

Il Codice della Privacy

Che cosa tratta

1 - Quali finalita si propone il Codice?

Le norme del Codice della privacy, in aderenza alla disciplina dell'Unione Europea, intendono garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle liberta fondamentali (tutelati, in generale, dalla Costituzione della Repubblica), nonch della dignita delle persone fisiche, con particolare riferimento alla riservatezza e all'identita personale. La tutela si estende anche ai diritti delle persone giuridiche.

2- Che cos'e il trattamento dei dati personali ?

Il trattamento dei dati personali e qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di strumenti elettronici, che concerne le operazioni di: -raccolta dei dati, -registrazione, -organizzazione, -conservazione, -consultazione, -elaborazione, -blocco, -modificazione, -utilizzo, -interconnessione, -comunicazione, -diffusione, -cancellazione, -distruzione, -selezione, -estrazione, -raffronto.

3- Quali sono i dati personali ?

I dati personali sono 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. Ad esempio, sono dati personali rientranti nelle previsioni del Codice, oltre ai dati anagrafici ed economici, anche le immagini, i suoni e i codici identificativi riconducibili a un individuo. Esiste, inoltre, una categoria di dati - i cosiddetti dati sensibili - attinenti alla sfera personalissima dei singoli (informazioni sulle opinioni religiose o politiche, sulle abitudini sessuali, etc.), per i quali la legge prevede una tutela piu forte rispetto agli altri. Il trattamento di dati giudiziari, cioe 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 qualita di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale, e ammesso solo se autorizzato da espressa disposizione di legge o provvedimento del Garante, che ne specifichi le finalita, i tipi di dati e le operazioni autorizzate.

4 - Che cos'e una banca dati ?

Una banca dati e un insieme di informazioni personali, raccolte e conservate in una o piu unita di supporto, dislocate in uno o piu siti, organizzata secondo una pluralita di criteri determinati, tali da facilitarne il trattamento.

5 - Che cos'e una base dati ?

Raccolta di dati digitali o cartacei in formato omogeneo (ad es. database fatture in formato Access o cassetto contenente tutte le bolle dei clienti).

6 - Che cos'e un sistema di archiviazione?

Unita sia digitale (server) che analogica (armadio, cassette e archivi), contenente una o piu base dati.

7 - Quali sono i soggetti del trattamento ?

Il titolare: la persona fisica o giuridica, la pubblica amministrazione o qualsiasi altro ente, associazione o organismo cui competono le decisioni circa le finalita e le modalita del trattamento di dati personali, ivi compresa la sicurezza dei dati. Il responsabile: la persona fisica o giuridica, la pubblica amministrazione o qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali. L'incaricato: colui che compie le operazioni del trattamento di dati personali, attenendosi alle istruzioni

impartite dal titolare o dal responsabile. L'interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali. Il rappresentante stabilito nel territorio dello Stato: nel caso in cui il titolare risieda all'estero, deve essere nominato un rappresentante che sia stabilito nel territorio dello Stato italiano.

8 - Qual'è l'ambito di applicazione del Codice?

Il Codice si applica al trattamento di dati personali (anche se detenuti all'estero) da chiunque effettuato nel territorio dello Stato, con o senza mezzi elettronici, o comunque automatizzati. Inoltre, il Codice si applica anche al trattamento di dati personali effettuato da chiunque sia stabilito in un qualunque Paese, anche extraeuropeo, ed impieghi per il trattamento mezzi situati nel territorio dello Stato, anche diversi da quelli elettronici o automatizzati, salvo che essi siano utilizzati a soli fini di transito nell'Unione Europea. In questi casi deve essere nominato il rappresentante stabilito nel territorio dello Stato italiano. Non è soggetto alla legge il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali (agende, elenchi, raccolte), sempre che i dati non siano destinati ad una comunicazione sistematica o alla diffusione. Anche in questo caso, comunque, il titolare deve garantire la sicurezza dei dati ed è responsabile del danno eventualmente prodotto per effetto di una qualunque operazione di trattamento.

9 - Quali sono gli obblighi del titolare nei confronti dell'Autorità Garante per la protezione dei dati personali?

