CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

GUIDA FORMATIVA DEGLI INCARICATI DEL TRATTAMENTO

GUIDA FORMATIVA DEGLI INCARICATI DEL TRATTAMENTO

La tutela della riservatezza, il diritto del cittadino a non subire invasioni nella propria sfera privata sono entrati a far parte della nostra vita quotidiana. Siamo però immersi in una società che non può astenersi dal trattare dati personali, soprattutto al fine di fornire beni o servizi.

Le informazioni vengono raccolte, elaborate, comunicate ad altri soggetti, anche tramite reti di comunicazione elettronica. Si è quindi ravvisata la necessità di tutelare sia l'identità personale che i dati personali.

Il Codice in materia di protezione dei dati personali (decreto legislativo 196/03), rappresentando una raccolta organica e sistematica delle norme sulla privacy, è finalizzato proprio a disciplinare un settore delicato come la tutela dei diritti, delle libertà fondamentali, della dignità della persona e la protezione dei dati personali, definendo regole generali e specifiche al fine di un corretto e trasparente trattamento dei dati raccolti.

Il Codice pone particolare attenzione alla tutela dei dati idonei a rivelare lo stato di salute in quanto, all'interno dei già tutelati dati sensibili, questa categoria rientra sicuramente nella sfera più intima della persona. Il Codice impone alcune regole specifiche per il trattamento di questa categoria di dati in ambito sanitario. Una sezione di questa guida formativa è mirata a informare gli incaricati che si trovino nella necessità di trattare dati sanitari.

Concetto fondamentale del Codice è quindi il diritto alla protezione dei dati personali.

Questo diritto viene tutelato sia con misure di tipo preventivo quali ad esempio l'informativa all'interessato o le misure di sicurezza, sia di tipo successivo quali ad esempio il controllo che può esercitare l'interessato sui propri dati o le sanzioni previste.

Il presente opuscolo mira ad informare gli incaricati sulle disposizioni previste e sui rischi che può comportare il trattamento di dati personali.

DEFINIZIONI

Il Codice in materia di protezione dei dati personali utilizza termini di cui è necessario conoscere il significato. Al fine di rendere più agevole l'utilizzazione della presente guida formativa e comprensibili le espressioni verbali utilizzate, in questa sezione si riportano i principali termini di cui si avvale il Codice.

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, identificata o identificabile, 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 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. (organo collegiale operante in piena autonomia e con indipendenza di giudizio e valutazione istituito al fine di assicurare la tutela dei diritti e delle libertà fondamentali nonché il rispetto della dignità dell'interessato nel trattamento di dati personali. Fra gli altri, ha il compito di controllare la conformità dei trattamenti, esaminare segnalazioni, reclami, ricorsi, adottare i provvedimenti previsti dalla normativa, promuovere la conoscenza del Codice. Ha inoltre poteri inibitori, sanzionatori e cautelari.)

REGOLE GENERALI

Il codice dispone regole generali finalizzate ad un corretto trattamento dei dati personali. In questa sezione vengono evidenziate le principali regole generali, valide per tutti i trattamenti e alcune indicazioni operative per conformare il trattamento alla normativa.

A) PRINCIPI GENERALI
L'art. 11 specifica le regole generali alle quali devono essere adeguati tutti i trattamenti di dati. Secondo tali principi ogni trattamento deve essere lecito e corretto; la nozione di liceità comporta ontologicamente che il trattamento debba essere eseguito sia nel rispetto delle disposizioni specifiche di legge previste dalla normativa a carattere speciale sia nel rispetto dei principi generali del diritto; la correttezza si riferisce a regole di condotta non giuridiche da applicarsi al trattamento di dati personali. Inoltre i dati devono essere raccolti e registrati per scopi determinati, espliciti e legittimi; questo significa che, prima dell'inizio del trattamento, si devono determinare le finalità per le quali i dati vengono raccolti e trattati, limitando la raccolta delle informazioni a quei dati che siano strumentali e funzionali allo scopo del trattamento, informandone l'interessato il quale potrà esercitare i propri diritti sui propri dati personali; i dati raccolti dovranno quindi essere esatti e, se necessario, aggiornati nonché pertinenti, completi e non eccedenti; risulta quindi necessario procedere ad un iniziale controllo in fase di raccolta dei dati al fine di evitare di raccogliere dati non necessari allo scopo del trattamento pur nella loro completezza al fine di avere un quadro completo dell'interessato in relazione al trattamento effettuato, seguito da periodiche verifiche al fine di aggiornare, se necessario, i dati.
Infine i dati devono essere conservati per un periodo non superiore a quello necessario allo scopo per il quale sono stati raccolti. E' quindi necessario valutare se e per quanto tempo la normativa di riferimento preveda la conservazione dei dati, tenendo presente la normativa contabile e fiscale, nonché la conservazione della documentazione per fini storici, statistici o scientifici, con particolare attenzione alla normativa archivistica.

