

BREVE GUIDA ALLA PRIVACY

Per amministrazioni pubbliche ed enti privati

Forniamo di seguito, sotto forma di *ipertesto*, una breve guida al Codice in materia di protezione dei dati personali attraverso la risposta a quesiti tipo.

In apertura, consigliamo la lettura delle definizioni generali contenute nell'[art.4](#) del D.lgs.196/2003.

A chi si rivolge il Codice?

A chiunque (soggetto pubblico e privato) tratta dati personali nel territorio dello Stato, anche se i dati sono all'estero, o li tratta in territori fuori dell'Unione Europea e impiega strumenti situati nel territorio dello Stato.

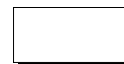
Sono escluse le persone fisiche che effettuano il trattamento dei dati per fini esclusivamente personali.

Cosa si intende per *trattamento*?

Qualunque operazione svolta sui dati personali.

Quindi: raccolta, registrazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, *comunicazione*, *diffusione*, cancellazione, distruzione di dati.

In particolare, tra *comunicazione* e *diffusione* la differenza sta nel fatto che i dati personali sono portati a conoscenza di uno o più soggetti ben identificati (nel primo caso), ad individui non preventivamente e specificatamente identificati (nel secondo caso).



Cosa si intende per *dato personale*?

Qualunque informazione relativa ad un soggetto (persona fisica, persona giuridica, ente, etc.) ben identificato o identificabile tramite il riferimento a qualsiasi altra informazione. [Approfondimento](#)

Quali *diritti* ha la persona cui si riferiscono i dati personali?

La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali, è definito "*interessato*" dal Codice. L'interessato ha diritto di **Accesso** ai dati che lo riguardano e tale diritto può essere esercitato senza che sia necessario instaurare subito una controversia dinanzi all'autorità giudiziaria o rivolgersi al Garante. [Approfondimento](#)

Perché adeguarsi?

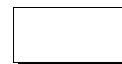
- 1) Adeguarsi non è una scelta, ma un **obbligo di Legge**.
- 2) Il mancato rispetto delle disposizioni comporta **sanzioni di tipo amministrativo** (fino a €180.000) e **penale** (fino a 2 anni di reclusione). [Approfondimento](#)
- 3) Adeguarsi significa lavorare in condizioni di **sicurezza**, in modo da ridurre al minimo i rischi di violazioni, e contribuisce a **migliorare l'immagine** dell'Ente.

Cosa vuole la *Legge*?

- 1) **Garantire** che il trattamento si svolga nel **rispetto**: della dignità - dei diritti e libertà fondamentali - del diritto alla riservatezza - del diritto alla protezione dei dati personali dell'interessato.
- 2) **Semplificare** l'esercizio dei **diritti** (dell'interessato) e l'adempimento degli **obblighi** (del Titolare del trattamento). [Approfondimento](#)

Chi e' *responsabile* della *privacy* in prima persona?

Il Codice stabilisce che al **Titolare** competono le decisioni in ordine alle finalità, alle modalità ed alla sicurezza del trattamento dei dati personali, pertanto egli è anche imputabile di fattispecie illecite o dannose (salvo le responsabilità personali).



Oltre al Titolare, sono previste 4 figure facoltative (tranne l'incaricato), di fatto indispensabili, con compiti specifici in merito alla privacy.

Tali figure sono: **Responsabile/i, incaricato/i, amministratore/i di sistema, custode/i delle password.** [Approfondimento](#)

Le regole sono le stesse per tutti?

No, si differenziano a seconda del **soggetto** che tratta i dati, a seconda dei tipi di **dati** trattati e del tipo di **trattamento** effettuato. [Approfondimento](#)

Quale documentazione bisogna predisporre?

- L'**Informativa agli interessati**
- Il **Documento Programmatico sulla Sicurezza** (DPS)
- Il **Regolamento**

[Approfondimento](#)

Quali adempimenti sono richiesti?

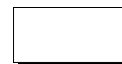
- La **Notificazione** al Garante
- La **Comunicazione** al Garante
- La **Richiesta di autorizzazione**

[Approfondimento](#)

Cosa intende il Codice per *sicurezza*?