Il titolare che intenda procedere ad un trattamento di dati personali, rientranti tra quelli previsti dall'art. 37 del Codice, deve darne comunicazione, mediante notificazione, all'Autorità Garante per la protezione dei dati personali. Il Garante è un'autorità pubblica, che opera in piena autonomia e con indipendenza di giudizio e di valutazione e che ha specifiche funzioni di controllo e vigilanza in materia di tutela dei dati personali. Si tenga però presente che, in virtù delle novità introdotte dal D.lgs. 196/2003, che ha abrogato la legge 675/1996, l'adempimento della notificazione, prima obbligo generalizzato, sarà in futuro limitato ai soli casi previsti da un emanando regolamento.

10 - Cosa deve essere comunicato al Garante?

Al Garante deve essere comunicato il trattamento dei dati personali riguardante particolari settori, specificatamente elencati dall'art. 37. Inoltre, il Garante con proprio provvedimento potrà individuare altri trattamenti suscettibili di recare pregiudizio ai diritti ed alle libertà dell'interessato. Le modifiche di cui sopra comportano un cambiamento anche nelle modalità di effettuazione della notifica, che pur avvenire solo per via telematica.

11 - Quali sono gli obblighi relativi al trattamento ?

I dati personali devono essere: a. trattati in modo lecito e corretto; b. raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi; c. esatti e, se necessario, aggiornati; d. pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati; e. conservati in una forma che consenta l'identificazione dell'interessato, per un periodo di tempo non superiore a quello necessario agli scopi per cui sono stati raccolti o trattati.

12 - Quali informazioni devono essere fornite agli interessati ?

Il soggetto interessato, o la persona presso la quale sono raccolti i dati personali devono essere preventivamente informati per iscritto, circa: a. le finalità e le modalità del trattamento; b. l'obbligo o la facoltà di conferire i dati; c. le conseguenze giuridiche del rifiuto a rispondere; d. i soggetti a cui i dati possono essere comunicati; e. l'ambito di diffusione dei dati personali; f. i diritti spettanti al soggetto interessato; g. l'identificazione anagrafico-logistica del titolare del trattamento, del responsabile nel territorio dello Stato, di almeno un responsabile del trattamento, se designato; occorre indicare, inoltre, le modalità

tramite cui reperire l'elenco completo ed aggiornato di tutti i responsabili del trattamento.

13 - E' necessario il consenso dell'interessato per il trattamento dei dati personali ?

Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso soltanto con il consenso espresso dell'interessato, salve le eccezioni di cui al punto seguente. Il consenso è validamente prestato soltanto se è espresso liberamente. Il consenso per il trattamento dei dati comuni può anche essere orale, purché documentato per iscritto, mentre quello per i dati sensibili deve essere prestato esclusivamente in forma scritta.

14 - Quando non è necessario il consenso dell'interessato ?

Il consenso dell'interessato non è richiesto quando il trattamento: a. riguarda dati trattati per adempiere ad obblighi previsti da leggi, regolamenti o disposizioni comunitarie; b. è necessario per l'esecuzione di un contratto di cui è parte l'interessato, o per l'esecuzione di misure precontrattuali adottate su richiesta di quest'ultimo; c. riguarda dati provenienti da pubblici registri, elenchi o documenti conoscibili da chiunque; d. riguarda dati relativi allo svolgimento di attività economiche; e. è necessario per la salvaguardia dell'incolumità o della vita dell'interessato o di un terzo; f. con l'esclusione della diffusione, è effettuato per lo svolgimento di investigazioni difensive; g. con l'esclusione della diffusione, è necessario, nei casi individuati dal Garante, per perseguire un legittimo interesse del titolare o di un terzo destinatario, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate; h. con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti o organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il raggiungimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo; i. è necessario, in conformità con i codici deontologici, per esclusivi scopi scientifici, statistici o storici.

15 - Quali sono i diritti dell'interessato ?

Il Codice prevede che, circa i suoi dati personali, l'interessato abbia diritto: a. di conoscere, mediante l'accesso al registro dei trattamenti presso il Garante, l'esistenza di trattamenti che lo riguardano; b. di essere informato dal titolare circa le finalità del trattamento; c. di ottenere dal titolare la conferma, l'aggiornamento, la cancellazione, la rettifica dei dati trattati, o la loro trasformazione in forma anonima; d. di opporsi in tutto o in parte, per motivi legittimi, al trattamento di dati che lo riguardano. e. di chiedere il blocco dei dati trattati in violazione di legge.