B) INFORMATIVA DELL'INTERESSATO
L'articolo 13 del Codice prevede altresì che l'interessato sia informato in merito all' identità del soggetto che ha intenzione di trattare i dati personali dell'interessato stesso e in merito all'utilizzo che ne verrà fatto. Scopo di questo adempimento è

consentire all’interessato di poter “ seguire “ le informazioni a lui riferite ed eventualmente esercitare i diritti conferitigli dal Codice.
In particolare la normativa prevede che l’interessato o la persona presso cui sono raccolti i dati debba essere previamente informato oralmente o per iscritto circa:

- Finalità e modalità del trattamento cui sono destinati i dati;
- La natura obbligatoria o facoltativa del conferimento dei dati;
- Le conseguenze di un eventuale rifiuto di rispondere;
- I soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati;
- L’ambito di diffusione dei dati
- Gli estremi identificativi del titolare e del responsabile

Nel caso in cui, poi, i dati siano di tipo sensibile o giudiziario, deve essere inserito il riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento di tali dati.
Se i dati non sono raccolti direttamente presso l’interessato ma sono raccolti presso terzi, l’informativa all’interessato può essere data all’atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione. In questo caso devono essere comprese nell’informativa le categorie di dati trattati.
Questa disposizione non si applica se i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria, se i dati sono trattati ai fini dello svolgimento delle investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria oppure su concessione del Garante.

C) ADEMPIMENTI PER GLI INCARICATI
Per una corretta applicazione di queste norme è necessario che gli incaricati, al momento della raccolta dei dati, provvedano a tali adempimenti:

- fornire l’informativa relativa al trattamento dei dati così come predisposta dal titolare del trattamento eventualmente integrandola nelle parti di competenza;
- verificare l’esattezza, la pertinenza e la completezza dei dati trattati;
- non raccogliere più dati del necessario;
- rispettare l’obbligo di riservatezza e segretezza in relazione ai dati di cui si viene a conoscenza;
- far rispettare la “ distanza di cortesia “ nei rapporti di tipo front-office al fine di garantire la riservatezza e la discrezione nel trattamento e nella comunicazione dei dati.

D) DIRITTI DEGLI INTERESSATI
L’articolo 7 del Codice conferisce all’interessato il diritto di accesso ai propri dati personali e altri diritti.
In particolare l’interessato ha diritto di:

1. Ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. Ottenere l'indicazione:

a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati

3. Ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. Opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Questi diritti possono essere esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato; alla richiesta è fornito idoneo riscontro senza ritardo. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Quando riguarda l'esercizio dei diritti previsti al punto 1 e 2 dell’elenco precedente, la richiesta può essere formulata anche oralmente e in tal caso deve essere annotata sinteticamente a cura dell'incaricato o del responsabile.
Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.
Nel caso in cui sia effettuata una richiesta in tal senso, il responsabile o gli incaricati devono estrarre i dati e comunicarli al richiedente. I dati possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.
Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare.

REGOLE SPECIFICHE PER I SOGGETTI PUBBLICI

Il codice prevede delle disposizioni specifiche alle quali devono attenersi i soggetti pubblici nel trattare dati personali. In questa sezione vengono evidenziate le principali regole specifiche per il settore pubblico, valide per tutti i trattamenti e alcune indicazioni operative per conformare il trattamento alla normativa.

A) REGOLE PER IL TRATTAMENTO DI DATI COMUNI DA PARTE DI SOGGETTI PUBBLICI

Il trattamento dei dati personali da parte di soggetti pubblici è consentito soltanto al fine dello svolgimento delle funzioni istituzionali, osservando i presupposti e i limiti stabiliti dal Codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

Inoltre è espressamente previsto che i soggetti pubblici siano esonerati dal richiedere il consenso dell'interessato.

Per quanto riguarda i dati diversi da quelli sensibili o giudiziari, che per semplificare vengono convenzionalmente definiti "comuni", in base all'art. 19, i soggetti pubblici possono legittimamente procedere al trattamento anche se non è espressamente previsto da leggi o regolamenti.

