



ISTITUTO COMPRENSIVO STATALE
"Selvazzano Dentro II - M. Cesarotti"



***Il Codice
della Privacy***

**Informativa n. 01
al Personale
in servizio**

VIGENTI DISPOSIZIONI DI LEGGE IN MATERIA DI TUTELA DEI DATI E DI CRIMINALITA' INFORMATICA ANCHE EUROPEE

INTRODUZIONE

Il **Codice privacy** è entrato in vigore il 1° gennaio 2004 e riunisce in un unico contesto la legge 675/1996 e gli altri decreti legislativi in materia, i regolamenti e i codici deontologici che si sono succeduti in questi anni.

Contiene inoltre importanti innovazioni tenendo conto sia della “giurisprudenza” del Garante che della direttiva UE 2000/58 sulla riservatezza nelle comunicazioni elettroniche.

In questo modulo vedremo:

- Il Quadro normativo di riferimento
- Come Nasce la legge sulla privacy

QUADRO NORMATIVO DI RIFERIMENTO

Le Basi del Testo Unico

La Gazzetta Ufficiale ha pubblicato l'8 gennaio 1997 il testo della legge 31.12.1996 n. 675 sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

L'approvazione del provvedimento di legge è stato il risultato di oltre dieci anni di dibattito e segna un decisivo passo in avanti a favore della tutela della privacy delle persone.

Le disposizioni europee che hanno gettato le basi per la normativa italiana sono in particolare tre:

- Convenzione consiglio d'Europa
- Direttiva UE 95
- Accordo di Schengen

Prima delle leggi

La legge sulla privacy nata alla fine del 1996 è uno dei provvedimenti che ha probabilmente più influenzato la vita quotidiana dell'uomo comune. Si tratta della prima difesa da parte dello Stato del diritto del cittadino alla riservatezza.

Prima dell'entrata in vigore della legge 675/96, c'erano comunque delle indicazioni Costituzionali relative alla salvaguardia del diritto alla privacy dei cittadini.

Si potrebbe così riassumere la situazione precedente all'emanazione della normativa:

- il diritto alla riservatezza esisteva, ed era previsto dalla nostra Costituzione, pur non essendo esplicitamente definiti i mezzi di tutela;
- la giurisprudenza, più che la legge, forniva le indicazioni per la tutela della riservatezza.

La tutela dei diritti

Abbiamo già detto che "**PRIVACY**" è un termine inglese che si riferisce a concetti di "riservatezza", "privatezza".

Oggi privacy non significa soltanto diritto di essere lasciati in pace o di proteggere la propria sfera privata, ma anche e soprattutto diritto di controllare l'uso e la circolazione dei propri dati personali.

Il diritto alla privacy e alla protezione dei dati personali, è un diritto fondamentale delle persone, ed è strettamente correlato alla salvaguardia della dignità umana, come sancito anche dalla Carta dei diritti fondamentali dell'Unione Europea.

Le misure minime di sicurezza

La legge 675/96 ha introdotto, per la prima volta nel nostro ordinamento, una ipotesi di reato per la omessa adozione delle misure necessarie a garantire la sicurezza dei dati.

Con il successivo D.P.R. 28 luglio 1999 n. 318, è stato predi-

Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, è punito con la reclusione sino ad un anno. Se dal fatto deriva nocumento, la pena è la reclusione da due mesi a due anni. Se il fatto è commesso per colpa si applica la reclusione fino ad un anno.

Art. 36 legge 675/96

sposto il regolamento con le norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali.

I dati e le pubbliche amministrazioni

Per evitare involontarie situazioni a rischio, e per adeguare la gestione dei dati della pubblica amministrazione alla regolamentazione prevista con la legge 675/96, sono stati indicati una serie di passi da compiere.

Entro il 31 dicembre 1999 le amministrazioni pubbliche, centrali e locali, dovevano avviare l'adeguamento alle norme sulla privacy relativamente al trattamento dei dati sensibili.

Le indicazioni sono state diramate dal Garante per la protezione dei dati personali, con il Comunicato stampa del 15 dicembre 1999.

In previsione di una legge che specifichi le finalità di rilevante interesse pubblico, i soggetti pubblici, con atto di natura regolamentare, adottano in conformità col parere espresso dal Garante, devono identificare e rendere pubblici i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi.

La sicurezza informatica

La "rivoluzione" apportata dalla legge 675—che sostanzialmente prevede un trattamento dei dati intimamente connesso al

consenso espresso dell'interessato—si ricollega anche al concetto di sicurezza informatica.

È necessario infatti:

- garantire la genuinità dei dati, impedendo alterazioni che ne possono mutare il significato originale;
- impedire le “esportazioni” non autorizzate d'informazioni riservate;
- impedire, in genere, l'utilizzo delle risorse del sistema per scopi diversi da quelli per i quali esso è stato progettato.

Il profondo mutamento di prospettiva segue anche l'evoluzione del fenomeno della cosiddetta **criminalità informatica**, che è pur sempre riconducibile alle esigenze di tutela della privacy.

La sicurezza dei dati

Lo sviluppo delle reti locali e la diffusione dei modem per i collegamenti su linea telefonica hanno introdotto nel dibattito tecnico giuridico sulla materia, l'argomento della prevenzione di possibili attacchi al sistema provenienti “dall'esterno” (ad opera degli hachers o per causa dei virus informatici).

L'art. 15 della legge 675 dispone che *“I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed 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”*.

La sicurezza in Europa

In data 11 dicembre 2003 è entrata in vigore la direttiva dell'Unione Europea sulla privacy nelle comunicazioni che disciplina le questioni relative alla sicurezza e alla privacy dei dati.

Questa nuova direttiva è stata studiata per integrare l'esistente direttiva dell'U.E. sulla protezione dei dati.

Le due sezioni più importanti della normativa europea sulla privacy sono:

- la direttiva U.E. sulla privacy nelle comunicazioni elettroniche (n. 2002/58/CE);
- la direttiva U.E. sulla protezione dei dati (n. 95/46/CE).

Il quadro normativo

Il quadro normativo che si va delineando è dunque il seguente:

- il gestore del sistema informativo ha il dovere di “**ridurre al minimo**” i rischi di distruzione o perdita accidentale dei dati;
- il gestore deve prevenire accessi non autorizzati al sistema informativo;
- per far ciò il gestore deve adottare “**misure di sicurezza**” adeguate all'importanza dei dati custoditi negli archivi e in linea con le conoscenze acquisite in base al progresso tecnologico.

Tra i casi di condotta colposa imputabili al titolare del trattamento dei dati, debbono farsi rientrare tutti i fatti contrari alla legge in cui il danno sia riconducibile direttamente alla omissione di cure e cautele che chiunque sarebbe tenuto ad adottare nelle medesime circostanze, come la omissione di una attività che il responsabile aveva il dovere di compiere.

Anche l'inosservanza di regole tecniche o norme di condotta costituisce una colposa negligenza, quindi, anche quando venga a mancare una specifica norma di legge che faccia obbligo di osservare una particolare linea di condotta, l'imprudenza, la negligenza o l'imperizia possono costituire elementi della colpa.

NASCE LA LEGGE SULLA PRIVACY

E Testo Unico fu

Il Testo Unico sulla privacy è entrato in vigore il 1° gennaio 2004 con D. Lg. n. 196/2003 e sostituisce la legge 675/1996 ed il suo D.P.R. di attuazione, il n. 318/99.

È stato elaborato sulla base delle seguenti disposizioni normative:

- Art. 1 legge 24 marzo 2001 n. 127 (delega al Governo per l’emanazione di un testo unico in materia di trattamento dei dati personali);
- Art. 26 legge 3 febbraio 2003 n. 14 (disposizioni per l’adempimento degli obblighi derivanti dall’appartenenza dell’Italia alle Comunità europee—legge comunitaria 2002);
- Legge 31 dicembre 1996 n. 675 e successive modificazioni;
- Legge 31 dicembre 1996 n. 676 (delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali);
- Direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995 n. 95/46/CE (tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati);
- Direttiva del Parlamento europeo e del Consiglio 12 luglio 2002 n. 2002/58/CE (trattamento dei dati personali e tutele della vita privata nel settore delle comunicazioni elettroniche).

Adempimenti

Il diritto alla privacy e alla protezione dei dati personali, è un diritto fondamentale delle persone, ed è strettamente correlato alla salvaguardia della dignità umana, come sancito anche dalla “Carta dei diritti fondamentali dell’Unione Europea”.

Il Codice prevede una serie di **adempimenti**, obbligatori per chiunque effettui il trattamento di dati, sia con strumenti cartacei sia elettronici.

Questi adempimenti riguardano in particolare:

- la **Notificazione al Garante** per trattamenti di dati sensibili e indicazione dei soggetti tenuti a tale notificazione (art. 37 e segg.);
- l'**Informativa** che il titolare deve fornire ai soggetti interessati al trattamento (art. 13);
- le **Misure minime di sicurezza** che devono essere adottate nel trattamento dei dati (art. 33 e segg.).

Notificazione al trattamento: questa dichiarazione deve essere effettuata al Garante per i trattamenti di dati sensibili.

A seguito dell'introduzione del Codice sono indicati analiticamente i soggetti tenuti a questo adempimento.

La notificazione deve essere effettuata prima di dare inizio al trattamento e non va ripetuta se non si modificano le caratteristiche del trattamento (quindi, se per esempio cambiano le finalità del trattamento o cambia la ragione sociale del titolare, la notificazione deve essere nuovamente presentata al Garante).

Tutte le notificazioni sono conservate in un "registro dei trattamenti" accessibile al pubblico.

Informativa: informazioni che il titolare deve fornire ai soggetti interessati al trattamento e le modalità del trattamento, l'ambito di comunicazione dei dati.

Nell'informativa si deve specificare:

- quali sono gli scopi e le modalità del trattamento;
- se l'interessato è obbligato o no a fornire i dati;
- quali sono le conseguenze se i dati non vengono forniti;
- a chi possono essere comunicati o diffusi i dati;
- quali sono i diritti riconosciuti all'interessato;
- se i dati sono presso l'interessato, oppure presso terzi;
- Chi sono il titolare e il responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax, etc.).

Misure minime di sicurezza: accorgimenti e dispositivi che devono essere adottati sia nel trattamento dei dati con strumenti elettronici che senza tale ausilio affinché i dati stessi non vengano distrutti o persi anche accidentalmente e che solo persone autorizzate possano avere accesso ai dati, che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui erano stati raccolti.

Modalità semplificate

Rispetto alla legge 675/96, il nuovo Codice introduce delle **modalità semplificate** per la raccolta del consenso.

Tali modalità sono applicabili per:

- **notificare** il trattamento dei dati al Garante;
- **informare** l'interessato relativamente ai dati personali raccolti presso il medesimo interessato o presso terzi;
- **manifestare** il consenso dei dati personali quando previsto dall'art. 76.

Semplificazione della notificazione

Il Nuovo Codice prevede la semplificazione della notificazione, cioè dell'atto con cui si segnalano all'Autorità i trattamenti di dati che si intende effettuare.