16 - Come possono essere fatti valere i propri diritti dall'interessato ?

L'interessato può e deve, in primo luogo, agire direttamente nei confronti del titolare, del responsabile, 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.

17 - Cosa è previsto per 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, 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

conformita col parere espresso dal Garante, devono identificare e rendere pubblici i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalita perseguite nei singoli casi. Nel caso in cui il trattamento non e espressamente previsto da una disposizione di legge, i soggetti pubblici possono chiedere una speciale autorizzazione al Garante, rendendo altresì pubblici, nei modi di cui sopra, i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalita perseguite nei singoli casi.

In tutti i casi, comunque, e necessario fornire all'interessato una completa informativa.

18 - Cosa e previsto per i dati inerenti alla salute ?

Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici possono, anche senza l'autorizzazione del Garante, trattare i dati personali idonei a rivelare lo stato di salute, limitatamente ai dati e le operazioni indispensabili per il perseguimento di finalita di tutela dell'incolumita fisica e della salute dell'interessato.

Se le finalita di tutela riguardano terzi o la collettivita, in mancanza del consenso dell'interessato, il trattamento puo avvenire soltanto previa autorizzazione del Garante.

Sono previste modalita semplificate per la raccolta del consenso.

E' in ogni caso vietata la diffusione dei dati inerenti alla salute.

19 - Quali sono le garanzie di sicurezza dei dati personali previsti dal Codice?

L'Allegato B del Codice ("Disciplinare tecnico in materia di misure minime di sicurezza") ha individuato le misure minime di sicurezza che tutti i titolari del trattamento, siano essi soggetti privati o pubblici, devono adottare, pena l'arresto sino a due anni.

Le misure individuate sono graduate per classi di dati e per tipologie di trattamento. Occorre pertanto verificare accuratamente quali misure di sicurezza sono obbligatorie, in relazione ai singoli trattamenti. I dati personali oggetto del trattamento devono, comunque, essere custoditi in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, nonche di accesso non autorizzato o di trattamento non consentito e non conforme alle finalita di raccolta.

A tale scopo devono essere predisposte tutte le idonee misure di sicurezza in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento. Eventuali danni subiti dagli interessati dovranno ottenere risarcimento.

20 - Cosa e previsto per la comunicazione e la diffusione dei dati personali ?

La comunicazione e la diffusione sono consentite, come il trattamento, con il consenso dell'interessato, ovvero nel caso in cui ricorra un'ipotesi di esenzione.

In ogni caso, non possono essere comunicati o diffusi i dati per i quali e stata ordinata la cancellazione, ovvero quando e stato superato il periodo di tempo necessario al raggiungimento degli scopi, ovvero per scopi diversi da quelli indicati nella notificazione del trattamento al Garante, ove prescritta.

21 - Quali sono le regole per i dati trattati da soggetti pubblici ?

Il trattamento, la comunicazione e la diffusione di dati personali da parte di soggetti pubblici sono ammessi unicamente per lo svolgimento di funzioni istituzionali, anche in mancanza di una norma di legge o regolamento che lo preveda espressamente.

La comunicazione e la diffusione a soggetti pubblici sono ammesse soltanto quando siano previste da leggi o regolamenti, o risultino comunque necessarie per lo svolgimento di funzioni istituzionali: in quest'ultimo caso deve essere data comunicazione al Garante.

La comunicazione e la diffusione a soggetti privati o ad enti pubblici economici e ammessa soltanto se prevista da legge o regolamento.

22 - Quali sanzioni sono previste ?

Il Codice sanziona penalmente i comportamenti adottati in difformita dallo stesso, quali il trattamento illecito di dati personali, la omessa adozione delle misure di sicurezza, nonche l'omessa osservanza dei provvedimenti del Garante, la falsita nelle dichiarazioni al Garante.

Sono, inoltre, previste sanzioni amministrative nei casi di omessa o incompleta notificazione del trattamento al Garante, di inosservanza delle richieste del Garante o per l'omessa informativa ai soggetti interessati.