Diverse invece sono le disposizioni in tema di comunicazione di dati. Infatti, se la comunicazione avviene nei confronti di un altro soggetto pubblico, essa è ammessa solo quando è prevista da una norma di legge o regolamento. In subordine la comunicazione è ammessa anche in mancanza di norma di legge o regolamento, ma quando questa sia comunque necessaria per lo svolgimento di funzioni istituzionali. In tal caso la legge obbliga ad una preventiva comunicazione di tale attività al Garante.

Se la comunicazione avviene invece nei confronti di soggetti privati o enti pubblici economici, essa è ammessa unicamente se prevista da norma di legge o regolamento.

Anche la diffusione dei dati è ammessa solamente se prevista da norma di legge o regolamento.

B) ADEMPIMENTI PER GLI INCARICATI

Per osservare tale norma è necessario che gli incaricati provvedano ai seguenti adempimenti:

- verificare se i trattamenti eseguiti sono svolti per le finalità istituzionali dell'Ente
- verificare, ogni volta che ci si ritrova nella necessità di dover comunicare dati all'esterno dell'Ente, le disposizioni di legge che consentono tali operazioni.

C) REGOLE PER IL TRATTAMENTO DI DATI SENSIBILI DA PARTE DI SOGGETTI PUBBLICI

Per quanto riguarda i dati sensibili invece, il soggetto pubblico può procedere al trattamento solo se autorizzato da espressa disposizione di legge, nella quale siano specificati i tipi di dati che possono essere trattati, il tipo di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

Nel caso in cui non sia presente una tale disposizione di legge il codice prevede che il Garante, su richiesta, possa procedere all'individuazione delle attività che perseguono finalità di rilevante interesse pubblico, autorizzando così, con proprio provvedimento, il trattamento.

A seguito del provvedimento del Garante o nel caso in cui la legge, individuate le finalità di rilevante interesse pubblico, non proceda a determinare i tipi di dati e le operazioni eseguibili, dovrà essere il soggetto pubblico stesso ad individuare tali elementi. Tale individuazione dovrà essere fatta con atto di natura regolamentare, adottato in conformità al parere espresso dal Garante.

D) REGOLE PER IL TRATTAMENTO DI DATI GIUDIZIARI DA PARTE DI SOGGETTI PUBBLICI

Similmente, anche per i dati giudiziari, il trattamento è consentito unicamente se autorizzato da espressa disposizione di legge o autorizzazione del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

Anche in questo caso, se non vengono determinati i tipi di dati e le operazioni eseguibili, si applica quanto indicato in merito al regolamento per i dati sensibili.

E) ADEMPIMENTI PER GLI INCARICATI

Il codice prevede ulteriori principi che si applicano ai trattamento di dati sensibili o giudiziari. In relazione a tali tipologie di dati devono essere quindi messe in atto le seguenti procedure:

- conformare il trattamento secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato;
- devono esser trattati solo i dati indispensabili per svolgere attività istituzionali che non possono essere adempiute caso per caso mediante il trattamento di dati anonimi o di dati personali di natura diversa;
- i dati dovranno essere, di regola, raccolti presso l'interessato;
- periodicamente dovranno essere verificate l'esattezza, l'aggiornamento, la pertinenza, la completezza, la non eccedenza e l'indispensabilità dei dati rispetto alle finalità perseguite nei singoli casi. I dati che, a seguito delle verifiche risultano eccedenti, non pertinenti o non indispensabili, non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene;
- particolare attenzione si deve porre al trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale. Tali dati devono essere conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo;
- i dati idonei a rivelare lo stato di salute non posso essere diffusi.

TRATTAMENTO DI DATI IN AMBITO SANITARIO

Il codice della privacy pone particolare attenzione alla tutela dei dati idonei a rivelare lo stato di salute in quanto, all'interno dei già tutelati dati sensibili, questa categoria rientra sicuramente nella sfera più intima della persona. Il codice impone alcune regole specifiche per il trattamento di questa categoria di dati in ambito sanitario. Questa parte della guida formativa è mirata a informare gli incaricati che si trovino nella necessità di trattare dati " sanitari ".

A)REGOLE PER I TRATTAMENTI DI DATI IDONEI A RIVELARE LO STATO DI SALUTE IN AMBITO SANITARIO

Il codice prevede che il trattamento di dati personali idonei a rivelare lo stato di salute effettuato da esercenti le professioni sanitarie o organismi sanitari pubblici può essere effettuato con il solo consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento è finalizzato alla tutela della salute o dell'incolumità fisica dell'interessato.