Con la nuova legge la notifica dovrà essere effettuata solo in particolari casi di trattamento di dati sensibili (specie se sanitari) con determinate modalità d'uso, ma anche per trattamenti particolarmente a rischio, effettuati con strumenti elettronici, nel campo della profilazione dei consumatori, oppure in relazione a procedure di selezione del personale e ricerche di marketing, nonché in ipotesi di utilizzo di informazioni commerciali e relative alla solvibilità.

Diminuiscono invece le ipotesi di notifica obbligatoria, e vengono snellite anche le modalità della stessa: solo per via telemati-

ca, seguendo le indicazioni del Garante per l'utilizzo della firma digitale.

Semplificazione dell'informativa

Per quello che riguarda l'informativa, l'interessato o la persona presso cui sono raccolti i dati devono essere informati preventivamente circa finalità, estremi identificativi del titolare del trattamento dei dati raccolti, etc., ma l'informativa può essere anche orale.

Il Garante può inoltre individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.

Semplificazione della raccolta del consenso

Il Codice della privacy sviluppa il principio del bilanciamento degli interessi con uno snellimento degli adempimenti a carico dei titolari di trattamento dei dati.

Resta sostanzialmente confermata la necessità del consenso, ma, come vedremo in seguito, si prevedono alcune ipotesi di esonero con riferimento a settori specifici.



PRESENTAZIONE ED ANALISI DETTAGLIATA DEL D. LGS. N. 196 DEL 30 GIUGNO 2003

INTRODUZIONE

Il Testo Unico sulla privacy è entrato in vigore il 1° gennaio 2004 con il Decreto Legislativo n. 196 del 30 giugno 2003 e sostituisce la legge 675/1996 e il suo D.P.R. di attuazione, il n. 318/1999.

Il nuovo “Codice in materia di protezione dei dati personali”, o più semplicemente “Codice privacy” contiene importanti innovazioni dal punto di vista normativo, introdotte alla luce delle indicazioni fornite dal Garante e della direttiva U.E. 58/2002 sulla riservatezza nelle comunicazioni elettroniche.

In questo modulo affronteremo i seguenti argomenti:

- Sintesi del provvedimento
- Regole generali per il trattamento dei dati

SINTESI DEL PROVVEDIMENTO

La struttura del Testo Unico

Il nuovo Testo Unico in materia di protezione dei dati personali, denominato “Codice della privacy” introduce nuove garanzie per i cittadini e razionalizza e semplifica le precedenti norme.

È suddiviso in tre parti:

- **la prima parte** è dedicata alle disposizioni generali, riordinate in modo tale da trattare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato;
- **la seconda parte** è la parte speciale, dedicata a specifici settori. Questa sezione, oltre a disciplinare aspetti in parte inediti (informazione giuridica, notificazioni di atti giudiziari, dati sui comportamenti debitori), completa anche la disciplina attesa da tempo per il settore degli organismi sanitari

- e quella dei controlli sui lavoratori;
- **la terza parte** affronta la materia delle tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante.

Finalità del Testo Unico

Le norme del Codice della privacy, in aderenza alla disciplina dell'Unione Europea, intendono garantire che il trattamento dei dati personali si rivolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. La tutela si estende anche ai diritti delle persone giuridiche.

Il Codice si applica al trattamento dei dati personali da chiunque effettuato nel territorio dello stato, con o senza mezzi elettronici, o comunque automatizzati.

I dati personali

Per **dati personali** si intendono tutte le informazioni relative a persone fisiche o giuridiche, oppure ad enti e associazioni, che consentano l'identificazione diretta o indiretta di questi stessi soggetti.

La comunicazione e la diffusione dei dati personali sono consentite, come il trattamento, con il consenso dell'interessato, o nel caso in cui ricorra un'ipotesi di esenzione. In ogni caso, non possono essere comunicati o diffusi i dati per i quali è stata ordinata la cancellazione, o quando è stato superato il periodo di tempo necessario al raggiungimento degli scopi, o per scopi diversi da quelli indicati nella notificazione del trattamento al Garante, ove prescritta.

Esiste inoltre una categoria di dati, i cosiddetti "**dati sensibili**", per i quali la legge prevede una tutela più forte rispetto agli altri.

Il Codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque sia stabilito in territorio nazionale.

Si applica anche al trattamento effettuato da parte di soggetti eventualmente extra-U.E. che utilizzino per il trattamento strumenti situati in Italia anche diversi da quelli elettronici, salvo che si tratti di un "mero transito di dati nell'U.E."

I dati sensibili

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, politico, filosofico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale, vengono definiti **dati sensibili** e possono essere trattati soltanto con il consenso scritto dell'interessato e con l'autorizzazione del Garante.

Per i soggetti pubblici il trattamento è consentito solo ed esclusivamente se è autorizzato da una legge, che specifichi quali sono i dati trattabili e le operazioni eseguibili, nonché le rilevanti finalità di interesse pubblico che si intendono perseguire.

In presenza di una previsione di legge che specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, i soggetti pubblici, con atto di natura regolamentare adottato in conformità col parere espresso dal Garante, devono identificare e rendere pubblici i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi.

I diritti dell'interessato

Il Codice rafforza ed integra i **diritti dell'interessato** (diritto ad ottenere conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati e la loro comunica-

zione in forma intelligibile; diritto di conoscerne la fonte, di sapere per quali finalità e con quali modalità sono trattati e se/a chi detti dati vengono comunicati) riconoscendo a quest'ultimo particolari tutele in relazione ai dati sensibili e, più in generale, il diritto di ottenerne l'aggiornamento, la rettifica/integrazione, la cancellazione, la trasformazione in forma anonima o il blocco, con attestazione che dette operazioni sono state portate a conoscenza anche di coloro ai quali i dati sono stati comunicati o diffusi.

Questi diritti sono riconosciuti all'interessato nei confronti del titolare/del responsabile del trattamento senza essere soggetti ad alcuna formalità specifica, essendo sufficiente la mera richiesta (reiterabile—salva l'esistenza di giustificati motivi—in un intervallo di tempo non inferiore ai novanta giorni) per posta elettronica, per fax o per raccomandata.

L'interessato può sempre opporsi al trattamento dei dati che lo riguardano, in particolare ove esso sia effettuato ai fini di invio di materiale pubblicitario o di vendita diretta, per il compimento di ricerche di mercato o di comunicazioni commerciali.

Per garantire l'effettivo esercizio dei diritti dell'interessato, il titolare è tenuto ad adottare idonee misure atte:

- ad agevolare, anche attraverso appositi programmi, l'accesso ai dati personali da parte dell'interessato;
- a semplificare le modalità ed a ridurre i tempi per il "riscontro" al richiedente, da effettuarsi oralmente oppure con "offerta in visione" mediante strumenti elettronici, purché la comprensione dei dati sia agevole, o ancora, su richiesta dell'interessato, con trasposizione dei suoi dati su cartaceo.

Qualora fosse opportuno, l'interessato può e deve, in primo luogo, agire direttamente nei confronti del titolare, del responsabi-

le, o tramite gli incaricati del trattamento, chiedendo che i suoi diritti, se violati, vengano ripristinati. L'interessato, dopo aver fatto valere i suoi diritti nei confronti del titolare del trattamento, in mancanza di soddisfazione della richiesta, può far valere i propri diritti dinanzi all'Autorità giudiziaria o con ricorso al Garante.

Se si sceglie la strada della giustizia ordinaria non è più possibile proporre ricorso al Garante.

L'informativa

L'interessato o la persona presso la quale sono raccolti i dati personali devono essere previamente informati per iscritto o oralmente circa:

- la finalità/modalità del trattamento cui i dati sono destinati;
- la natura obbligatoria/facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti/le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in quanto responsabili/incaricati, o nell'ambito della diffusione dei dati stessi;
- i diritti dell'interessato;
- gli estremi identificativi del titolare, o di un suo rappresentante stabilito in Italia.

Il consenso

Il Testo Unico prevede che, salvo alcune ipotesi specificatamente individuate, il trattamento dei dati da parte di privati o di enti pubblici economici non possa prescindere dal consenso espresso dell'interessato, che può riguardare l'intero trattamento ovvero una o più operazioni dello stesso. Il consenso si intende validamente prestato solo se:

- è espresso liberamente e specificatamente in relazione ad un trattamento chiaramente individuato;
- è documentato per iscritto;
- è preceduto dall'informativa all'interessato.

Nel caso specifico dei dati sensibili, il consenso deve essere manifestato in forma scritta.

Esclusione del consenso

Si esclude il consenso per il caso di:

- trattamento effettuato per adempiere a prescrizioni di legge/regolamenti/norme CE;
- trattamento necessario per eseguire un contratto di cui sia parte l'interessato o, prima della conclusione del contratto, per adempiere a specifiche richieste dell'interessato;
- trattamento di dati provenienti da pubblici registri, elenchi o atti di dominio pubblico;
- trattamento necessario per la salvaguardia della vita/incolumità fisica di un terzo;
- trattamento necessario per lo svolgimento di investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria;
- trattamento necessario, nei casi individuati dal Garante, per perseguire un interesse legittimo del titolare/del terzo destinatario dei dati;
- trattamento effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, ove il trattamento abbia ad oggetto dati degli aderenti o di soggetti che abbiano con l'ente dei contatti regolari;
- trattamento necessario, nel rispetto dei rispettivi codici deontologici, per scopi di archiviazione scientifica, statistica o storica.

Finalità del Testo Unico

Il Codice individua come **"trattamento dei dati personali"** qualunque operazione o complesso di operazioni svolte con o senza l'ausilio di strumenti elettronici, che concerne le operazioni di:

- raccolta dei dati;
- conservazione;

- blocco;
- interconnessione;
- cancellazione;
- estrazione;
- registrazione;
- consultazione;
- modificazione;
- comunicazione;
- distruzione;
- raffronto;
- organizzazione;
- elaborazione;
- utilizzo;
- diffusione;
- selezione.

REGOLE GENERALI PER IL TRATTAMENTO DEI DATI

Il trattamento dei dati

Il Codice per la tutela della Privacy prevede che i dati siano:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- 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 siano raccolti e successivamente trattati.

Il trattamento da parte dei soggetti pubblici

Per quello che riguarda il trattamento di dati da parte dei **sog-**

getti pubblici, questo è consentito soltanto per lo svolgimento delle funzioni istituzionali. Nel trattare i dati, il soggetto pubblico è tenuto all'osservanza dei presupposti e dei limiti di cui al Codice, anche in relazione alla diversa natura dei dati, nonché della legge e dei regolamenti.

Per il trattamento di dati sensibili e giudiziari, il Testo Unico stabilisce regole specifiche e dispone che per gli altri dati il trattamento da parte di un soggetto pubblico possa essere consentito anche in mancanza di una espressa previsione di legge o regolamento.

Comunicazione dei dati da parte dei soggetti pubblici

Relativamente alla comunicazione dei dati da parte dei soggetti pubblici, il Codice prevede che:

- **la comunicazione da soggetto pubblico a soggetto pubblico** è ammessa se prevista da una norma di legge/di regolamento o in mancanza, ove necessaria per lo svolgimento di funzioni istituzionali;
- **la comunicazione/diffusione da soggetto pubblico a privati/a enti pubblici economici**, è ammessa solo ove prevista da una norma di legge/di regolamento.

Inoltre, con specifico riferimento all'accesso a documenti amministrativi, il Testo Unico prevede che: *"... i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990 n. 241 e successive modifiche e dalle disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico"*.