Cos'è il D.P.S.

(DPS) acronimo di **Documento programmatico sulla Sicurezza** Il DPS è l'unico documento in grado di attestare l'adeguamento alla normativa sulla tutela dei dati personali (privacy) e deve essere redatto entro il 30 GIUGNO 2005 ed alla scadenza fissata al 31 di marzo di ogni anno.

Il DPS è un manuale per la pianificazione della sicurezza dei dati in azienda: descrive come si tutelano i dati personali di dipendenti, collaboratori, clienti, utenti, fornitori ecc.

Il Garante ha individuato una figura responsabile per il trattamento dei dati più una serie di punti per i quali l'azienda deve adottare tutte le misure necessarie per l'esplicitamento della legge.

Lo scopo del DPS è proprio quello di descrivere la situazione attuale con riferimento ai punti stabiliti dal garante.

Ma vediamo più da vicino quali sono questi punti o regole (la numerazione è riferita al testo di legge di cui all'allegato B):

- 19.1 Elenco dei trattamenti di dati personali
individuare i trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati. Nella redazione della lista si può tener conto anche delle informazioni contenute nelle notificazioni eventualmente inviate al Garante anche in passato.
- 19.2 Distribuzione dei compiti e delle responsabilità
descrizione sintetica dell'organizzazione della struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati. Si possono utilizzare anche mediante specifici riferimenti documenti già predisposti (provvedimenti, ordini di servizio, regolamenti interni, circolari), indicando le precise modalità per reperirli.
- 19.3 Analisi dei rischi che incombono sui dati
Descrivere in questa sezione i principali eventi potenzialmente dannosi per la sicurezza dei dati, e valutarne le possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.
- 19.4 Misure in essere e da adottare
Riportate, in forma sintetica, le misure in essere e da adottare per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.
- 19.5 Criteri e modalità di ripristino della disponibilità dei dati
Descrivere i criteri e le procedure adottate per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati. L'importanza di queste attività deriva dall'eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che, quando sono necessarie, le copie dei dati siano disponibili e che le procedure di reinstallazione siano efficaci. Pertanto, è opportuno descrivere sinteticamente anche i criteri e le procedure adottate per il salvataggio dei dati al fine di una corretta esecuzione del loro ripristino.
- 19.6 Pianificazione degli interventi formativi previsti
Riportare le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.
- 19.7 Trattamenti affidati all'esterno
Redigere un quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.
- 19.8 Cifratura dei dati o separazione dei dati identificativi
Vanno rappresentate le modalità di protezione adottate in relazione ai dati per cui è richiesta la cifratura - o la separazione fra dati identificativi e dati sensibili, nonché i criteri e le modalità con cui viene assicurata la sicurezza di tali trattamenti.
Questo punto riguarda solo organismi sanitari e esercenti professioni sanitarie.

I tempi di stesura del DPS variano a secondo della dimensione dell'azienda e dalla mole di dati da processare, certamente non ci si mette un giorno... il documento programmatico richiede una attenta valutazione della situazione aziendale e dei trattamenti effettuati. Mediamente la stesura definitiva avviene nel giro di qualche settimana.

Il DPS deve avere data certa e deve essere aggiornato annualmente. Il testo unico impone come data per la redazione e l'aggiornamento il 31 marzo di ogni anno, solo per questo anno il termine è stato prorogato al 30/06/05. Si consiglia di non aspettare l'ultimo mese utile, perché potrebbe non bastare. 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.

Il Titolare del trattamento nella logica di una gestione consapevole deve individuare tutte le persone che hanno accesso ai dati ed a ciascuna dice esattamente come si deve comportare. Inoltre deve predisporre le informative da dare a tutti coloro che gli affidano dati in cui spiega le metodiche usate nei trattamenti.

Chi deve adeguarsi?

Dal 1° gennaio 2004 è entrato in vigore il nuovo Codice che riunisce tutte le regole in materia di Privacy succedutesi nel corso degli anni a partire dalla legge 675/96.

Il 31 marzo 2006, è il termine ultimo ed improrogabile per adempiere agli obblighi richiesti dalla nuova Legge sulla Privacy e per adottare le misure minime di sicurezza individuate dal Codice.