Se invece la finalità di tutela della salute o dell'incolumità fisica riguarda un terzo o la collettività, il trattamento di dati personali idonei a rivelare lo stato di salute può essere effettuato anche senza il consenso dell'interessato ma previa autorizzazione del Garante. (l'Authority ha emesso un'autorizzazione generale allo scopo – Autorizzazione n. 2/2004 " trattamento di dati idonei a rivelare lo stato di salute").

In parziale deroga alla norma generale che prevede che il consenso dell'interessato al trattamento di dati sensibili sia manifestato in forma scritta, nel caso considerato il consenso può esser manifestato anche oralmente e documentato con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico.

Il consenso deve essere espresso da una persona maggiorenne, non interdetta e capace di intendere e volere. Nel caso in cui l'interessato sia impossibilitato fisicamente, incapace di agire, intendere o volere, il consenso può essere prestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato.
Particolare attenzione dovrà essere posta in caso di comunicazione di dati idonei a rivelare lo stato di salute all'interessato o ai soggetti legittimati.
Il codice infatti prevede che la comunicazione di questa categoria di dati possa avvenire solo per il tramite di un medico designato dall'interessato o dal titolare. Questa disposizione, in considerazione della delicatezza delle informazioni, è finalizzata ad evitare che il paziente venga a conoscenza di notizie sul suo stato di salute da soggetti professionalmente non preposti a tale compito. Questa norma non si applica però in riferimento ai dati personali già conosciuti dal medesimo interessato in quanto da lui forniti in precedenza.
E' previsto inoltre che il titolare o il responsabile possano autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici che, nell'esercizio dei propri compiti, intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai soggetti legittimati.

B) ADEMPIMENTI PER GLI INCARICATI
In relazione a tali norme è necessario che gli incaricati di tali trattamenti si attengano alle seguenti disposizioni:

- all'ingresso dell'ospite, deve essere consegnata l'informativa così come redatta dal titolare del trattamento e richiesto il consenso al trattamento di dati idonei a rivelare lo stato di salute;
- durante i colloqui con l'interessato o con terzi legittimati, adottare soluzioni tali da prevenire l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute; a tal fine è opportuno che i colloqui avvengano nello studio del medico o nella camera dell'interessato;
- rispettare la dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dati senza discriminazioni di età, di sesso, di razza, di religione, di nazionalità, di condizione sociale, di ideologia;
- rispettare eventuali opposizioni a taluni trattamenti di dati, quali ad esempio l'opposizione dell'interessato alla conoscenza di terzi della sua presenza nella struttura;
- tutti gli incaricati che non sono tenuti per legge al segreto professionale, devono comunque attenersi a regole di condotta analoghe al segreto professionale e in particolare:
  - mantenere il segreto su tutto ciò che viene confidato o di cui si può venire a conoscenza in ragione della propria professione nonché sulle prestazioni professionali effettuate o programmate, nel rispetto dei principi che garantiscano la tutela della riservatezza.
  - La rivelazione non autorizzata o non necessitata assume particolare gravità quando ne derivi profitto, proprio o altrui, o nocumento della persona o di altri.
  - La morte dell'ospite non esime l'incaricato dall'obbligo del segreto.

Nel caso in cui il titolare o il responsabile abbiano provveduto ad autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici a rendere noti i dati personali idonei a rivelare lo stato di salute all'interessato o ai terzi legittimati, gli incaricati dovranno attenersi, oltre alle disposizioni contenute nella presente guida formativa, alle modalità e alle cautele previste dall'autorizzazione e dall'atto di incarico.

RISCHI CHE INCOMBONO SUI DATI E MISURE DI SICUREZZA

Il codice prevede l'adozione di misure di sicurezza idonee e preventive in modo tale da ridurre al minimo i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, tenendo conto del progresso tecnico, della natura dei dati trattati e delle specificità dei trattamenti.
Il titolare del trattamento deve quindi, anche attraverso la collaborazione del responsabile, se nominato, e degli incaricati provvedere a mettere in atto tutte le misure di sicurezza a protezione dei dati personali trattati.
In particolare il codice individua alcune misure di sicurezza, definite " minime ", volte ad assicurare un livello minimo di protezione dei dati personali.
In questa sezione vengono evidenziati i principali rischi che possono incombere sui dati e le misure di sicurezza adottate a disposizione degli incaricati. La puntuale applicazione e il corretto utilizzo di tali misure da parte degli incaricati sono condizione essenziale per una sicurezza dei dati.