Semplificazione del trattamento

Alla base del trattamento dei dati il Codice pone due **principi**:

- **di semplificazione**—il trattamento dei dati deve essere effettuato in modo da garantire il rispetto dei diritti di protezione dei dati personali, di riservatezza e d'identità personale, che devono essere contemperati con l'esigenza di semplificazione per l'esercizio di tali diritti da parte degli interessati nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.
- **di necessità**—con specifico riferimento al trattamento dei dati effettuato con mezzi informatici, l'utilizzazione dei dati personali—identificativi, deve essere ridotta al minimo e riservata ai soli casi in cui non possano essere utilizzati dati anonimi oppure non sia possibile ricorrere a modalità che permettano di identificare l'interessato solo in caso di necessità.

I codici deontologici e di buona condotta

L'articolo 12 del Testo Unico prevede l'applicazione di **Codici di deontologia e di buona condotta**.

Il Garante promuove, nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

Tali codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante.

Il rispetto delle disposizioni contenute nei codici deontologici costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici.

Trattamento di dati relativi a studenti

L'articolo 96 del Testo Unico ha per oggetto il trattamento dei dati relativi agli studenti.

Esso prevede che, al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le scuole e gli istituti scolastici di istruzione secondaria, su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità e indicati nell'informativa resa agli interessati.

I dati possono essere successivamente trattati esclusivamente per le predette finalità.

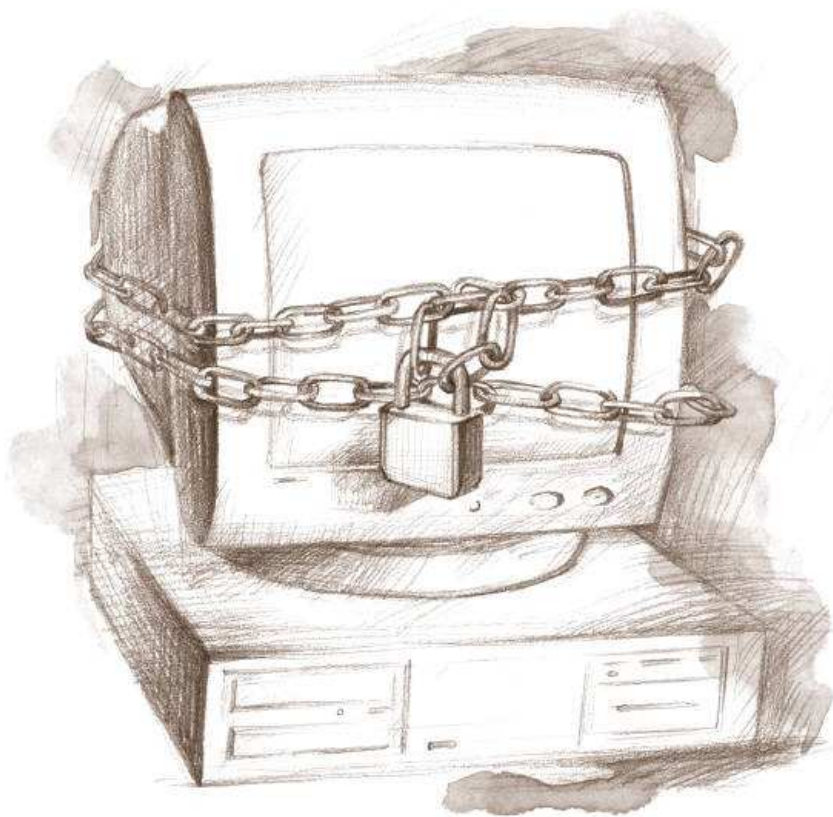
Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza, nonché alle vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.

Cessazione del trattamento

In caso di cessazione del trattamento, per qualsiasi causa, i dati devono essere:

- distrutti;
- ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
- conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
- 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 o di altre disposizioni rilevanti in materia di trattamento dei dati personali è priva di effetti ed è punibile amministrativamente.



ANALISI ED ILLUSTRAZIONE DEI RUOLI PREVISTI NELL'ORGANIZZAZIONE

INTRODUZIONE

I **soggetti** coinvolti nel trattamento dei dati personali, sono espressamente indicati dal Testo Unico sulla privacy, che ha provveduto anche a descriverne profilo e funzioni.

Tali soggetti sono:

- il **Titolare del trattamento**
- il **Referente del trattamento**
- l'**incaricato del trattamento**

Sul tema dei soggetti coinvolti nel trattamento dei dati personali, il Garante ha ritenuto di dover intervenire con alcune precisazioni, miranti, soprattutto, a **distinguere tra loro** le varie figure e ad evitare equivoci e confusione di ruoli.

IL TITOLARE DEL TRATTAMENTO

Definizione di Titolare

il **titolare del 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 a:

- le **finalità** perseguite;
- le **modalità** del trattamento dei dati personali;
- gli **strumenti utilizzati**, compreso il profilo della sicurezza.

Il titolare inoltre:

- **designa il referente** al trattamento;
- **specifica per iscritto i compiti del referente**;
- **vigila**, anche con verifiche periodiche, sull'**attività del re-**

ferente.

Precisazioni del Garante

Il **titolare del trattamento** è l'entità nel suo complesso o l'unità od organismo periferico che esercita il **potere decisionale** previsto dalla normativa sulla privacy, in modo del tutto **autonomo**. A questo proposito, il Garante ha specificato che il titolare del trattamento, nel caso di pubbliche amministrazioni, **non è la persona fisica che le rappresenta**, ma l'Amministrazione stessa, nella veste dell'organismo o unità che, come prevede la legge, detiene concretamente il potere decisionale.

Le funzioni del Titolare del trattamento

Cosa fa il Titolare del trattamento dei dati personali?

Il Titolare:

- **decide:** finalità, modalità, strumenti utilizzabili;
- **nomina:** il Referente;
- **assegna** l'ambito gestionale e i compiti del referente;
- **vigila.**

Le Misure di sicurezza

Il titolare del trattamento ha l'obbligo di garantire che i dati personali oggetto di trattamento siano **custoditi** e **controllati** in modo **da ridurre al minimo**, i rischi di:

- distruzione o perdita, anche accidentale, dei dati stessi;
- accesso non autorizzato;
- trattamento non consentito o non conforme alle finalità della raccolta.

Questa garanzia è assicurata mediante l'adozione di idonee e preventive **misure di sicurezza**.

Le misure di sicurezza vengono trattate nel modulo: Misure di sicurezza adottate dall'Amministrazione.

Precisazioni del garante

Anche i dati non organizzati in un archivio sono soggetti alle norme sulla privacy.

La semplice raccolta da parte di un ente di dati personali, anche se non inseriti in banche dati, costituisce un trattamento di dati ed è quindi soggetto alle sue norme.

Il principio è stato ribadito dal Garante in risposta ad alcuni quesiti posti da diversi Comuni italiani.

La legge sulla privacy, infatti, non riguarda solo i dati strutturalmente organizzati in banche dati o archivi, ma tutti i “trattamenti di dati personali” e quindi le varie operazioni che li costituiscono.

questo significa che bisogna garantire agli interessati i diritti previsti dalla legge, relativi all’accesso ai dati, integrazione, cancellazione, opposizione al loro trattamento e provvedere alla nomina delle figure responsabili del trattamento e adottare le misure di sicurezza per la salvaguardia delle informazioni.



IL REFERENTE

Definizione di Referente

Il **referente del trattamento** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che **siano preposti dal titolare al trattamento di dati personali**.

La designazione del referente è **facoltativa** ed è effettuata individuando i soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di privacy.

Il referente deve effettuare il trattamento, **attenendosi alle istruzioni impartite dal titolare**.

Precisazioni del Garante

Possono essere designati responsabili (o referenti) anche **più soggetti**, tra i quali è possibile prevedere una suddivisione di compiti, qualora ciò sia necessario per esigenze organizzative.

Sulla **designazione dei responsabili**, il Garante ha suggerito che, laddove sia compatibile con l'organizzazione o le attività dell'ente, siano designate responsabili le persone **relazione alla funzione svolta**, in modo tale da creare degli automatismi che vanno a tutto vantaggio degli adempimenti burocratici.

L'INCARICATO DEL TRATTAMENTO

Definizione di incaricato

Sono **incaricati del trattamento**, le persone fisiche **autorizzate** a compiere **operazioni di trattamento** dal titolare o dal referente.

Le operazioni di trattamento possono essere effettuate solo da incaricati, che operano sotto la diretta autorità del titolare o del

referente, attenendosi alle istruzioni impartite.

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

Precisazioni del Garante

Si considera **incaricata** anche la persona fisica **preposta ad una unità**, per la quale sia stato individuato per iscritto l'ambito del trattamento consentito agli addetti dell'unità stessa.

Per la **nomina degli incaricati** del trattamento, il **Garante** ha puntualizzato la necessità che tale compito sia formalmente attribuito a **tutti i soggetti che materialmente trattano dati personali**.



PANORAMICA DEGLI ADEMPIMENTI IN TEMA DI PRIVACY

INTRODUZIONE

La precedente legge 675/1996 prevedeva già l'obbligo di notificazione, con il nuovo Codice in materia di protezione dei dati personali la notificazione è stata semplificata.

In questo modulo tratteremo:

- la **Notificazione del trattamento**
- la **Modalità di notificazione**
- gli **Obblighi di comunicazione**
- le **Autorizzazioni generali**
- le **Richieste di autorizzazioni**

NOTIFICAZIONE DEL TRATTAMENTO

Definizione

La **notificazione** è una dichiarazione con la quale un soggetto pubblico o privato rende nota al Garante, per la protezione dei dati personali, l'esistenza di un'attività di raccolta e di utilizzazione dei dati personali, svolta quale autonomo titolare del trattamento.

Viene trasmessa al Garante, in via telematica, tramite il sito **www.garanteprivacy.it**, e utilizzando la procedura indicata nelle istruzioni.

Per le attività di trattamento dei dati che non esistevano prima del 1° gennaio 2004, la notificazione va effettuata prima che inizi il trattamento medesimo.

Per le attività che erano già in essere prima del 1° gennaio 2004, la notificazione poteva essere effettuata entro il 30 aprile 2004.

La **notificazione riguarda l'attività di trattamento di dati personali** e non una banca dati o un archivio in quanto tale: può aversi infatti un trattamento anche se materialmente i dati non sono organizzati in una banca dati.

Trattamenti da notificare

Il titolare del trattamento deve notificare al Garante il trattamento di dati personali cui intende procedere, solo se questo riguarda:

- **dati genetici, biometrici o dati che indicano la posizione geografica** di persone od oggetti mediante una rete di comunicazione elettronica;
- **dati idonei a rilevare 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, rilevazioni di malattie mentali, infettive e diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- **dati idonei a rilevare 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;
- **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;
- **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;
- **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.

Che fine fanno le notificazioni?

Il Garante inserisce le notificazioni ricevute in un registro dei trattamenti accessibile a chiunque e determina le modalità per la sua consultazione gratuita per via telematica, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio.

Le notizie accessibili tramite la consultazione del registro possono essere trattate per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali. Il cittadino può così acquisire notizie e può utilizzarle per le finalità di applicazione della disciplina in materia di protezione dei dati personali (ad esempio, per esercitare il diritto di accesso ai dati o altri diritti riconosciuti dal Codice in materia di protezione dei dati personali).