Qualsiasi persona giuridica pubblica o privata (azienda, professionista, associazione, ente, ecc.) che tratti dati personali di terzi (clienti, dipendenti o fornitori ecc.) nell'esercizio della propria attività professionale è obbligata ad adottare tutte le misure minime di sicurezza richieste dal nuovo Codice affinché venga tutelata la riservatezza e la sicurezza dei dati personali contenuti negli archivi. Questi dati sono intesi sia archiviati elettronicamente che in qualunque altro modo, incluso il cartaceo.

In pratica, sono escluse dall'adeguamento al Nuovo Codice solo le persone fisiche che effettuano il trattamento di dati personali per soli fini personali e, in nessun caso, prevedano la cessione o la comunicazione a terzi dei dati in loro possesso.

Il Decreto Legislativo 30 Giugno 2003, n. 196 non lascia dubbi sulle conseguenze della sua violazione estendendo e riprendendo in modo assolutamente chiaro gli articoli della 675/96 e tutte le norme precedenti.

Il nuovo Codice:

- **OBBLIGA** tutti i titolari che trattano dati sensibili, di redigere entro il 31 marzo di ogni anno il Documento Programmatico Sulla Sicurezza (DPS) dei dati.
- **IMPONE** l'adozione di misure minime di sicurezza dei dati.
- **STABILISCE** il principio che il trattamento si svolga nel rispetto dei diritti, della dignità e della riservatezza dell'interessato.
- **CHIARISCE e SOTTOLINEA** che il consenso dovrà essere **ESPRESSO**, fornito cioè in riferimento ad un trattamento chiaramente individuato.
- **PRECISA** che le figure del Responsabile e degli Incaricati devono essere individuate per iscritto e che sia definito il loro ambito di trattamento.
- **SANZIONA** fino a 60.000 euro e impone il risarcimento dei danni.
- **AGISCE PENALMENTE** con la reclusione fino a 3 anni in caso di gravi violazioni.

IN PAROLE SEMPLICI

Tutti coloro che trattano dati personali e/o sensibili* sia tramite strumenti informatici che in forma cartacea.

* Es. buste paga/certificati medici

Tutti coloro che trattano dati sensibili e/o giudiziari tramite strumenti informatici e rientrano nelle casistiche definite dal Garante

Adeguarsi alle MISURE MINIME DI SICUREZZA (MMS) e redigere il Documento Programmatico sulla Sicurezza con rinnovo annuale e/o ad ogni modifica sostanziale.
NOTIFICA AL GARANTE.

Tutti coloro che rientrano nelle casistiche definite dal Garante e trattano dati personali in modo informatico o manuale

Le sanzioni

Amministrative

Omessa o inadeguata informativa per trattamenti che non contengono dati sensibili

Da 3000€ a 18000€

Tale somma può essere aumentata fino al triplo se, in ragione delle condizioni economiche del contravventore, risulta inefficace.

Può essere applicata la sanzione accessoria della pubblicazione dell'ordinanza ingiunzione su uno o più giornali indicati con il provvedimento sanzionatorio.

Omessa o inadeguata informativa per trattamenti che contengono dati sensibili

Da 5000€ a 30000€

Tale somma può essere aumentata fino al triplo se, in ragione delle condizioni economiche del contravventore, risulta inefficace.

Può essere applicata la sanzione accessoria della pubblicazione dell'ordinanza ingiunzione su uno o più giornali indicati con il provvedimento sanzionatorio.

Illegittima cessione di dati

Da 5000€ a 30000€

Può essere applicata la sanzione accessoria della pubblicazione dell'ordinanza ingiunzione su uno o più giornali indicati con il provvedimento sanzionatorio.

Violazione delle prescrizioni in ordine alla comunicazione di dati in ambito sanitario.

Da 500€ a 3000€

È prevista la sanzione accessoria della pubblicazione dell'ordinanza ingiunzione su uno o più giornali indicati con il provvedimento sanzionatorio.

Omessa o incompleta notificazione

Da 10000€ a 60000€

Può essere applicata la sanzione accessoria della pubblicazione dell'ordinanza ingiunzione su uno o più giornali indicati con il provvedimento sanzionatorio.

