parzialmente per motivi legittimi al trattamento dei dati personali che lo riguardano, anche se pertinenti allo scopo della raccolta</p>
<i>È garantito il diritto ad essere informati del trattamento di</i>	<p>L'informativa consente all'interessato di venire a conoscenza del trattamento dei dati che lo riguardano, dei fini perseguiti attraverso il trattamento, delle modalità del trattamento e di tutte le altre informazioni, a far acquisire una consapevolezza piena sui propri diritti, le libertà fondamentali e la dignità personale, da proteggere in modo effettivo anche attraverso i mezzi di tutela previsti a suo</p>

*dati personali* favore.

Si tratta di un istituto posto a garanzia dell'interessato presso il quale i dati sono raccolti. Può essere fatta oralmente o per iscritto alle famiglie, al personale dipendente, ai fornitori

La scuola, come tutti i soggetti pubblici, non deve chiedere il consenso al trattamento di dati personali

Il Codice prevede: a) il trattamento di dati personali da parte di soggetti pubblici; b) la comunicazione di dati personali da parte di soggetti pubblici ad altri soggetti pubblici; c) la comunicazione di dati personali da parte di soggetti pubblici e privati e la diffusione di tali dati.

*La comunicazione e la diffusione di dati personali* I dati che vengono presi in considerazione sono solo quelli personali, non quindi i dati sensibili. È necessaria una previsione normativa specifica per la comunicazione da un soggetto pubblico ad un altro soggetto pubblico. Mentre tra soggetti privati la comunicazione è libera, tra soggetti pubblici la comunicazione è vietata, a meno che non sia espressamente prevista da una norma di legge o regolamento. La previsione deve essere reciproca, cioè sia il soggetto richiedente che il soggetto titolare devono rifarsi ad una norma o a regolamenti. Questo divieto è mitigato dal principio che, in mancanza di una norma esplicita, interviene il principio che la comunicazione è necessaria ai fini dell'esercizio di funzioni istituzionali.

In questo caso però il soggetto titolare del trattamento deve comunicare al Garante i dati personali comunicati ad altro soggetto pubblico; il trattamento può iniziare decorsi quarantacinque giorni dalla comunicazione, salva diversa disposizione del Garante.

Diverso è il regime per la comunicazione da parte di soggetti pubblici a soggetti privati o a enti pubblici economici. Essa è ammessa solo se prevista da una norma di legge o regolamento. Lo stesso principio vale per la diffusione. I soggetti pubblici non possono richiamare lo svolgimento delle funzioni istituzionali

Alla loro riservatezza si è voluta garantire una maggiore protezione rispetto a quella accordata in genere ai dati personali, attraverso una disciplina più severa del loro trattamento. L'autonoma rilevanza attribuita ai dati sensibili risponde all'obiettivo generale di garantire in maniera efficace la persona relativamente a quelle informazioni ricollegabili agli aspetti più profondi e delicati della sua identità.

*Il trattamento dei dati sensibili* Ai sensi dell'art. 20 del Codice, il trattamento dei dati sensibili da parte di soggetti pubblici è consentito:

- in maniera diretta, quando vi sia una espressa disposizione di legge che specifichi la tipologia dei dati trattabili, le operazioni eseguibili e le finalità perseguite;
- se la legge invece non indica né la tipologia né le operazioni eseguibili, il

trattamento dei dati può avvenire solo previa emanazione, a cura dei soggetti che effettuano il trattamento, di un atto regolamentare, da adottare in conformità del parere reso al riguardo dal Garante, che identifichi i tipi di dati e di operazioni;

Il Ministro della Pubblica istruzione ha emanato il decreto 7 dicembre 2006, n.305 "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196

**Il Garante ha emanato le Linee Guida in materia di trattamento dei dati personali di lavoratori per le finalità di gestione del rapporto di lavoro in ambito pubblico in data 14 giugno 2007 (G.U. 13 luglio 2007, n. 161)**

**Gli ambiti trattati sono i seguenti:**

*1. Assenze per malattia, certificati e visite mediche* - In caso di assenza per malattia all'amministrazione vanno consegnati certificati medici privi di diagnosi e con la sola indicazione dell'inizio e della durata dell'infermità. Se il lavoratore produce documentazione in cui è presente anche la diagnosi, l'ufficio deve astenersi dall'utilizzare queste informazioni e deve invitare il personale a non produrre altri certificati con le stesse caratteristiche. Particolari cautele devono essere adottate dall'ente pubblico quando tratta dati sulla salute dei dipendenti nei casi di visite medico legali, denunce di infortunio all'Inail, abilitazioni al porto d'armi e alla guida.