Mediante il registro saranno effettuati controlli sui trattamenti oggetto di notificazione, verificando le notizie in essa contenute.

MODALITÀ DI NOTIFICAZIONE

Quando notificare

La notificazione deve precedere l'inizio del trattamento (art. 38, comma 1) e può riguardare uno o più trattamenti con finalità correlate.

Chi esegue la notificazione secondo la nuova procedura deve dichiarare che effettua una “**nuova notificazione**”, anche se in passato ha già presentato una notificazione in base alla legge n. 675/1996.

Ulteriori eventuali notificazioni costituiscono “**modifiche del**

trattamento” (mutamento di taluno degli elementi previsti nella notificazione stessa), oppure **“cessazione del trattamento”** (nel caso in cui l’intero trattamento precedentemente notificato venga a cessare definitivamente).

Come notificare

La “nuova notificazione” va eseguita unicamente in via telematica, compilando i campi del modello disponibile sul sito internet www.garanteprivacy.it.

Non sono previste e ammesse altre modalità.

A differenza della notificazione prevista dalla legge n. 675/1996, non è quindi possibile utilizzare modelli cartacei o dischetti, né per la compilazione, né per l’invio.

Compilazione della notificazione

Per la compilazione della notificazione è necessario collegarsi all’indirizzo: [“web.garanteprivacy.it/rgt/NotificaTelematica.php”](http://web.garanteprivacy.it/rgt/NotificaTelematica.php).

Nella compilazione della notificazione i campi del modello contrassegnati con un asterisco sono obbligatori: la loro mancata compilazione impedisce il completamento della procedura di notificazione.

Il notificante deve osservare le seguenti indicazioni:

- selezionare dal menù principale **“COMPILAZIONE DELLA NOTIFICAZIONE”**;
- selezionare la casella **“NUOVA NOTIFICAZIONE”**;
- barrare una delle tre opzioni indicate (**“prima notificazione”** - **“modifica alla precedente notificazione”** - **“cessazione del trattamento”**);
- compilare i campi di interesse, utilizzando anche i menù a tendina;
- al termine delle descritte operazioni, salvare il *file* median-

- te l'apposito tasto;
- versare i diritti di segreteria *on line*, oppure compilare l'apposito riquadro indicando gli estremi del pagamento avvenuto;
 - sottoscrivere con firma digitale il *file* salvato;
 - trasmettere al Garante per via telematica la notificazione così completata mediante l'apposito tasto.

Il Garante invierà all'indirizzo di posta elettronica indicato dal notificante un messaggio di conferma del ricevimento della notificazione che attesta il buon esito della procedura.
E' possibile stampare copia della notificazione; tale copia cartacea, comunque, non deve essere trasmessa al Garante.

Convenzioni per la notificazione

La legge prevede che il Garante favorisca la disponibilità del modello per via telematica e la notificazione anche attraverso convenzioni stipulate con soggetti autorizzati in base alla normativa vigente, anche presso associazioni di categoria e ordini professionali.

E chi non è soggetto a notificazione?

Il titolare del trattamento che non è tenuto alla notificazione deve comunque fornire le notizie contenute nel modello di notificazione a chi ne fa richiesta (nell'esercizio del diritto di accesso e degli altri diritti riconosciuti all'interessato), a meno che il trattamento riguardi pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

OBBLIGHI DI COMUNICAZIONE

Comunicazioni al Garante

Il titolare del trattamento è **tenuto a comunicare** al Garante le seguenti circostanze:

- comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione;
- trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria (di cui all'articolo 110, comma 1, primo periodo).

Come effettuare la comunicazione

Per i casi di comunicazione obbligatoria descritti, questa deve essere trasmessa al Garante per via telematica osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento, oppure mediante telefax o lettera raccomandata.

I trattamenti oggetto di comunicazione possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione salvo diversa determinazione anche successiva del Garante.

AUTORIZZAZIONI GENERALI

Applicazione delle autorizzazioni generali

Le disposizioni del Codice sulla Privacy che prevedono un'autorizzazione del Garante sono applicate anche mediate il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti, pubblicate nella Gazzetta Ufficiale della Repubblica Italiana.

RICHIESTE DI AUTORIZZAZIONI

Chi deve presentare la richiesta

Il titolare del trattamento che rientra nell'ambito di applicazione di un'autorizzazione rilasciata nell'ambito delle autorizzazioni generali (art. 40) non è tenuto a presentare al Garante una ri-

chiesta di autorizzazione se il trattamento che indente effettuare è conforme alle relative prescrizioni.

Se le specifiche modalità del trattamento lo giustificano, il Garante può comunque prevedere la richiesta.

Come effettuare la richiesta

L'eventuale richiesta di autorizzazione deve essere formulata utilizzando esclusivamente il modello predisposto e reso disponibile dal Garante e trasmessa a quest'ultimo per via telematica, osservando le modalità di sottoscrizione e conferma del ricevimento.

La medesima richiesta e l'autorizzazione possono essere trasmesse anche mediante telefax o lettera raccomandata.

Se il richiedente è invitato dal Garante a fornire informazioni o ad esibire documenti, il termine di quarantacinque giorni previsto dal Codice, decorre dalla data di scadenza del termine fissato per l'adempimento richiesto.

In presenza di particolari circostanze, il Garante può rilasciare un'autorizzazione provvisoria a tempo determinato.

La risposta del Garante

Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali **la mancata pronuncia equivale a rigetto**.

Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

MISURE DI SICUREZZA ADOTTATE DALL'AMMINISTRAZIONE

INTRODUZIONE

Il nuovo Codice prevede ed indica una serie di misure definite “minime” di sicurezza da adottare per l'idoneo trattamento dei dati.

In questo modulo tratteremo di:

- **Misure minime ed idonee di sicurezza dei dati**
- **Misure minime per trattamenti con strumenti elettronici**
- **Illustrazione del Documento Programmatico sulla Sicurezza (DPS)**

MISURE MINIME ED IDONEE DI SICUREZZA DEI DATI

Il Codice entrato in vigore il 1° gennaio 2004 ha confermato e aggiornato la disciplina in materia di sicurezza dei dati personali e dei sistemi informatici e telematici introdotta nel 1996.

Diversi principi affermati dal nuovo Codice non sono nuovi, ma in particolare è stato confermato il principio (evidenziato con maggiore chiarezza dalle nuove disposizioni) secondo cui le “**misure minime**”, cioè di importanza tale da indurre il legislatore a prevedere anche una sanzione penale, sono solo una parte degli accorgimenti obbligatori in materia di sicurezza.

In materia, come già previsto dalla legge n. 675/1996, si distinguono **due distinti obblighi**:

- l'obbligo di ridurre al minimo determinati rischi;
- Il dovere di adottare in ogni caso le “misure minime”.

Obbligo di ridurre al minimo determinati rischi

I dati personali oggetto del trattamento devono essere custoditi e controllati, per contenere al massimo il rischio che possano essere distrutti, dispersi, conoscibili fuori dei casi consentiti o altrimenti trattati in modo illecito.

Come già previsto dalla legge 675/1996, l'inosservanza di questo obbligo rende il trattamento illecito.

Come già previsto dalla legge 675/1966, l'inosservanza di questo obbligo rende il trattamento illecito anche se non si determina un danno per gli interessati; viola inoltre i loro diritti, compreso il diritto fondamentale alla protezione dei dati personali che può essere esercitato nei confronti del titolare del trattamento ed espone a responsabilità civile per danno anche non patrimoniale qualora, davanti al giudice ordinario, non si dimostri di aver adottato tutte le misure idonee ad evitarlo.

Dovere di adottare in ogni caso le "misure minime"

Nel quadro degli accorgimenti più ampi da adottare per effetto dell'obbligo, occorre assicurare comune un livello minimo di protezione dei dati personali.

Ciò significa che l'omessa adozione di alcune misure indispensabili ("minime"), le cui modalità sono specificate tassativamente nell'Allegato B del Codice, costituisce anche reato.

Trattati "a mano"

Vediamo quali sono le modalità tecniche da adottare a cura del titolare, del referente (ove designato) e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

- Agli incaricati devono essere impartite istruzioni scritte finalizzate al controllo ed alla custodia degli atti e dei documenti contenenti dati personali.
- Quando agli atti e i documenti contenenti dati personali

sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e vanno restituiti al termine delle operazioni per i quali vengono affidati.

- L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati di vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Termini per l'adozione

Analogamente a quanto avveniva in passato, le misure minime sono diverse a seconda che il trattamento sia effettuato o meno con strumenti elettronici, oppure riguardi dati sensibili o giudiziari.

Le "misure minime" che erano già obbligatorie in passato devono comunque essere adottate, senza attendere il decorso di termini transitori.

Il termine transitorio che permetteva di adottare le misure entro il 30 giugno 2004 riguardava solo le nuove misure. Un più ampio periodo per l'adeguamento è previsto solo se, in casi del tutto particolari, ricorrano obiettive ragioni di natura tecnica.

Autorizzazioni al trattamento

Nel Testo Unico sulla Privacy il trattamento di dati personali effettuato con **strumenti elettronici** è consentito solo se sono adottate, nei modi previsti dal *disciplinare tecnico*, le seguenti misure minime:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di au-

- tenticazione;
- utilizzazione di un sistema di autorizzazione;
 - aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
 - protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
 - adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
 - tenuta di un aggiornato documento programmatico sulla sicurezza;
 - 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.

Sistema di autenticazione informatica

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Le **credenziali di autenticazione** consistono in un codice per l'identificazione dell'incaricato, associato o una parola chiave riservata, conosciuta solamente dal medesimo, oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato.

Sistema di autorizzazione

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso deve essere utilizzato un sistema di autorizzazione.

I profili di autorizzazione, per ciascun incaricato o per classi o-

mogenee di incaricati, devono essere individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Periodicamente e comunque almeno annualmente, è necessario verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

Nell'ambito dell'aggiornamento periodico—con cadenza almeno annuale—dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione (alla manutenzione degli strumenti elettronici), la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

I dati personali devono essere protetti contro il rischio di intrusione mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti devono essere effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento deve essere almeno semestrale.

Devono essere previste ed impartite istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con frequenza almeno settimanale, e devono essere approntati i sistemi di ripristino in caso di distruzione o danneggiamento dei dati.

Il disciplinare tecnico (allegato B), relativo alle misure minime di sicurezza è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

ILLUSTRAZIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS)

Che cos'è il DPS

Anche la redazione del DPS è una “misura minima”, prevista dall'Allegato B.

È l'unico documento in **grado di attestare l'adeguamento** della struttura alla normativa.

Il documento deve avere data certa e deve essere aggiornato annualmente, allo scopo di descrivere la situazione attuale (analisi dei rischi, distribuzione dei compiti, misure approntate, distribuzione delle responsabilità, etc.) ed il percorso di adeguamento prescelto dalla struttura per adeguarsi alla normativa privacy.