Omessa informazione o esibizione di documenti al Garante

Da 4000€ a 24000€

Può essere applicata la sanzione accessoria della pubblicazione dell'ordinanza ingiunzione su uno o più giornali indicati con il provvedimento sanzionatorio.

Le sanzioni Penali

Trattamento da parte di soggetti pubblici per scopi non istituzionali

Se il trattamento causa un danno:

reclusione da 6 a 18 mesi

Se il trattamento è effettuato in violazione delle regole in ordine alla comunicazione e alla diffusione :

reclusione da 6 a 24 mesi

Se il trattamento causa un danno:

reclusione da 6 a 18 mesi

Se il trattamento è effettuato in violazione delle regole in ordine alla comunicazione e alla diffusione :

reclusione da 6 a 24 mesi

Se il trattamento causa un danno:

reclusione da 6 a 18 mesi

Se il trattamento è effettuato in violazione delle regole in ordine alla comunicazione e alla diffusione :

reclusione da 6 a 24 mesi

Se il trattamento causa un danno:

reclusione da 6 a 18 mesi

Se il trattamento è effettuato in violazione delle regole in ordine alla comunicazione e alla diffusione :

reclusione da 6 a 24 mesi

Se il trattamento causa un danno:

reclusione da 1 a 3 anni

Se il trattamento causa un danno:

reclusione da 1 a 3 anni

Se il trattamento causa un danno:

reclusione da 1 a 3 anni

Reclusione da 6 mesi a 3 anni

Arresto sino a 2 anni o ammenda da 10000€ a 50000€

Violazione da parte di un soggetto pubblico delle regole di comunicazione dei dati personali comuni

Trattamento di dati senza il prescritto consenso

Violazione delle regole di trattamento imposte ai gestori dei servizi di comunicazione elettronica

Violazione dei divieti di comunicazione e diffusione

Trattamento di dati sensibili o giudiziari in violazione delle garanzie specificamente previste

Violazione dei divieti di trasferimento dei dati all'estero

False dichiarazioni e notificazioni rese al garante
Omessa adozione delle misure minime di sicurezza

Nel caso di violazione degli obblighi relativi all'adozione delle misure minime di sicurezza, all'autore del reato viene concesso un termine entro il quale può regolarizzare la propria posizione. Se la regolarizzazione avviene nei 60 giorni successivi alla scadenza del termine, il trasgressore è ammesso a pagare una sanzione pari al quarto del massimo dell'ammenda stabilita per la violazione (12500€).

Inosservanza dei provvedimenti del garante
Inosservanza dello statuto dei lavoratori

Reclusione da 3 mesi a 2 anni
Ammenda da 51.65€ a 516.5€ o arresto da 15gg ad 1 anno

Danni cagionati all'interessato

Non è l'interessato a dover provare il danno ma colui che l'ha provocato a dover provare di aver fatto tutto il possibile per evitarlo - risarcibile il danno non patrimoniale - pagano il titolare ed il responsabile

Art. 15 Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali e tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

L'art. 2050 c.c. parla di "attività pericolosa" (elevata potenzialità di danno, per la natura dell'attività o dei mezzi di lavoro utilizzati). Il trattamento dati viene dunque qualificato come esercizio di attività pericolosa.

Da questa qualificazione deriva un'importante conseguenza circa l'onere della prova. Solitamente chi si ritiene danneggiato da un fatto illecito, deve provare la responsabilità di colui che ha commesso il fatto.

Nell'ipotesi regolata dall'art. 2050 è sancito invece il "principio dell'inversione dell'onere della prova". Sulla base di questo principio 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.

La prova è particolarmente rigorosa, in quanto non è sufficiente la sola dimostrazione, in negativo, di non aver commesso alcuna violazione della legge o delle regole di comune prudenza, ma è necessaria la prova positiva di aver impiegato ogni cura o misura atta ad impedire l'evento dannoso.

NB: è risarcibile anche il danno non patrimoniale.

RESPONSABILITÀ CIVILE E PENALE

Aspetti di responsabilità penale

Così recita l'art. 169 del TESTO UNICO PRIVACY:

Omissa adozione di misure necessarie alla sicurezza dei dati

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 e punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.