*Il trattamento dei dati personali dei lavoratori per la gestione del rapporto di lavoro in ambito pubblico*

*2. Diffusione dei dati in Internet* - Le amministrazioni devono assicurare l'esattezza, l'aggiornamento e la pertinenza dei dati pubblicati in rete e garantire il "diritto all'oblio", cioè una tutela dinamica della riservatezza delle persone (trascorso un certo periodo dalla pubblicazione è opportuno spostare i nominativi in un parte del sito dove non siano più rintracciabili dai motori di ricerca esterni). Nelle graduatorie relative a concorsi o selezioni vanno riportati solo dati pertinenti (elenchi nominativi abbinati ai risultati, elenchi di ammessi alle prove scritte o orali, no a recapiti telefonici, codice fiscale ecc.) É sempre vietata la diffusione di informazioni sulla salute del lavoratore o dei familiari interessati.

*3. Dati biometrici dei lavoratori pubblici* - Anche nell'ambito del pubblico impiego non è consentito un uso generalizzato dei dati biometrici dei dipendenti (impronte digitali, iride) per controllare le presenze o gli accessi sul luogo di lavoro. Il Garante può autorizzare l'attivazione di tali sistemi di rilevazione solo in presenza di particolari esigenze (aree adibite alla sicurezza dello Stato, torri di controllo, conservazione di oggetti di particolare valore) e con precise garanzie (verifica preliminare dell'Autorità, no ad archivi centralizzati, codice cifrato dell'impronta memorizzato solo nel badge del dipendente).

*4. Comunicazioni tra amministrazione e lavoratore* - Per prevenire la conoscenza ingiustificata di dati da parte di persone non autorizzate, l'amministrazione deve adottare forme di comunicazione con il dipendente protette e individualizzate: inoltrando le note in busta chiusa, inviandole all'e-mail personale o invitandolo a ritirare personalmente la documentazione

*Documento* In base al nuovo Codice, la misura minima del DPS deve essere adottata dal

*programmatico sulla sicurezza (DPS)* titolare di un trattamento di dati sensibili o giudiziari effettuato con strumenti elettronici, attraverso l'organo, ufficio o persona fisica a ciò legittimata in base all'ordinamento aziendale o della pubblica amministrazione interessata (art. 34, comma 1, lett. g), del Codice; regola 19 dell'Allegato B)

Nel DPS occorre descrivere i criteri e le modalità per ripristinare la disponibilità dei dati in caso di distruzione o danneggiamento delle informazioni o degli strumenti elettronici; occorre individuare poi i criteri da adottare per cifrare o per separare i dati idonei a rivelare lo stato di salute e la vita sessuale trattati da organismi sanitari ed esercenti le professioni sanitarie (regole 19.8 e 24 dell'Allegato B).

L'art. 141 prevede le forme di tutela differenziate all'interessato che ritiene siano state violate norme poste a garanzia del suo diritto alla privacy.

*Le forme di tutela* Il primo strumento offerto all'interessato è il reclamo circostanziato secondo le modalità previste dall'art. 142. A seguito di reclamo il garante può adottare, anche prima della chiusura del procedimento, vari provvedimenti sia disponendo il blocco o vietando il trattamento se illecito o potrebbe potenzialmente produrre pregiudizi per l'interessato. Può anche prevedere di invitare direttamente il titolare del dato per invitarlo a bloccare spontaneamente il trattamento.

Il secondo strumento è la segnalazione al Garante al fine di attivare un controllo.

L'ultimo strumento è il ricorso da proporre sempre al garante al fine di far valere i diritti di cui all'art. 7 (Allegato 1). Si tratta di una procedura che l'interessato può seguire solo se ha già esperito la richiesta nei confronti del titolare o del responsabile ai sensi dell'art. 8, c. 1 ed è decorso il termine di 15 gg. dal suo ricevimento. Il termine è portato a 30 gg. per i casi di notevole complessità, che va comunicata all'interessato.

*Risorse normative*

D.lgs 30.06.2003, n. 196, Codice in materia di protezione dei dati personali