Si tratta di una misura non nuova, sebbene sia aumentato il numero dei soggetti che deve redigere il DPS e sia parzialmente diverso il suo necessario contenuto. Infatti, la precedente disciplina prevedeva già l'obbligo di predisporre e aggiornare il DPS, almeno annualmente, in caso di trattamento di dati sensibili o relativi a determinati provvedimenti giudiziari effettuato mediante elaboratori accessibili mediante una rete di telecomunicazioni.

Chi è tenuto a redigerlo

Entro il 31 marzo di ogni anno, il **titolare di un trattamento di dati sensibili o di dati giudiziari** redige anche attraverso il re-

sponsabile, 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 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 rilevare lo stato di salute e la vita sessuale, l'**individuazione dei criteri da adottare per la cifratura** o la separazione di tali dati dagli altri dati personali dell'interessato.

Le novità del DPS

Con il nuovo Codice, il DPS deve essere redatto da alcuni soggetti che non vi erano precedentemente tenuti (ad esempio, da

chi tratta dati sensibili o giudiziari, ma con elaboratori non accessibili mediante una rete di telecomunicazioni disponibili al pubblico).

Il contenuto stesso del DPS è arricchito da nuovi elementi che si aggiungono a quelli necessari in base alla precedente disciplina o ne specificano alcuni aspetti. Ad esempio, nel DPS occorre ora 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 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).

Suggerimenti

- Per agevolare la corretta redazione del Documento Programmatico sulla Sicurezza, il Garante ha messo a disposizione una guida, semplificata sulla base dei commenti pervenuti all'esito della consultazione pubblica.
- Si ricorda che una copia del DPS deve essere custodita presso la sede per essere consultabile e deve essere esibita in caso di controlli.
- Il titolare del trattamento deve dare conto nella relazione accompagnatoria del bilancio aziendale annuale dell'avvenuta redazione/aggiornamento del DPS.



MINISTERO DELLA PUBBLICA ISTRUZIONE
DECRETO 7 dicembre 2006, n.305
(in GU 15 gennaio 2007, 15)

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, recante «Codice in materia di protezione dei dati personali».

IL MINISTRO DELLA PUBBLICA ISTRUZIONE

Visto il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali»;

Visti in particolare gli articoli 20, comma 2, e 21, comma 2, del citato decreto legislativo 30 giugno 2003, n. 196, i quali dispongono che, nel caso in cui una disposizione di legge specifichi la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e giudiziari trattabili ed i tipi di operazioni su questi eseguibili, il trattamento e' consentito solo in riferimento a quei tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi;

Visto in particolare l'articolo 20, comma 2, del citato decreto legislativo 30 giugno 2003, n. 196, in cui e' stabilito che detta identificazione deve avvenire con atto di natura regolamentare adottato in conformità al parere espresso dal Garante, ai sensi dell'articolo 154, comma 1, lettera g) del medesimo decreto legislativo;

Considerato che possono spiegare effetti maggiormente signifi-

cativi per l'interessato le operazioni svolte, in particolare, pressoché interamente mediante siti web o volte a definire in forma completamente automatizzata profili o personalità di interessati, le interconnessioni e i raffronti, di cui all'articolo 4, comma 1, lettera a) del citato decreto legislativo 30 giugno 2003, n. 196, tra banche di dati gestite da diversi titolari oppure con altre informazioni sensibili e giudiziarie detenute dal medesimo titolare del trattamento, nonché la comunicazione dei dati a terzi;

Ritenuto di individuare analiticamente nelle schede allegato al presente regolamento, con riferimento alle predette operazioni che possono spiegare effetti maggiormente significativi per l'interessato, quelle effettuate da questa amministrazione, dalle istituzioni scolastiche e educative e dagli istituti regionali di ricerca educativa, in particolare le operazioni di interconnessione e di raffronto tra banche di dati gestite da diversi titolari, oppure con altre informazioni sensibili e giudiziarie detenute dal medesimo titolare del trattamento, nonché di comunicazione a terzi;

Ritenuto, altresì, di indicare sinteticamente anche le operazioni ordinarie che i diversi titolari indicati nel presente regolamento devono necessariamente svolgere per perseguire le finalità di rilevante interesse pubblico individuate per legge (operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione);

Considerato che per quanto concerne tutti i trattamenti di cui sopra è stato verificato il rispetto dei principi e delle garanzie previste dall'articolo 22 del citato decreto legislativo 30 giugno 2003, n. 196, con particolare riferimento alla pertinenza, non eccedenza e indispensabilità dei dati sensibili e giudiziari utilizzati rispetto alle finalità perseguite, all'indispensabilità delle predette operazioni per il perseguimento delle finalità di rilevante interesse pubblico individuate per legge, nonché all'esistenza di

fonti normative idonee a rendere lecite le medesime operazioni o, ove richiesta, all'indicazione scritta dei motivi;

Visto il provvedimento generale del Garante della protezione dei dati personali del 30 giugno 2005 (pubblicato in Gazzetta Ufficiale n. 170 del 23 luglio 2005);

Visto l'articolo 17, commi 3 e 4, della legge 23 agosto 1988, n. 400;

Visto il decreto del Presidente della Repubblica 11 agosto 2003, n. 319 relativo al regolamento dell'organizzazione e delle funzioni degli uffici di livello dirigenziale generale dell'amministrazione centrale e periferica del Ministero dell'istruzione, dell'università e della ricerca;

Vista la direttiva del Ministro della funzione pubblica in data 11 febbraio 2005, riguardante le «Misure finalizzate all'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel decreto legislativo 30 giugno 2003, n. 196»;

Ravvisata la necessità di provvedere ad identificare le tipologie di dati sensibili e giudiziari trattati nell'ambito dell'amministrazione dell'istruzione, le finalità d'interesse pubblico perseguite attraverso il trattamento dei citati dati, nonché le operazioni eseguite con gli stessi;

Sentito il Garante per la protezione dei dati personali di cui all'articolo 154, comma 1, lettera g) del citato decreto legislativo 30 giugno 2003, n. 196;

Udito il parere del Consiglio di Stato espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 6 novembre 2006;

Vista la comunicazione al Presidente del Consiglio dei Ministri effettuata, a norma dell'articolo 17, comma 3, della citata legge n. 400 del 1988, con nota del 21 novembre 2006;

Adotta il seguente regolamento:

Art. 1.

Oggetto del regolamento

1. Il presente regolamento, in attuazione degli articoli 20, comma 2, e 21, comma 2, del decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali», di seguito denominato «codice», identifica nelle schede allegate, che ne formano parte integrante, le tipologie di dati sensibili e giudiziari e di operazioni indispensabili per la gestione del sistema dell'istruzione, nel perseguimento delle finalità di rilevante interesse pubblico individuate dal codice e dalle specifiche previsioni di legge.

Art. 2.

Individuazione dei tipi di dati e di operazioni eseguibili

1. I dati sensibili e giudiziari individuati dal presente regolamento sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie quando la raccolta non avvenga presso l'interessato.
2. Le operazioni di interconnessione e raffronto con banche di dati di altri titolari del trattamento e di comunicazione a terzi individuate nel presente regolamento sono ammesse soltanto se indispensabili allo svolgimento degli obblighi o compiti di volta in volta indicati e solo per il perseguimento delle rilevanti finalità di interesse pubblico specificate, le operazioni sopraindicate sono inoltre svolte nel rispetto delle

disposizioni in materia di protezione dei dati personali e degli altri limiti stabiliti dalla legge e dai regolamenti.

3. I raffronti e le interconnessioni con altre informazioni sensibili e giudiziarie sono consentite soltanto previa verifica della loro stretta indispensabilità rispetto ai singoli casi e previa indicazione scritta dei motivi che ne giustificano l'effettuazione. Le operazioni effettuate utilizzando banche di dati di diversi titolari del trattamento e la diffusione di dati sensibili e giudiziari sono ammesse esclusivamente previa verifica della loro stretta indispensabilità in relazione ai singoli casi e nel rispetto dei limiti e con le modalità stabiliti dalle disposizioni legislative che le prevedono.
4. Sono inutilizzabili i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali.

Art. 3.

Norma finale

1. L'identificazione dei tipi di dati sensibili e giudiziari e delle operazioni su questi eseguibili, di cui alle schede allegate al presente decreto, e' aggiornata in relazione ad eventuali esigenze sopravvenute e, comunque, con periodicità triennale.

Il presente decreto, munito del sigillo di Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Roma, 7 dicembre 2006

Il Ministro: Fioroni

Visto, il Guardasigilli: Mastella

Registrato alla Corte dei conti il 5 gennaio 2007. Ufficio di controllo preventivo sui Ministeri dei servizi alla persona e dei beni culturali, registro n. 1, foglio n. 1.

SCHEDA N. 01

Indicazioni del trattamento e descrizione riassuntiva del contesto.

Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro:

- del personale dipendente dall'Amministrazione centrale e periferica del Ministero dell'istruzione, e dirigente, docente, educativo ed ATA delle istituzioni scolastiche ed educative, personale IRRE;
- Dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato.

Il trattamento concerne tutti i dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro.

1. *I dati inerenti lo stato di salute sono trattati per: l'adozione di provvedimenti di stato giuridico ed economico, verifica dell'idoneità al servizio, assunzioni del personale appartenente alle c.d. categorie protette, benefici previsti dalla normativa in tema di assunzioni, protezione della maternità, igiene e sicurezza sul luogo di lavoro, causa di servizio, equo indennizzo, onorificenze, svolgimento di pratiche assicurative, pensionistiche e previdenziali obbligatori e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortuni e/o sinistri e malattie professionali, fruizione di assenze, particolari esenzioni o permessi lavorativi per il personale e provvidenze, collegati a particolari condizioni di salute dell'interessato o dei suoi familiari, assistenza fiscale, mobilità territoriale, professionale e intercompartimentale;*

2. *I dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali;*
3. *I dati sulle convinzioni religiose per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose. I dati sulle convinzioni religiose vengono in rilievo anche ai fini del reclutamento dei docenti di religione;*
4. *I dati sulle convinzioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza;*
5. *I dati di carattere giudiziario sono trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l'adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato.*
6. *Le informazioni sulla vita sessuale possono desumersi unicamente in caso di eventuale rettificazione di attribuzione di sesso.*
7. *È di seguito descritto sinteticamente il flusso informativo dei dati.*

I dati sono raccolti su iniziativa degli interessati o previa richiesta dell'Ufficio presso i medesimi interessati, ovvero presso altri soggetti pubblici o privati, e sono trattati, sia in forma cartacea che telematica, per l'applicazione dei vari istituti disciplinati dalla legge e dai regolamenti in materia di selezione, reclutamento, gestione giuridica, economica, previdenziale, pensionistica, aggiornamento e formazione del personale.