I dati personali devono essere custoditi e controllati in modo da ridurre al minimo i rischi di: distruzione e perdita (anche accidentale); accesso non autorizzato; trattamento non consentito o non conforme alle finalità.

La custodia ed il controllo dei dati deve avvenire mediante misure di sicurezza idonee e preventive, ed in relazione alle conoscenze acquisite in base a: progresso tecnico; natura dei dati; caratteristiche del trattamento. [Approfondimento](#)



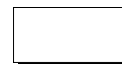
Come applicare il Codice?

Posto che il concetto di Privacy deve per prima cosa far parte del bagaglio culturale di ciascuno di noi, l'applicazione del Codice nell'Ente o nell'Azienda si attua in due fasi distinte:

- di impianto, nella quale operare nella struttura per definire ruoli, individuare le figure previste dalla legge, censire gli archivi contenenti dati personali, redigere i documenti richiesti;
- di regime, che richiede un impegno minore, ma continuo e prolungato nel tempo, tale da garantire costantemente la perfetta aderenza dell'operato dell'Amministrazione alla norma.

Il metodo che **Privacy&Sicurezza** propone si articola nelle seguenti 5 fasi:

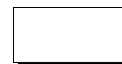
- 1 **Studio dell'organizzazione**, per stabilire le aree e le funzioni del trattamento.
- 2 **Formazione** di tutti coloro che operano nel trattamento dei dati personali (obbligatoria secondo legge).
- 3 **Progettazione**: dall'analisi sullo stato di applicazione della normativa, all'ideazione del "Sistema Privacy".
- 4 **Censimento** del patrimonio informativo (degli "ambienti", degli strumenti elettronici, degli archivi, dei trattamenti).
- 5 **Gestione**, sulla base del "Sistema Privacy" progettato, attraverso l'applicativo web "SoluzionePrivacy".



Art. 4 (Definizioni)

1. Ai fini del presente codice si intende per:

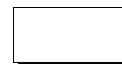
- "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
- "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, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;



- "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- "Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del presente codice si intende, inoltre, per:

- "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- "chiamata", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
- "reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- "rete pubblica di comunicazioni", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
- "servizio di comunicazione elettronica", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;
- "abbonato", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
- "utente", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
- "dati relativi al traffico", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;



- “dati relativi all’ubicazione”, ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell’apparecchiatura terminale dell’utente di un servizio di comunicazione elettronica accessibile al pubblico;
- “servizio a valore aggiunto”, il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all’ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;
- “posta elettronica”, messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell’apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

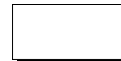
3. Ai fini del presente codice si intende, altresì, per:

- “misure minime”, il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell’articolo 31;
- “strumenti elettronici”, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- “autenticazione informatica”, l’insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell’identità;
- “credenziali di autenticazione”, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l’ autenticazione informatica;
- “parola chiave”, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- “profilo di autorizzazione”, l’insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- “sistema di autorizzazione”, l’insieme degli strumenti e delle procedure che abilitano l’accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

4. Ai fini del presente codice si intende per:

- "scopi storici", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
- "scopi statistici", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
- "scopi scientifici", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

[\[indietro\]](#)



Dati personali

La Legge distingue i dati **comuni** da quelli **particolari**.

Sono comuni: il nome, il cognome, l'indirizzo

I dati particolari, invece, si differenziano a loro volta in **sensibili** e relativi a provvedimenti giudiziari.

Alla prima categoria appartengono tutti quei dati che storicamente hanno dato luogo a discriminazioni, quali:

- l'origine razziale ed etnica;
- le convinzioni religiose, filosofiche o altro;
- le opinioni politiche, adesioni a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale;
- lo stato di salute;
- la vita sessuale.

I dati **relativi a provvedimenti giudiziari** sono quei dati idonei a rivelare:

- provvedimenti di cui all'art. 3 del T.U. del Casellario giudiziale:
 - in materia di casellario giudiziale;
 - di anagrafe delle sanzioni amministrative dipendenti da reato;
 - dei relativi carichi pendenti.
- la qualità di imputato o indagato (artt. 60 e 61 del Codice di procedura penale).