TRATTAMENTI CON STRUMENTI ELETTRONICI

Protezione dei dati da accessi non consentiti o trattamenti non autorizzati:

Ogni utente del sistema informatico è dotato di credenziali di autenticazione consistenti in un codice per l'identificazione dell'incaricato (nome utente) e una password oppure in un dispositivo di autenticazione in possesso ed uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato, eventualmente associati ad un codice identificativo o ad una password, in modo tale che solo gli incaricati dotati di tali credenziali di autenticazione possano accedere a uno specifico trattamento o insieme di trattamenti attraverso il superamento di un'idonea procedura di identificazione. Questa misura di sicurezza protegge i dati da accessi non autorizzati. E' obbligatorio che la password che compone le credenziali di autenticazione sia mantenuta segreta dalla persona a cui è assegnata. Infatti una divulgazione a terzi di tale password comprometterebbe la sicurezza dei dati permettendo un accesso abusivo ad essi da parte di persone non autorizzate.
Altre misure di sicurezza riguardano l'obbligo di modifica della password da parte dell'utente del sistema informatico al primo utilizzo e successivamente ogni tre mesi(nel caso di trattamento di dati sensibili o giudiziari) o sei mesi in caso di trattamento di dati comuni, la lunghezza della password e il divieto di utilizzare riferimenti agevolmente riconducibili all'incaricato. Tale obbligo ha la funzione di proteggere sia i dati personali trattati (un soggetto estraneo che si introduca nel sistema potrebbe modificare o cancellare i dati contenuti), sia l'incaricato stesso che utilizza la password (in caso di accesso ai dati tramite la password dell'utente, il sistema registra l'accesso attribuendolo all'utente stesso). L'associazione di una password non facilmente riconducibile all'incaricato (ad esempio è vietato indicare il proprio nome o cognome, quello dei familiari o la data di nascita e tantomeno utilizzare il nome utente), unita ad una lunghezza adeguata e il suo cambiamento in tempi ragionevolmente brevi permette di contrastare accessi abusivi al sistema informatico o eventuali tentativi di scoprire o sottrarre, anche con modalità informatiche, la password utilizzata.
Nel caso in cui, ora o in futuro, siano utilizzati come credenziali di autenticazione al posto di codice identificativo (nome utente) e password, dispositivi di autenticazione (ad esempio smart card) eventualmente associate ad una password, fermo restando quanto già indicato per la password, è necessario che la persone in possesso di tali dispositivi di autenticazione si preoccupino di conservarli con cura, non cedendoli a

terzi né lasciandoli a disposizione di terzi (ad esempio non lasciare questi dispositivi a disposizione di chiunque sulla scrivania o posto di lavoro).
La collaborazione degli utenti del sistema informatico è richiesta anche in relazione alla custodia degli strumenti elettronici. In particolare è misura minima di sicurezza provvedere a non permettere che terzi non autorizzati utilizzino gli strumenti informatici in assenza dell'incaricato. A tal fine è obbligatorio che al termine dell'orario lavorativo il PC in dotazione venga spento. E' inoltre previsto che, in caso di assenza temporanea dalla propria postazione (ad esempio nelle pause pranzo, o in caso di allontanamento in genere) si provveda a bloccare la possibilità di utilizzo. A tal fine sono possibili varie soluzioni quali spegnere il PC o chiudere la porta a chiave.
La soluzione più immediata e facilmente adottabile rimane comunque quella di bloccare il PC. (ctrl + alt + canc – blocca computer). In tal modo solo inserendo la password di accesso sarà possibile accedere ai dati ripartendo esattamente dal punto lasciato in sospeso. Altra soluzione possibile è attivare la procedura di screen saver con password: in caso di non utilizzo del sistema, a cadenza prestabilita, si attiverà lo screen saver obbligando l'utente all'inserimento della password.
E' possibile che talora sia necessario accedere ai dati in assenza dell'incaricato. Questo può avvenire in caso di manutenzione del sistema, di sicurezza o di continuità operativa. Se tali operazioni di accesso ai dati o agli strumenti possono avvenire solo con l'utilizzo della password dell'incaricato, è necessario che ogni incaricato, al primo utilizzo della password e successivamente ad ogni cambio, comunichi la sua password in busta chiusa al custode delle password il cui nome sarà comunicato da parte del titolare stesso. Tale comunicazione è necessaria solo nel caso in cui sia necessario conoscere, da parte del titolare e nei casi indicati, la password dell'incaricato. Nel caso in cui il titolare del trattamento possa comunque accedere ai dati senza conoscere tale password (ad esempio tramite la password di amministratore di sistema o resettando la password dell'incaricato o qualora agli stessi dati accedano più persone, evitando quindi la paralisi lavorativa in caso di assenza dell'incaricato) tale procedura non è necessaria.