Finalità di rilevante interesse pubblico perseguite

- **Art. 112:** *“instaurazione e gestione da parte dei soggetti*

pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato”;

- Art. 62: *“rilascio di documenti di riconoscimento”;*
- Art. 67: *“attività di controllo e ispettive”;*
- Art. 68: *“applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni”;*
- Art. 70: *“applicazione della legge 8 luglio 1998 n. 230, e delle altre disposizioni di legge in materia di obiezione di coscienza”;*
- Art. 72: *“rapporti con Enti di culto”;*
- Art. 73: *“supporto al collocamento e avviamento al lavoro”.*

Fonti normative

- Norme comuni: D.P.R. 10 gennaio 1957, n. 3; Legge 5 febbraio 1992, n. 104; Legge 12 marzo 1999, n. 68; D. Lgs. 30 marzo 2001, n. 165; Legge 15 luglio 2002, n. 145; R.D. 30 settembre 1922, n. 1290; Legge 24 maggio 1970, n. 336; Legge 30 dicembre 1971, n. 1204; D.P.R. 29 dicembre 1973, n. 1032; D.P.R. 29 dicembre 1973, n. 1092; Legge 7 febbraio 1979, n. 29; Legge 5 marzo 1990, n. 45; D. Lgs. 30 dicembre 1992, n. 503; Legge 14 gennaio 1994, n. 20; Legge 8 agosto 1995, n. 335; D.P.R. 20 febbraio 1998, n. 38; Legge 12 marzo 1999, n. 68; D.P.C.M. 20 dicembre 1999; Legge 8 marzo 2000, n. 53; D.P.R. 29 ottobre 2001, n. 461.
- Norme relative al personale amministrativo del Ministero Istruzione: Legge n. 472/1987; Contratti collettivi nazionali e contratti integrativi del Comparto Ministeri e della separata area della Dirigenza amministrativa.
- Norme per il personale delle istituzioni scolastiche: D. Lgs. 16 aprile 1994, n. 297; Legge 3 maggio 1999, n. 124; Leg-

ge 28 marzo 2003, n. 53; Legge 18 luglio 2003, n. 186; D. Lgs. 19 febbraio 2004, n. 59; Legge 6 giugno 2004, n. 14-3; Contratti collettivi nazionali e integrativi del Comparto Scuola e della separata area della Dirigenza scolastica; Legge 28 febbraio 1990, n. 37; Legge 23 dicembre 1998, n. 448; art. 26, commi 8, 9 e 10; D.P.R. 6 marzo 2001, n. 190; Legge 27 dicembre 2002, n. 289; art. 35; D. Lgs. 17 ottobre 2005, n. 227.

- Norme per il personale IRRE: D.P.R. 6 marzo 2001, n. 190.

Tipi di dati trattati

- Convinzioni: religiose, filosofiche, sindacali, d'altro genere;
- Stato di salute: patologie attuali, patologie pregresse, terapie in corso, dati sulla salute relativi anche ai familiari;
- Vita sessuale: solo in caso di rettificazione di attribuzione di sesso:
- Dati di carattere giudiziari (art. 4, comma 1, lett. E, del Codice)

Operazioni eseguite

PARTICOLARI FORME DI TRATTAMENTO:

- interconnessioni e raffronti di dati con altro titolare;
- Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;
- Comunicazione ai seguenti soggetti per le seguenti finalità:
 - Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;
 - Organi preposti al riconoscimento della causa di servizio/ equo indennizzo, ai sensi del DPR 461/2000;
 - Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del DPR n. 1124/1965;

- Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della Legge 68/1999;
- Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;
- Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità.
- Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge 18 luglio 2003, n. 186;
- Organi di controllo (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex Legge n. 20/94 e DPR 20 febbraio 1998, n. 38;
- Agenzia delle Entrate: ai fini degli obblighi fiscali del personale ex Legge 30 dicembre 1991, n. 413;
- MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335;
- Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art. 50, comma 3, D. Lgs. n. 165/2001).

ALTRE TIPOLOGIE PIÙ RICORRENTI DI TRATTAMENTI

Raccolta: presso gli interessati, presso terzi;

Elaborazione: in forma cartacea, con modalità informatizzate;

Altre operazioni ordinarie: registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA N. 2

Indicazioni del trattamento e descrizione riassuntiva del contesto

Gestione del contenzioso e procedimenti disciplinari.

Il trattamento dei dati sensibili e giudiziari concerne tutte le attività relative alla difesa in giudizio del Ministero dell'Istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili.

Finalità di rilevante interesse pubblico perseguite

- ⇒ Art. 112: *“instaurazione e gestione da parte dei soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato”*;
- ⇒ Art. 67: *“attività di controllo e ispettive”*;
- ⇒ Art. 71: *“attività sanzionatorie e di tutela”*.

Fonti normative

- ⇒ Norme comuni: Codice Civile; Codice Penale; Codice di Procedura Civile; Codice di Procedura Penale; D.P.R. 10 gennaio 1957, n. 3; D.P.R. 24 novembre 1971, n. 1199; Legge 6 dicembre 1971, n. 1034; Legge 15 marzo 1997, n. 59; Legge 21 luglio 2000, n. 205; D. Lgs. 28 agosto 2000, n. 274; Legge 27 marzo 2001, n. 97; D. Lgs. 30 marzo 2001, n. 165; Accordi quadro.
- ⇒ Norme per il personale amministrativo del Ministero Istruzione: Contratti collettivi nazionali e integrativi del Comparto Ministeri e della separata area della Dirigenza amministrativa.
- ⇒ Norme per il personale delle istituzioni scolastiche e degli IRRE: D. Lgs. 16 aprile 1994, n. 297; D.P.R. 6 marzo 2001, n. 190; Contratti collettivi nazionali e integrativi del Comparto Scuola e della separata area della Dirigenza scolastica.

Tipi di dati trattati

- ⇒ Origine: razziale, etnica;
- ⇒ Convinzioni: religiose, filosofiche, politiche, sindacali, d'altro genere;
- ⇒ Stato di salute: patologie attuali, patologie pregresse, terapie in corso, dati sulla salute relativi anche ai familiari;ù
- ⇒ Vita sessuale
- ⇒ Dati di carattere giudiziario (art. 4, comma 1, lett. E, del Codice.

Operazioni eseguite

PARTICOLARI FORME DI TRATTAMENTO:

Comunicazione con altri soggetti pubblici o privati:

- ⇒ Ministero del Lavoro e delle Politiche Sociali: per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi a Collegi di conciliazione ex D. Lgs. 30 marzo 2001, n. 165;
- ⇒ Organi arbitrali: per lo svolgimento delle procedure arbitrali ai sensi dei CCNL di settore;
- ⇒ Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di giustizia;
- ⇒ Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria: per l'esercizio dell'azione di giustizia;
- ⇒ Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

ALTRE TIPOLOGIE PIÙ RICORRENTI DI TRATTAMENTI

Raccolta: presso gli interessati; presso terzi;

Elaborazione: in forma cartacea, con modalità informatizzate;

Altre operazioni ordinarie: registrazione, organizzazione, conservazione, consultazione; modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA N. 3

Indicazione del trattamento e descrizione riassuntiva del contesto

Organismi collegiali e commissioni istituzionali

Il trattamento dei dati sensibili è necessario per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero Istruzione e dell'ordinamento scolastico. Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, delle famiglie e delle associazioni sindacali.

Il dato sensibile trattato è quello dell'appartenenza alle organizzazioni sindacali, con riferimento agli organismi o comitati che richiedano la partecipazione di rappresentanti delle organizzazioni sindacali.

Finalità di rilevante interesse pubblico perseguite

- ⇒ Art. 65: “pubblicità dell'attività di organi”.
- ⇒ Art. 95: “dati sensibili e giudiziari relativi alle finalità di istruzione e di formazione in ambito scolastico, professionale, superiore o universitario”.

Fonti normative

D. Lvo n. 297/1994; Contratti collettivi nazionali e integrativi di comparto.

Tipi di dati trattati

- ⇒ Convinzioni sindacali;
- ⇒ Dati di carattere giudiziario (art. 4, comma 1, lett. E, del Codice).

Operazioni eseguite

ALTRE TIPOLOGIE PIÙ RICORRENTI DI TRATTAMENTI

- ⇒ Raccolta: presso gli interessati, presso terzi;
- ⇒ Elaborazione: in forma cartacea, con modalità informatizzate;
- ⇒ Altre operazioni ordinarie: registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA N. 4

Indicazioni del trattamento e descrizione riassuntiva del contesto

Attività propedeutiche all'avvio dell'anno scolastico

I dati sono forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio nelle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali. Nell'espletamento delle attività propedeutiche all'avvio dell'anno scolastico da parte delle istituzioni scolastiche, possono essere trattati dati sensibili relativi:

- ⇒ *alle **origini razziali ed etniche**, per favorire l'integrazione degli alunni con cittadinanza non italiana;*
- ⇒ *alle **convinzioni religiose**, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento;*
- ⇒ *allo **stato di salute**, per assicurare l'erogazione del sostegno agli alunni diversamente abili e per la composizione delle classi;*
- ⇒ *alle **vicende giudiziarie**, per assicurare il diritto allo studio anche a soggetto sottoposti a regime di detenzione; i dati giudiziari emergono anche nel caso in cui l'autorità giudiziaria abbia predisposto su programma di protezione nei confronti dell'alunno nonché nei confronti degli alunni che abbiano commesso reati.*

Finalità di rilevante interesse pubblico perseguite

Le finalità di cui agli artt. 68, 73, 86, 95 del D. Lgs. 30 giugno 2003, n. 196.

Fonti normative

Leggi regionali sul diritto allo studio ai sensi del D.P.R. 24 luglio 1977, n. 616; Legge 25 marzo 1985, n. 121; Legge 5 febbraio 1992, n. 104; D. Lgs. 16 aprile 1994, n. 297; Legge 24 giugno 1997, n. 196; D. Lgs. 31 marzo 1998, n. 112; D.P.R. 24 giugno 1998, n. 249; D.P.R. 8 marzo 1999, n. 275; D.P.R. 31 agosto

1999, n. 394; Legge 10 marzo 2000, n. 62; Legge 28 marzo 2003, n. 53; D. Lgs. 19 febbraio 2004, n. 59; D. Lgs. 15 aprile 2005, n. 76; D. Lgs. 17 ottobre 2005, n. 226.

Tipi di dati trattati

- ⇒ Origine: razziale, etnica;
- ⇒ Convinzioni: religiose, d'altro genere;
- ⇒ Stato di salute: patologie attuali, patologie pregresse, terapie in corso, dati sulla salute relativi anche ai familiari;
- ⇒ Dati di carattere giudiziario (art. 4, comma 1, lettere E, del Codice).

Operazioni eseguite

PARTICOLARI FORME DI TRATTAMENTO

Comunicazione ai seguenti soggetti per le seguenti finalità:

1. agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgs. 31 marzo 1998, n. 112; limitatamente ai dati indispensabili all'erogazione del servizio;
2. ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
3. Alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la predisposizione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104.

ALTRE TIPOLOGIE PIÙ RICORRENTI DI TRATTAMENTI

- ⇒ Raccolta: presso gli interessati; presso terzi;
- ⇒ Elaborazione: in forma cartacea, con modalità informatizzate;
- ⇒ Altre operazioni ordinarie: registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, raffronto, utilizzo, blocco, cancellazione e distruzione.

SCHEDA N. 5

Indicazioni del trattamento e descrizione riassuntiva del contesto

Attività educativa, didattica e formativa, di valutazione

Nell'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami, da parte delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali, possono essere trattati dati sensibili relativi:

- ⇒ *alle **origini razziali ed etniche** per favorire l'integrazione degli alunni con cittadinanza non italiana;*
- ⇒ *alle **convinzioni religiose** per garantire la libertà di credo religioso;*
- ⇒ *allo **stato di salute**, per assicurare l'erogazione del servizio di refezione scolastica, del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate e ai viaggi di istruzione;*
- ⇒ *ai **dati giudiziari**, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione;*
- ⇒ *alle **convinzioni politiche**, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei genitori.*

I dati sensibili possono essere trattati per le attività di valutazione periodica e finale, per le attività di orientamento e per la compilazione delle certificazioni delle competenze.