Infine, sono da segnalare i dati **semisensibili** (né sensibili né giudiziari) che presentano rischi specifici per i diritti e la dignità dell'interessato. Relativamente a questi dati, le misure e gli accorgimenti da adottare saranno prescritti dal Garante.

[\[indietro\]](#)



Diritto di Accesso

L'interessato ha diritto di:

- ottenere dal Titolare o dal Responsabile la conferma dell'esistenza di dati personali che lo riguardano e la loro comunicazione;
- conoscere il contenuto e l'origine dei dati, farli aggiornare, rettificare o integrare;
- farli cancellare se trattati illecitamente;
- conoscere i soggetti ai quali i dati possono essere comunicati;
- opporsi al trattamento se non pertinente allo scopo della raccolta o se finalizzato al marketing;
- opporsi a qualsiasi valutazione del comportamento fondata unicamente sul trattamento automatizzato volto a definire il profilo o la personalità.

L'interessato esercita il diritto di accesso attraverso l'invio di un'istanza rivolta, senza formalità, al Titolare o al Responsabile del trattamento dei dati personali che lo riguardano.

Il diritto di accesso non può essere esercitato se il trattamento dei dati personali è effettuato in materia di: riciclaggio, sostegno alle vittime di estorsioni, politica monetaria, investigazioni difensive, giustizia.

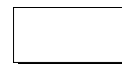
In caso di mancata o insoddisfacente risposta del Titolare o del Responsabile, l'interessato può adire l'autorità giudiziaria ordinaria o proporre ricorso al Garante.

A garanzia del diritto di accesso, il Titolare deve:

- adottare le misure necessarie ad agevolare l'accesso ai dati (anche con l'impiego di software ad hoc);
- semplificare le modalità e ridurre i tempi per il riscontro (anche con uffici e servizi per le Relazioni con il Pubblico).

Se i dati dell'interessato non esistono, il Titolare può chiedere un contributo spese non eccedente i costi della ricerca effettuata.

[\[indietro\]](#)



Cosa prescrive la Legge per il trattamento dei dati personali

I dati personali devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi;
- esatti e se necessario aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi originari.

I dati trattati in violazione alla Legge non possono essere utilizzati.

In caso di cessazione del trattamento, i dati saranno:

- distrutti;
- ceduti ad altro titolare (per il perseguimento degli stessi scopi);
- conservati a fini personali senza comunicarli ne diffonderli;
- conservati o ceduti a fini storici, statistici, scientifici (secondo legge).

[\[indietro\]](#)

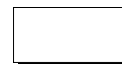


Figure che effettuano il trattamento

Il **Titolare** è la persona fisica, persona giuridica, pubblica amministrazione, ente, associazione, organismo cui competono le decisioni in ordine alle finalità, alle modalità ed alla sicurezza del trattamento dei dati personali. E' pertanto la figura centrale del sistema di protezione dei dati personali e centro di imputazione giuridica del trattamento.

Il **Responsabile** è la persona fisica, persona giuridica, pubblica amministrazione, ente, associazione, organismo preposto dal Titolare al trattamento dei dati personali. Inoltre:

- è una figura facoltativa (si pensi ad un piccolo negozio a conduzione familiare);
- è individuato tra soggetti che forniscono garanzie in materia di trattamento e sicurezza;
- possono essere designati più soggetti;
- i compiti sono specificati per iscritto e controllati dal Titolare con verifiche periodiche.

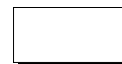
L'**Incaricato** è la persona fisica autorizzata, dal Titolare o dal Responsabile, a compiere operazioni di trattamento. Inoltre:

- è designato per iscritto, individuando l'ambito del trattamento e le specifiche mansioni;
- altrimenti è sufficiente l'appartenenza documentata ad una unità organizzativa nella quale è individuato l'ambito del trattamento.

L'**Amministratore di sistema** è colui che sovrintende il sistema operativo di un sistema di banche dati (in genere il Responsabile CED).

Il **Custode delle password** è la persona fisica, individuata per iscritto dal Responsabile, preposta alla custodia delle password (parole chiave) dei vari incaricati del trattamento.

[\[indietro\]](#)



Regole

Il Codice detta discipline differenti, a seconda che a trattare i dati personali sia un **soggetto pubblico**, o un **soggetto privato (o ente pubblico economico)**.