Protezione dei dati da attacchi di virus o programmi intrusivi

Il titolare del trattamento ha provveduto a installare programmi antivirus e anti programmi pericolosi e ad aggiornarli periodicamente.
E' comunque necessaria anche in questo caso la collaborazione degli incaricati e in particolare:
Se l'aggiornamento dell'antivirus non è previsto in modalità automatica ma è necessario effettuarlo manualmente a cura di ogni singolo incaricato, tale aggiornamento deve avvenire almeno una volta in settimana.
La maggior parte dei virus vengono diffusi tramite la posta elettronica e Internet; di conseguenza è necessario attenersi alle seguenti ulteriori istruzioni:

- non aprire e- mail che contengano un'estensione doppia;
- prima di aprire una e – mail, in particolare se non richiesta o nel caso in cui si ritenga quantomeno insolita, verificare il mittente ed eventualmente non aprire allegati o collegarsi a siti internet contenuti nel testo della e – mail;
- prima di utilizzare floppy o CD di qualsiasi provenienza, procedere con un controllo da parte dell'antivirus;

Protezione dei dati da distruzione o perdita, anche accidentale

Il titolare del trattamento ha provveduto a installare un sistema di salvataggio centralizzato e automatico dei dati. Il salvataggio viene eseguito a cadenza stabilita e comunque non superiore a sette giorni, da personale appositamente incaricato.

Gli incaricati dovranno però anche in questo caso concorrere e mettere in atto tutte le procedure affinché la misura di sicurezza non risulti inefficace a causa di attività non corrette.
In particolare è necessario che gli incaricati provvedano a salvare tutti i dati sul server evitando di mantenerli in locale sui singoli PC.
E' talora comunque possibile che, a causa del sistema informatico utilizzato o dei programmi installati, i dati siano elaborati in locale sul singolo PC. In tal caso è necessario segnalare la situazione all'amministratore di sistema o al responsabile del trattamento o al titolare il quale provvederà ad attuare le procedure automatiche o manuali al fine di inviare periodicamente i dati sul server in modo tale da procedere al loro salvataggio automatico. Nel caso in cui non sia possibile prevedere l'invio degli archivi sul server, sarà cura dei singoli incaricati provvedere al salvataggio di tali dati.
Di regola comunque è opportuno che il salvataggio non avvenga tramite floppy ma tramite masterizzazione su CD. Tale salvataggio dovrà essere eseguito con cadenza almeno settimanale. Naturalmente i supporti sui quali saranno eseguiti i salvataggi dovranno essere conservati in modo appropriato. E' necessario quindi che siano conservati in contenitori chiusi a chiave e protetti (armadi, cassetti,ecc.) o consegnati al soggetto preposto al back up centralizzato.

Protezione dei dati contenuti nei supporti rimovibili

Anche l'utilizzo di supporti rimovibili deve essere conforme alle norme di sicurezza previste. In particolare, nel caso tali supporti siano riutilizzati, anche da altri incaricati, e in essi siano contenuti dati sensibili o giudiziari, primo del loro riutilizzo, devono esser cancellate tutte le informazioni contenute, in modo tale da non consentire in alcun modo la conoscenza da parte di terzi di tali dati. Si raccomanda quindi:
nel caso in cui sia necessario conservare i supporti informatici contenenti dati sensibili o giudiziari, la conservazione deve avvenire in contenitori chiusi a chiave.
Nel caso in cui i supporti informatici siano riutilizzati, anche da altri incaricati, deve essere eseguita la formattazione totale del supporto.
Nel caso in cui, per motivi tecnici, non possa essere eseguita la formattazione, il supporto deve essere distrutto.
Nonostante questa misura minima sia riferita ai dati sensibili o giudiziari, è buona norma applicare questa procedura a tutti i supporti utilizzati, indipendentemente dal tipo di dato registrato.