Finalità di rilevante interesse pubblico perseguite

Le finalità di cui agli artt. 68, 73, 86, 95, del D. Lgs. 30 giugno 2003, n. 196.

Fonti normative

Leggi regionali sul diritto allo studio ai sensi del D.P.R. 24 luglio

1977, n. 616; Legge 25 marzo 1985, n. 121; Legge 5 febbraio 1992, n. 104; D. Lgs. 16 aprile 1994, n. 297; D.P.R. 10 ottobre 1996, n. 567; Legge 24 giugno 1997, n. 196; D. Lgs. 31 marzo 1998, n. 112; D.P.R. 24 giugno 1998, n. 249; D.P.R. 8 marzo 1999, n. 275; D.P.R. 31 agosto 1999, n. 394; Legge 10 marzo 2000, n. 62; Legge 28 marzo 2003, n. 53; D. Lgs. 19 febbraio 2004, n. 76; D. Lgs. 21 aprile 2005, n. 77; D. Lgs. 17 ottobre 2005, n. 226; D.P.R. 23 dicembre 2005, n. 301.

Tipi di dati trattati

- ⇒ Origine: razziale, etnica;
- ⇒ Convinzioni: religiose, filosofiche, politiche, d'altro genere;
- ⇒ Stato di salute: patologie attuali; patologie pregresse, terapie in corso, dati sulla salute relativi anche ai familiari;
- ⇒ Vita sessuale;
- ⇒ Dati di carattere giudiziario (art. 4, comma 1, lett. E, del Codice).

Operazioni eseguite

PARTICOLARI FORME DI TRATTAMENTO

Comunicazione ai seguenti soggetti per le seguenti finalità:

1. Alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente la carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio;
2. agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgs. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
3. ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
4. Agli Istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;
5. All'INAIL per la denuncia di infortuni ex-D.P.R. 30 giugno

- 1965, n. 1124;
6. alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro di istituto per l'Handicap e per la predisposizione e la verifica del Piano Educativo Individuale, ai sensi della Legge 5 febbraio 1992, n. 104;
 7. ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro, ai sensi della Legge 24 giugno 1997, n. 196 e del D. Lgs. 21 aprile 2005, n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio.

ALTRE TIPOLOGIE PIÙ RICORRENTI DI TRATTAMENTI

- ⇒ Raccolta: presso gli interessati, presso terzi;
- ⇒ Elaborazione: in forma cartacea, con modalità informatizzate;
- ⇒ Altre operazioni ordinarie: registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, raffronto, utilizzo, blocco, cancellazione e distruzione.

SCHEDA N. 6

Indicazione del trattamento e descrizione e riassuntiva del contesto

Scuole non statali

Nell'ambito delle procedure di accreditamento e autorizzazione delle istituzioni scolastiche non statali, l'Amministrazione scolastica periferica esercita attività di: concessione o revoca della parità; concessione della parifica (scuola primaria); concessione o revoca del riconoscimento legale (scuole secondarie); concessione o revoca della presa d'atto.

Dati sensibili emergono nel caso di attività di vigilanza e controllo effettuate dall'amministrazione centrale e periferica che prevedono l'accesso ai fascicoli personali dei docenti e degli alunni.

Dati sensibili sono, inoltre, trattati dai dirigenti scolastici delle scuole dell'infanzia e primarie incaricati della vigilanza sulle scuole non statali provviste di autorizzazione.

Finalità di rilevante interesse pubblico perseguite

Le finalità di cui all'art. 67 del D. Lgs. 30 giugno 2003, n. 196.

Fonte normativa

D. Lgs. 16 aprile 1994, n. 297; Legge 10 marzo 2000, n. 62; Legge 3 febbraio 2006, n. 27.

Tipi di dati trattati

- ⇒ Origine: razziale, etnica;
- ⇒ Convinzioni: religiose, filosofiche, politiche, sindacali, d'altro genere;
- ⇒ Stato di salute: patologie attuali, patologie pregresse, terapie in corso, dati sulla salute relativi anche ai familiari;
- ⇒ Dati di carattere giudiziario (art. 4, comma 1, lettera E, del Codice).

Operazioni eseguite

ALTRE TIPOLOGIE PIÙ RICORRENTI DI TRATTAMENTI

- ⇒ Raccolta: presso gli interessati, presso terzi;
- ⇒ Elaborazione: in forma cartacea, con modalità informatizzate;
- ⇒ Altre operazioni ordinarie: registrazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, cancellazione e distruzione.

SCHEDA N. 7

Indicazioni del trattamento e descrizione riassuntiva del contesto

Rapporti scuola-famiglie: gestione del contenzioso

Il trattamento di dati sensibili e giudiziari concerne tutte le attività connesse alla instaurazione di contenzioso (reclami, ricorsi,

esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, etc.) con gli alunni e con le famiglie, e tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandi e scuole speciali.

Finalità di rilevante interesse pubblico perseguite

Le finalità di cui agli artt. 67 e 71 del D. Lgs. 30 giugno 2003, n. 196.

Fonte normativa

Codice civile; Codice penale; Codice di procedura civile; Codice di procedura penale; D.P.R. 24 novembre 1971, n. 1199; D. Lgs. 16 aprile 1994, n. 297; D.P.R. 24 giugno 1998, n. 249; D.P.R. 8 marzo 1999, n. 275; Legge 28 marzo 2003, n. 53; D. Lgs. 19 febbraio 2004, n. 59; D. Lgs. 21 aprile 2005, n. 76; D. Lgs. 21 aprile 2005, n. 77; D. Lgs. 17 ottobre 2005, n. 226.

Tipi di dati trattati

- ⇒ Origine: razziale, etnica;
- ⇒ Convinzioni: religiose, filosofiche, politiche, sindacali, d'altro genere;
- ⇒ Stato di salute: patologie attuali, patologie pregresse, terapie in corso, dati sulla salute relativi anche ai familiari;
- ⇒ Vita sessuale;
- ⇒ Dati di carattere giudiziario (art. 4, comma 1, lettera E, del Codice).

Operazioni eseguire

Comunicazione con altri soggetti pubblici e privati:

- ⇒ Avvocature dello Stato, per la difesa erariale e consulenze presso gli organi di giustizia;
- ⇒ Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia;
- ⇒ Liberi professionisti, ai fini di patrocinio o di consulenza,

compresi quelli di controparte per le finalità di corrispondenza.

ALTRE TIPOLOGIE PIÙ RICORRENTI DI TRATTAMENTI

- ⇒ Raccolta: presso gli interessati, presso terzi;
- ⇒ Elaborazione: in forma cartacea, con modalità informatizzate;
- ⇒ Altre operazioni ordinarie: registrazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.



ILLUSTRAZIONE DETTAGLIATA DEI COMPITI E DELLE RESPONSABILITA' CIVILI E PENALI

INTRODUZIONE

Il Testo Unico per la privacy sancisce che chiunque, essendovi tenuto, omette di adottare le misure necessarie ad assicurare la sicurezza dei dati è perseguibile sia civilmente che penalmente. La legge presume la colpa del titolare del trattamento, e invertendo l'onere della prova, pone a suo carico ogni possibile conseguenza dei danni cagionati a terzi, se non prova di avere adottato tutte le misure idonee ad evitare il danno.

In questo modulo prenderemo dettagliatamente in esame:

- le **Violazioni amministrative**
- gli **Illeciti penali**

VIOLAZIONI AMMINISTRATIVE

Le responsabilità

I soggetti tenuti al risarcimento dei danni causati dai trattamenti dei dati personali, sono:

- il **titolare**, ossia colui cui competono le decisioni in ordine alle finalità del trattamento e della sicurezza;
- il **responsabile**, ossia colui che è preposto dal titolare al trattamento dei dati, avendo "esperienza, capacità ed affidabilità", tale da fornire idonea garanzia del pieno rispetto delle disposizioni di legge in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Le violazioni previste

Chiunque, essendovi tenuto, non provveda all'adeguamento delle misure di sicurezza e agli adempimenti previsti dal Codice sulla privacy è responsabile civilmente nei confronti di terzi, ai sensi dell'art. 2050 del Codice Civile.

L'impatto sanzionatorio previsto dalla nuova normativa contempla le seguenti violazioni amministrative:

- **Omessa o inidonea informativa all'interessato;**
- **Omessa o incompleta notificazione;**
- **Omessa informazione o esibizione al Garante.**

Omessa o inidonea informativa all'interessato

La violazione delle disposizione relative **all'informativa**, è punita con la sanzione amministrativa del pagamento di una somma da 3.000,00 a 18.000,00 euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici o comunque di maggiore rilevanza del pregiudizio per uno o più interessati, da 5.000,00 a 30.000,00 euro.

Il Codice prevede inoltre che quando la sanzione risulta **inefficace** in ragione delle **condizioni economiche del contravventore**, la somma indicata può essere aumentata sino al triplo.

E' prevista anche la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

...e inoltre

Anche per la violazione della norma che regola la **cessione** dei dati o di altre disposizioni in materia di disciplina del trattamento dei dati o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da 5.000,00 a 30.000,00 euro.

La violazione della disposizione relativa ai dati personali idonei a rivelare lo stato di salute, è invece punita con la sanzione amministrativa del pagamento di una somma da 500,00 a 3.000

euro.

Omessa o incompleta notificazione

Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione, o indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da 10.000,00 a 60.000,00 euro.

Omessa informazione o esibizione al Garante

Per l'espletamento dei propri compiti il Garante può richiedere al titolare, al responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti.

Chiunque omette di fornire informazioni o di esibire i documenti richiesti dal Garante, così come chi omette di rilasciare le informazioni richieste in sede di esame di un ricorso, è punibile con la sanzione amministrativa del pagamento di una somma da 4.000,00 a 24.000,00 euro.

Anche in questo caso è prevista la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

Procedimento di applicazione

L'organo competente a ricevere i ricorsi e ad irrogare le sanzioni previste è il Garante.

ILLECITI PENALI

Le sanzioni penali

Il Codice sulla privacy applica le **sanzioni penali** nei casi di:

- **trattamento illecito dei dati;**
- **falsità nelle dichiarazioni e notificazione al Garante;**

- **omessa adozione delle misure minime di sicurezza previste;**
- **inosservanza dei provvedimenti adottati dal Garante.**

Il Testo Unico qualifica il trattamento dei dati personali in generale come **attività pericolosa**, ai sensi dell'art. 2050 del codice civile.

L'articolo sancisce il "**principio dell'inversione dell'onere della prova**", per il quale 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 ad evitarlo.

Trattamento illecito di dati

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli concernenti:

- **i trattamenti effettuati da soggetti pubblici** (art. 18);
- **il trattamento di dati diversi da quelli sensibili e giudiziari** (art. 19);
- **il consenso** (art. 23);
- **i dati relativi al traffico di abbonati ed utenti** (art. 123);
- **i dati relativi all'ubicazione di utenti o abbonati** (art. 126);
- **le comunicazioni indesiderate** (art. 130);

è punito,

- con la reclusione da sei a diciotto mesi se dal fatto deriva nocumento;
- con la reclusione da sei a ventiquattro mesi se il fatto consiste nella comunicazione o diffusione.