Nel caso di **soggetti privati (o enti pubblici economici)**, è necessario il *consenso* dell'interessato per il trattamento dei dati personali che lo riguardano, tranne in casi particolari individuati dal Codice. Tale consenso può essere chiesto per l'intero trattamento oppure per una o più operazioni dello stesso. E' valido se preceduto dall'*Informativa* sul trattamento e se espresso liberamente, in forma specifica e documentato per iscritto.

Il trattamento dei *dati sensibili* richiede il consenso in forma scritta.

Per i **soggetti pubblici**, il trattamento dei dati personali è consentito senza la resa del consenso da parte dell'interessato. Tuttavia tale trattamento, per essere lecito, deve necessariamente essere svolto per *finalità di tipo istituzionale* e non per altri scopi (che risulterebbero illeciti). In particolare:

- Il *trattamento di dati comuni* è consentito se previsto dalle funzioni istituzionali del soggetto pubblico, anche senza una norma di legge o di regolamento che individuino il trattamento.
- La *comunicazione* (che è un tipo di trattamento) *di dati comuni*, da soggetto pubblico *ad altri soggetti pubblici*, è consentita se lo prevede una norma di legge o di regolamento, in mancanza è necessario fare Comunicazione al Garante.
- La *comunicazione di dati comuni* rivolta *a soggetti privati* (o enti pubblici economici) e la *diffusione di dati comuni* è consentita solo in presenza di una norma di legge o di regolamento.
- Il *trattamento di dati sensibili e giudiziari* è consentito solo se lo prevede una norma di legge o di regolamento. Nel caso in cui la legge non specifichi i tipi di dati e le operazioni eseguibili, è necessario identificare gli uni e gli altri e renderli pubblici con atto di natura regolamentare (Regolamento). Infine, qualora il trattamento dei dati sensibili e giudiziari non sia previsto da alcuna legge, va fatta richiesta di Autorizzazione al Garante e quindi adottato un Regolamento. Il Garante per la Privacy ha predisposto schemi tipo di Regolamento che possono essere presi a modello dal Titolare del trattamento.

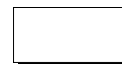
Il Garante della privacy ha individuato una rilevante finalità istituzionale nei trattamenti relativi a:

- tenuta dei registri di stato civile, APR, AIRE, liste elettorali, rilascio documenti (art. 62);
- cittadinanza, immigrazione e condizione dello straniero (art. 64);
- diritti politici e pubblicità dell'attività di organi (art. 65);



-
- materia tributaria e doganale (art. 66);
 - attività di controllo e ispettive (art. 67);
 - benefici economici ed abilitazioni (art. 68);
 - volontariato e obiezione di coscienza (art. 70);
 - interventi di sostegno psico-sociale in favore di soggetti che versano in condizioni di disagio sociale, economico o familiare (art. 73)
 - interventi di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto (art. 73);
 - assistenza nei confronti di minori, anche in relazione a vicende giudiziarie (art. 73);
 - indagini psico-sociali relative a provvedimenti di adozione anche internazionale (art. 73);
 - compiti di vigilanza per affidamenti temporanei (art. 73);
 - iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi (art. 73);
 - interventi in tema di barriere architettoniche (art. 73).

[\[indietro\]](#)



Documentazione

Informativa

Il Titolare, soggetto pubblico o privato, è tenuto ad informare preventivamente l'interessato (oralmente o per iscritto), circa:

- le finalità e le modalità del trattamento dei dati personali che detiene;
- la natura obbligatoria o facoltativa del conferimento dei dati personali;
- le conseguenze del rifiuto a rispondere;
- i soggetti ai quali i dati personali sono comunicati (ed anche i responsabili e gli incaricati che ne vengono a conoscenza);
- i diritti dell'interessato (art. 7);
- gli estremi del Titolare e del Responsabile/i;

L' Informativa è data all'interessato all'atto della registrazione dei dati personali che lo riguardano, oppure quando è prevista la loro comunicazione. Non è data quando il trattamento dei dati personali avviene in base ad obblighi di legge, di regolamento o di normativa comunitaria.