Attenzione al trattamento dei dati dovrà avvenire anche in caso di utilizzo di altri strumenti per i quali sono disposte queste ulteriori istruzioni:

Fax.:

Verificare la correttezza del numero telefonico relativo al fax dell'utente e porre attenzione alla digitazione del numero telefonico;
provvedere a stampare sul retro del fax inviato il report di stampa verificando l'esattezza delle pagine inviate e la correttezza dell'invio;
Nel caso in cui siano inviati documenti contenenti dati sensibili o giudiziari provvedere, se possibile, a inviare il documento in due fasi, dividendo il dato identificativo dagli altri dati o, in alternativa, chiamando il destinatario per informarlo dell'arrivo del fax in modo tale che quest'ultimo possa provvedere alla tempestiva raccolta del documento stesso ed eventualmente comunicare al mittente eventuali errori di trasmissione o leggibilità del documento ricevuto.

Fotocopiatrici:
non dimenticare sotto il coperchio della fotocopiatrice il documento da duplicare;

nel caso in cui il documento contenga dati sensibili o giudiziari provvedere personalmente all'effettuazione della fotocopia e non consegnarlo ad altri soggetti per l'esecuzione del compito.

Scanner:
verificare la correttezza dell'esecuzione, la leggibilità del documento od eventuali errori di acquisizione del testo.

TRATTAMENTI CON STRUMENTI NON ELETTRONICI

Protezione dei dati dal rischio di accessi non consentiti agli atti e ai documenti cartacei

Anche gli atti e i documenti cartacei contenenti dati personali devono essere sottoposti a misure di sicurezza.
In particolare è necessario che tutti i documenti siano conservati negli apposti armadi, cassettiere, raccoglitori o archivi in genere. E' necessario inoltre che al termine dell'orario lavorativo le scrivanie siano prive di documenti, fascicoli, faldoni contenenti dati personali. Ogni incaricato è responsabile della protezione fisica dei documenti a lui affidati. Particolare attenzione dovrà essere destinata a eventuali stampe dei tabulati prodotti dall'esecuzione di programmi informatici. Le stampe dovranno quindi essere immediatamente raccolte e conservate da parte di chi ha eseguito i comandi di stampa, in particolare se la stampante è condivisa con altri uffici/servizi ed è situata in altri locali. Le stesse procedure dovranno essere attuate per l'utilizzo di fax o fotocopiatrici.
Ulteriore attenzione dovrà essere rivolta alla distruzione dei documenti, ad esempio strappando i documenti prima di cestinarli, o utilizzando i tritadocumenti in particolar modo per atti contenenti dati sensibili o giudiziari o particolarmente riservati.
Ulteriore attenzione dovrà essere rivolta ai documenti contenenti dati sensibili o giudiziari con particolare attenzione alla documentazione sanitaria contenuta nelle schede sanitarie e/o nei piani di assistenza individualizzati quando vengono consultati per l'assistenza giornaliera agli ospiti. A tal fine è necessario che tali documenti, quando sono al di fuori dei loro archivi durante l'utilizzo quotidiano, siano tenuti sotto il controllo e la custodia degli incaricati, mentre al termine dell'impiego quotidiano, devono essere riposti in armadi, cassetti, archivi o contenitori chiusi a chiave. Non devono assolutamente essere lasciati sulle scrivanie o postazioni di lavoro a disposizione di chiunque entri nell'ufficio/locale/reparto. In caso di ingresso nel locale/ufficio/reparto di persone estranee è buona norma fare in modo di impedire l'accesso a tali documenti, ad esempio conservandoli temporaneamente in un cassetto o in una teca, sempre comunque sotto il controllo dell'incaricato.
Si ricorda inoltre di provvedere alla separazione dei dati idonei a rivelare stato di salute e vita sessuale da altri dati non necessari alle finalità del trattamento. Ad esempio, i certificati medici possono essere mantenuti nel faldone contenente la documentazione dell'interessato, ma separandoli dagli altri documenti, ad esempio utilizzando una busta chiusa.

UTILIZZO DI ALTRI STRUMENTI

E' possibile che, per il trattamento di dati personali, vengano utilizzati anche altri strumenti quali ad esempio telecamere, macchine fotografiche, cellulari con integrata fotocamere, ecc….
Anche per l'utilizzo di tali strumenti è necessario attuare misure di sicurezza.
In particolare il rischio più probabile è quello di perdere o dimenticare nei luoghi visitati lo strumento.