... e inoltre

Salvo che il fatto costituisca più grave reato, chiunque, al fine di

trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli concernenti:

- **il trattamento che presenta rischi** (art. 17);
- **i principi applicabili al trattamento di dati sensibili e giudiziari** (art. 20 e 21);
- **i principi applicabili al trattamento di dati idonei** a rivelare lo stato di salute, i dati sensibili e giudiziari trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato (art. 222, commi 8 e 11);
- **i divieti di comunicazione e diffusione** (art. 25);
- **le garanzie per i dati sensibili e giudiziari** (art. 26 e 27);
- **i trasferimenti vietati** (art. 45);

è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

Falsità nelle dichiarazioni e notificazioni al Garante

Chiunque, essendo tenuto alla notificazione come previsto dal codice, nella notificazione stessa, o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

Omessa adozione delle misure minime di sicurezza

Chiunque, essendovi tenuto, omette di adottare le misure minime volte ad assicurare un livello minimo di protezione dei dati personali è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.

All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non

eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi.

Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato.

Innoservanza dei provvedimenti adottati dal Garante

Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante relativo a:

- le decisioni adottate **sulla richiesta di autorizzazione al trattamento dei dati sensibili** (art. 26, comma 2);
- le decisioni adottate **sulla richiesta di autorizzazione al Trattamento dei dati genetici o donatori di midollo osseo** 90;
- le decisioni relativa **al blocco** in tutto o in parte di taluno dei dati, o **all'immediata sospensione** di una o più operazioni del trattamento, o **alla cessazione** del comportamento illegittimo (art. 150, commi 1 e 2);

è punito con la reclusione da tre mesi a due anni.

La violazione delle disposizioni relative a:

- **raccolta di dati e pertinenza** nell'ambito di annunci di lavoro e dati riguardanti prestatori di lavoro (art. 113, comma 1);
- **controllo a distanza** nell'ambito del divieto di controllo a distanza e telelavoro (art. 114);

è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300 (l'arresto da 15 giorni ad un anno).

La condanna per uno degli illeciti succitati comporta la pubblicazione della sentenza.

FUNZIONI DELL'UFFICIO DEL GARANTE

INTRODUZIONE

Il Garante per la protezione dei dati personali è un'autorità indipendente istituita dalla legge sulla privacy (legge 31 dicembre 1996 n. 675) per assicurare la tutela dei diritti e delle libertà fondamentali ed il rispetto della dignità nel trattamento dei dati personali.

In questo modulo prenderemo visione:

- della figura del **Garante per la protezione dei dati personali**
- dei **Compiti del Garante**
- del **Ruolo del Garante**

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Chi è costui

Con il termine **Garante** si indica un organo collegiale, composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di quattro anni rinnovabile.

Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione.

I quattro membri che compongono l'organo collegiale eleggono nel loro ambito un Presidente, il cui voto prevale in caso di parità. Eleggono altresì un vice presidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

I membri sono scelti tra persone che assicurino indipendenza e che siano esperti di riconosciuta competenza nelle materie del diritto o dell'informatica, garantendo la presenza di entrambe le

qualificazioni.

Le rinunce del Garante

Per tutta la durata dell'incarico, il presidente e i membri non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive.

All'atto dell'accettazione della nomina il presidente e i membri sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attività di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni (il personale collocato fuori ruolo o in aspettativa non può essere sostituito).

La legge e il codice etico

L'istituzione del Garante e della composizione del suo ufficio e delle attività affidate al collegio che lo compone, vengono trattate nel Decreto del Presidente della Repubblica n. 501 del 31 marzo 1998.

L'ufficio del Garante si è dotato inoltre di un proprio Codice Etico, che ha la finalità di recare i principi guida del comportamento dei soggetti che operano presso il Garante per la protezione dei dati personali.

La disponibilità delle informazioni

Al fine di offrire la più ampia diffusione alle informazioni relative sulle normative e le disposizioni a tutela dei dati dei cittadini, per fornire strumenti di consultazione immediati ed aggiornati e per agevolare al massimo la possibilità di far rispettare i propri diritti e di adempiere ai propri doveri, il Garante della privacy ha attivato un proprio sito internet.

Il sito è mantenuto in aggiornamento costante e riporta, di importanza fondamentale, tutti i provvedimenti emessi dal Garan-

te (che fanno giurisprudenza in questo ambito), nonché i facsimile dei modelli utilizzabili per gli adeguamenti di legge e le istruzioni per la loro compilazione.

www.garanteprivacy.it

COMPITI DEL GARANTE

Gli incarichi stabiliti

Abbiamo già detto che l'attività del Garante ha toccato praticamente tutti i settori della vita del nostro Paese ed in particolar modo gli interventi più importanti hanno riguardato i provvedimenti adottati in materia di attività delle pubbliche amministrazioni, sanità, lavoro, credito ed assicurazioni, giornalismo, telecomunicazioni, videosorveglianza, marketing.

Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al Nuovo Codice, ha in particolare il compito di svolgere una ben definita serie di incarichi.

La funzione di controllo del Garante

Il Garante svolge anche la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da regolamenti comunitari e, in particolare:

- dalla legge 30 settembre 1993, n. 388, e successive modificazioni, di ratifica ed esecuzione dei protocolli e degli accordi di adesione all'accordo di Schengen e alla relativa convenzione di applicazione;
- dalla legge 23 marzo 1998, n. 93 e successive modificazioni, di ratifica ed esecuzione della convenzione istitutiva dell'Ufficio europeo di polizia (Eurogol);
- dal regolamento (Ce) n. 515/978 del Consiglio, del 13

marzo 1997, e dalla legge 30 luglio 1998, n. 291 e successive modificazioni, di ratifica ed esecuzione della convenzione sull'uso dell'informatica nel settore doganale;

- dal regolamento (Ce) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'”Eurodac” per il controllo delle impronte digitali e per l'efficace applicazione della convenzione di Dublino;
- nel capitolo IV della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della convenzione medesima.

Collaborazione con l'autorità amministrativa

Il Codice prevede che il Garante cooperi con altre autorità amministrative indipendenti nello svolgimento dei rispettivi compiti.

A tale fine, il Garante può anche invitare rappresentanti di un'altra autorità a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorità, prendendo parte alla discussione di argomenti di comune interesse.

Il Garante può inoltre richiedere la collaborazione di personale specializzato addetto ad altra autorità.

Anche il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante, all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie dal Codice sulla Privacy.

Altri compiti del Garante

Oltre ai compiti espressamente previsti dal Codice, il Garante svolge una serie di attività che vanno dalla presentazione annuale delle attività del suo Ufficio effettuate attraverso la Rela-

zione Annuale al Parlamento, alla pubblicazione di bollettini e dossier, all'organizzazione di convegni e seminari. Oltre alle citate attività di ambito nazionale, il Garante svolge la sua attività anche nel contesto comunitario ed internazionale.

RUOLO DEL GARANTE

Le responsabilità

All'Ufficio del Garante, al fine di garantire la responsabilità e l'autonomia insite nella propria funzione, si applicano i principi riguardanti l'individuazione e le funzioni del responsabile del procedimento, nonché quelli relativi alla distinzione fra le funzioni di indirizzo e controllo, attribuite agli organi di vertice e le funzioni di gestione attribuite ai dirigenti, previste dal decreto legislativo n. 165 del 2001 relativo alle norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche.

Organico

Il ruolo organico del personale dipendente dall'Ufficio del Garante è stabilito nel limite di cento unità. Con propri regolamenti pubblicati nella Gazzetta ufficiale della Repubblica italiana, il Garante definisce:

- l'organizzazione e il funzionamento dell'Ufficio anche ai fini dello svolgimento dei compiti per esso previsti dal Codice;
- l'ordinamento delle carriere e le modalità di reclutamento del personale secondo le procedure previste;
- la ripartizione dell'organico tra le diverse aree e qualifiche;
- il trattamento giuridico ed economico del personale, e per gli incarichi dirigenziali tenuto conto delle specifiche esigenze funzionali e organizzative;
- la gestione amministrativa e la contabilità, anche in deroga alle norme sulla contabilità generale dello Stato, l'utilizzo

dell'avanzo di amministrazione nel quale sono iscritte le somme già versate nella contabilità speciale, nonché l'individuazione dei casi di riscossione e utilizzazione dei diritti di segreteria o di corrispettivi per servizi resi in base alle disposizioni di legge.

Personale

L'Ufficio del Garante, per motivate esigenze, può avvalersi di dipendenti dello Stato o di altre amministrazioni o enti pubblici collocati in posizione di fuori ruolo o equiparati nelle forme previste dai rispettivi ordinamenti, o in aspettativa, in numero non superiore complessivamente a venti unità e per non oltre il venti per cento delle qualifiche dirigenziali, lasciando non coperto un corrispondente numero di posti di ruolo.

Al suddetto personale deve essere corrisposta un'indennità pari all'eventuale differenza tra il trattamento erogato dall'amministrazione o dall'ente di provenienza e quello spettante al personale di ruolo, sulla base dell'apposita tabella di corrispondenza adottata dal Garante e comunque non inferiore al cinquanta per cento della retribuzione in godimento, con esclusione dell'indennità integrativa speciale.

In aggiunta al personale di ruolo, l'Ufficio può assumere direttamente dipendenti con contratto a tempo determinato, in numero non superiore a venti unità ivi compresi i consulenti assunti con contratto a tempo determinato.

Consulenti e segretezza

Se la natura tecnica o la delicatezza dei problemi lo richiedono, il Garante può avvalersi dell'opera di consulenti, i quali sono remunerati in base alle vigenti tariffe professionali o sono assunti con contratto a tempo determinato, di durata non superiore a due anni (rinnovabili per non più di due volte).

Il personale addetto all'ufficio del Garante ed i consulenti sono tenuti alla riservatezza su ciò di cui sono venuti a conoscenza,

nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete.

Qualifiche speciali

Il personale dell'Ufficio del Garante addetto agli accertamenti che prevedono accesso a banche dati, archivi o altre ispezioni attinenti l'art. 158 del Codice sulla Privacy, è individuato in numero non superiore a cinque unità e, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, assume la qualifica di ufficiale o agente di polizia giudiziaria.

La polizia giudiziaria (PG) svolge prevalentemente compiti investigativi, lavorando anche in stretta collaborazione con la Magistratura.

La sua attività spazia dalla raccolta di informazioni, all'accertamento dei fatti, alle inchieste, agli arresti, al ripristino—quando possibile— della situazione iniziale, alla prevenzione, all'analisi strategica e comparativa di fenomeni criminali, all'analisi criminale operativa in supporto all'inchiesta, all'impiego di metodologie tecnico scientifiche, alla collaborazione con altre forze di polizia intercantionali o internazionali.

Le spese per l'Ufficio del Garante

Le spese di funzionamento del Garante sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposito capitolo dello stato di previsione del Ministero dell'economia e delle finanze. Il rendiconto della gestione finanziaria dell'Ufficio del Garante è soggetto al controllo della Corte dei conti.