Il Garante ha inoltre previsto la possibilità di individuare con proprio provvedimento modalità semplificate per l'informativa fornita, ad esempio, da servizi telefonici di assistenza e di informazione al pubblico.

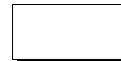
Infine, il Garante definirà a breve un modello semplificato di informativa in ambito sanitario, agevolmente utilizzabile anche dai medici di base.

Documento Programmatico Sulla Sicurezza

Il Documento Programmatico Sulla Sicurezza è la descrizione delle "politiche" e degli standard di sicurezza adottati all'interno dell'ente (sia pubblico che privato) per garantire la protezione, l'integrità, la conservazione e la tutela dei dati personali che detiene.

Il DPS va redatto entro il 31 di marzo di ogni anno, per il trattamento di dati sensibili e/o giudiziari che avviene a mezzo di strumenti elettronici. E' comunque consigliabile estenderlo a tutti i trattamenti svolti dall'ente, in quanto può aiutare concretamente a verificare il livello di sicurezza esistente. Ad esempio, il documento può essere utile a dimostrare, in caso di incidente, che sono state adottate tutte le misure minime idonee per la sicurezza dei dati, in considerazione del fatto che l'art. 31 del Codice inverte l'onere della prova.

Il DPS deve essere conosciuto e applicato da tutte le funzioni dell'ente ed è fatto obbligo al titolare del trattamento di riferire nella relazione di accompagnamento a ciascun bilancio d'esercizio circa l'avvenuta redazione o aggiornamento del DPS, proprio allo scopo di mantenere informati gli organi di vertice.

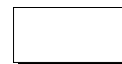


Regolamento (atto di natura regolamentare)

Il Regolamento (atto di natura regolamentare) è richiesto ai soggetti pubblici in casi specifici.

Di norma il *trattamento* di dati *sensibili e giudiziari* è consentito solo se lo prevede una norma di legge o di regolamento. Tuttavia, nel caso in cui la legge non specifichi i tipi di dati sensibili e le operazioni eseguibili, il soggetto pubblico è tenuto ad identificarli e renderli pubblici con atto di natura regolamentare adottato in conformità al parere reso dal Garante (anche su schemi tipo). Qualora il trattamento dei dati sensibili e giudiziari non sia previsto da alcuna legge, il soggetto pubblico deve fare richiesta di Autorizzazione al Garante e quindi adottare un regolamento (anche su schema tipo).

[\[indietro\]](#)



Adempimenti

Notificazione

Sia per i soggetti pubblici che per i soggetti privati, la notificazione si riduce a casi molto particolari, quando cioè il trattamento è suscettibile di recare pregiudizio ai diritti e alle libertà dell'interessato in ragione delle relative modalità o della natura dei dati personali (tali casi sono elencati nell'articolo 37 del Codice).

La notificazione va presentata al Garante prima dell'inizio (o della cessazione) del trattamento, e va trasmessa per via telematica su modello predisposto.

Comunicazione

Il titolare del trattamento è tenuto a comunicare previamente 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;
- 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.

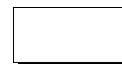
Tali trattamenti possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione, salvo diversa determinazione anche successiva del Garante. La comunicazione va inviata utilizzando il modello predisposto e reso disponibile dal Garante.

Autorizzazione

Il soggetto pubblico che effettua trattamenti di dati sensibili e giudiziari che non siano previsti da una legge, deve fare richiesta di Autorizzazione al Garante e quindi adottare un regolamento (anche su schema tipo).

La richiesta di autorizzazione al trattamento dei dati va formulata utilizzando esclusivamente il modello predisposto e reso disponibile dal Garante. Se poi il richiedente è invitato dal Garante a fornire informazioni o ad esibire documenti, questo va fatto entro quarantacinque giorni dalla data di scadenza del termine fissato per l'adempimento richiesto.

[\[indietro\]](#)



Sicurezza

Il Titolare del trattamento è tenuto ad adottare le misure minime volte ad assicurare un livello minimo di protezione dei dati personali.

Le misure minime di sicurezza, da adottare obbligatoriamente, sono dettate nell'Allegato B al Codice e vengono adeguate dal Garante con cadenza biennale, in relazione all'evoluzione tecnica ed alle esperienze maturate.