2. 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.

L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

Aspetti di responsabilità civile

Art. 2050 c.c.

Il TESTO UNICO PRIVACY qualifica il trattamento dei dati come attività pericolosa, art. 2050 c.c.

È prevista pertanto una inversione dell'onere della prova nell'azione risarcitoria ex articolo 2043 c.c.:

l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire la sicurezza dei dati detenuti.

A livello pratico questo significa che l'azienda, il professionista, la PA ecc., per evitare ogni responsabilita deve dimostrare di aver adottato "tutte le misure idonee ad evitare il danno", e quindi di aver messo in essere tutte le misure di sicurezza al meglio possibile (la miglior tecnologia disponibile). Il che non e affatto facile da dimostrare...

Art. 2049 c.c.

In generale poi a carico dell'azienda risulta comunque la responsabilita ex art art. 2049 c.c., ovvero la responsabilita prevista in capo a padroni e committenti.

L'art. 2049 difatti recita: "padroni e committenti sono responsabili per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze cui sono adibiti".

Legge n. 547/1993

Crimini informatici commessi da dipendenti ed addebitabili all'azienda

La legge 547/93 ha introdotto nel nostro ordinamento vari "crimini informatici", ovvero l'attentato a impianti informatici di pubblica utilita, falsificazione di documenti informatici, accesso abusivo ad un sistema informatico o telematico, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, violazione di corrispondenza telematica, intercettazione di e-mail, danneggiamento di sistemi informatici o telematici (...).

Il datore di lavoro rischia di essere ritenuto in concorso con il dipendente a lui subordinato che ha commesso il crimine informatico, per non aver posto in essere tutte le misure di prevenzione e controllo idonee a garantire la sicurezza del trattamento dei dati.

La mancata adozione di tutte le misure idonee a ridurre al minimo i rischi viene considerata difatti un agevolazione alla commissione del crimine.

CHI E' TENUTO AL RISARCIMENTO?

I soggetti tenuti al risarcimento dei danni causati dal trattamento dei dati personali, sono il "titolare" (ossia colui "cui competono le decisioni in ordine alle finalita del trattamento" e "della sicurezza") ed il "responsabile" (ossia colui che e preposto dal titolare al trattamento dei dati, avendo "esperienza, capacita ed affidabilita" tale da fornire "idonea garanzia del pieno rispetto delle disposizioni di legge in materia di trattamento, ivi compreso il profilo relativo alla sicurezza").

Di seguito troverete tutti i facsimili da compilare per le richieste, i consensi e i dinieghi al trattamento dati sensibili in rispetto alla legge sulla privacy. Ricordiamo a tutti gli utenti che i modelli sono tracce generalizzate per trarre spunto ed adattarli alla propria realta aziendale.

[Informativa ex art. 13 D.lgs. 196/2003 in materia di privacy e trattamento dati](#)

[Formula di consenso al trattamento dati a norma di legge sulla privacy](#)

[Informativa ex art. 13 D.lgs. 196/2003 per il trattamento di dati sensibili](#)

[Formula di consenso per trattamento di dati sensibili](#)

[Opposizione al trattamento dei dati per motivi legittimi](#)

[Esercizio dei diritti dell'interessato di essere informato sull'esistenza dei dati presso archivi](#)

[Esercizio dei diritti dell'interessato di ottenere la cancellazione o il blocco di dati dei quali gia conosce l'esistenza presso gli archivi cui si rivolge e per i quali si e constatato il trattamento in violazione di legge](#)

[Esercizio dei diritti dell'interessato di ottenere la rettifica o l'aggiornamento di dati dei quali già conosce l'esistenza presso gli archivi cui si rivolge](#)

[Accesso al registro dei trattamenti tenuto dal Garante per la protezione dei dati personali](#)

ELENCO DELLE MISURE MINIME

ALLEGATO B. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
(Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. 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.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della

componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalita con le quali il titolare puo assicurare la disponibilita di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessita di operativita e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali e organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso e utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, e verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

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

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

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

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilita nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. 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;

19.7. 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;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi

all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne

attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli 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 sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. 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 della vigilanza, le persone che vi accedono sono preventivamente autorizzate.