E’ quindi opportuno, se lo strumento è predisposto, inserire un PIN per proteggere i dati inseriti. Tale PIN può essere condiviso con altre persone autorizzate a tali trattamenti o consegnato al custode delle password o al titolare.
Una volta effettuate le foto o le riprese, le stesse dovranno essere riversate sul sistema informatico se si utilizzano modelli elettronici e dovranno essere cancellate le immagini dalla memoria dello strumento. Se invece vengono utilizzati modelli non elettronici, le foto sviluppate o le videocassette devono essere conservate con le stesse modalità indicate nella sezione dedicata ai trattamenti con strumenti cartacei.

VIDEOSORVEGLIANZA

In caso di installazione di sistemi di videosorveglianza, gli addetti alla visione delle immagini, nonché alla loro registrazione, se prevista, dovranno utilizzare tali strumenti unicamente per le funzioni di controllo degli accessi e/o delle zone in cui il titolare ha rilevato vi siano rischi specifici e di conseguenza installato le telecamere. Non potrà essere concessa la visone delle immagini a persone non autorizzate. I monitor dovranno esser spenti o dovranno essere attivate le chiusure dei locali ove sono posti, quando gli incaricati non sono presenti. Nel caso in cui sia predisposto un sistema di registrazione delle immagini, eventuali supporti audiovisivi rimovibili (come ad esempio le cassette VHS), dovranno essere custoditi in contenitore chiuso a chiave (armadio, cassetto) e i dati dovranno essere cancellati dopo al massimo 24 ore (fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.). Nel caso in cui le immagini siano registrate su supporto informatico si provvederà, ove possibile, alla cancellazione automatica delle immagini entro tale termine. Se ciò non fosse possibile, saranno date specifiche istruzioni agli incaricati in merito alle modalità di cancellazione.

RESPONSABILITÀ’ E SANZIONI

Il codice della Privacy prevede sanzioni amministrative e penali, oltre al risarcimento del danno ai fini civilistici.
In questa sezione saranno indicate le principali sanzioni previste dal Codice le quali coinvolgono, oltre il titolare e il responsabile, anche gli incaricati

OMESSA O INIDONEA INFORMATIVA ALL’INTERESSATO (art. 161)
La violazione dell’obbligo di fornire un’idonea informativa sul trattamento dei dati comuni comporta una sanzione amministrativa da tremila a diciottomila euro. Nel caso di dati trattamenti di sensibili o giudiziari la sanzione può essere aumentata fino a trentamila euro con un minimo di cinquemila euro.

OMESSA ADOZIONE DI MISURE MINIME DI SICUREZZA (art. 169)
La mancata adozione delle misure minime di sicurezza è sanzionata penalmente con l’arresto sino a due anni o con l’ammenda da diecimila a cinquantamila euro. E’ previsto il cosiddetto “ravvedimento operoso”. All’autore del reato, all’atto dell’accertamento, è impartita una prescrizione e fissato un termine per la regolarizzazione. L’adempimento della prescrizione e il pagamento di una somma pari a un quarto del massimo dell’ammenda stabilita per la contravvenzione, estinguono il reato.
All’adozione delle misure minime di sicurezza è tenuto il titolare. Tuttavia, il disciplinare tecnico nel quale sono previsti i modi di adozione di tali misure, prevede che le modalità tecniche siano adottate a cura del titolare, del responsabile e dell’incaricato. La responsabilità quindi di mantenere in attuazione le misure di

sicurezza adottate dal titolare e a disposizione degli incaricati ricade anche su questi ultimi.

TRATTAMENTO ILLECITO DI DATI (art. 167)

“ 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 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.
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 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.”
Come si evince dall’articolo la responsabilità del fatto illecito è ascritta a “chiunque”, ciò significa che si dovrà, in caso di trattamento illecito, verificare il soggetto che lo ha commesso, non esentando dalla sanzione né il titolare, né il responsabile ma nemmeno l’incaricato.

Il codice prevede inoltre responsabilità civile per il risarcimento del danno.

L’articolo 15 prevede che “ chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell’articolo 2050 del codice civile.
Il danno non patrimoniale è risarcibile anche in caso di violazione dell’articolo 11.”
Questo significa che innanzitutto si viene ritenuti responsabili del danno se non si riesce a dimostrare di aver adottato ogni possibile misura idonea ad evitare il danno stesso. Inoltre, poiché l’articolo 11 (vedi sezione regole generali) è uno degli articoli più significativi del Codice in merito alla correttezza del trattamento, viene prevista la possibilità di richiesta di risarcimento del danno non patrimoniale anche in caso di violazione di quest’articolo.