A seconda che il Titolare tratti dati personali comuni o sensibili e giudiziari, e a seconda che tali trattamenti avvengano senza l'ausilio di strumenti elettronici o con l'ausilio di tali strumenti, sono stabilite differenti misure minime di sicurezza da applicare.

In presenza di strumenti elettronici, il Codice non fa distinzione tra sistemi stand alone e sistemi collegati in rete esterna o interna (ciò significa che le sicurezza da adottare saranno le stesse).

Il trattamento di dati personali con strumenti elettronici è consentito solo se sono adottati i seguenti gruppi di sicurezze (ciascuno dei quali contiene una serie di misure minime elencate nell'Allegato B al Codice):

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'ambito dei trattamenti consentiti agli incaricati e addetti alla manutenzione;
- protezione degli strumenti elettronici e dei dati da: trattamenti illeciti, accessi non consentiti, programmi informatici non desiderati;
- procedure per: la custodia di copie di sicurezza e il ripristino della disponibilità dei dati e dei sistemi;
- Documento Programmatico sulla Sicurezza;
- nel caso di organismi sanitari: per i trattamenti con dati sullo stato di salute o vita sessuale, occorre adottare tecniche di cifratura.

Il trattamento di dati personali senza l'ausilio di strumenti elettronici è consentito solo se sono adottati i seguenti gruppi di sicurezze (ciascuno dei quali contiene una serie di misure minime elencate nell'Allegato B al Codice):

- aggiornamento periodico della individuazione dell'ambito dei trattamenti consentiti agli incaricati o unità organizzative;
- procedure per la custodia di atti e documenti affidati agli incaricati;
- procedure per la conservazione degli atti in archivi ad accesso selezionato e controllo degli accessi per quanto riguarda l'identificazione degli interessati.



[\[indietro\]](#)

Sanzioni

Con l'articolo 44 del D.L. 30.12.2008 n. 207 sono state inasprite le sanzioni previste dal "Codice in materia di protezione dei dati personali"

Le sanzioni prima del D.L. 30.12.2008 n. 207

SANZIONI AMMINISTRATIVE		SANZIONI AMMINISTRATIVE	
Omessa o inidonea informativa	da € 3.000 a 18.000	Trattamenti illeciti di dati	Reclusione da 6 a 24 mesi
Omessa o inidonea informativa (dati particolari e trattamenti con rischi specifici)	da € 5.000 a 30.000	Trattamenti illeciti di dati (dati particolari e trattamenti con rischi specifici)	Reclusione da 1 a 3 anni
Cessione illecita di dati	da € 5.000 a 30.000	Falsità nelle dichiarazioni e notificazioni al Garante	Reclusione da 6 a 3 anni
Violazione relativa ai dati personali idonei a rilevare lo stato di salute	da € 500 a 3.000	Omessa adozione delle misure minime di sicurezza	Arresto fino a 2 anni. Sanzione pecuniaria da €10.000 a 50.000
Omessa o incompleta notificazione	da € 10.000 a 60.000	Violazione da parte dei datori di lavoro del divieto di effettuare indagini su opinioni politiche. Controllo attraverso l'uso di impianti audiovisivi o altre apparecchiature	Arresto da 15 gg. a 1 anno
Omessa informazione o esibizione al Garante dei documenti richiesti	da € 4.000 a 24.000		

Gli inasprimenti delle sanzioni già previste

SANZIONI AMMINISTRATIVE	<i>Prima del DL 207/2008</i>	<i>Dopo il DL 207/2008</i>
Omessa od inidonea informativa all'interessato	da 3.000 a 18.000 euro	da 6.000 a 36.000 euro
Cessione illecita dei dati	da 5.000 a 30.000 euro	da 10.000 a 60.000 euro
Violazioni relative ai dati personali idonei a rivelare lo stato di salute	da 500 a 3.000 euro	da 1.000 a 6.000 euro
Omessa o incompleta notificazione	da 10.000 a 60.000 euro	da 20.000 a 120.000
Omessa informazione o esibizione di documenti al Garante	da 4.000 a 24.000 euro	da 10.000 a 60.000 euro

[\[indietro\]](#)