



FNOVI

*FEDERAZIONE NAZIONALE
ORDINI VETERINARI ITALIANI*

La privacy nelle attività veterinarie

Dott. Giorgio Neri

Dicembre 2006

Sede: Via del Tritone, 125 – 00187 ROMA
Tel. 06.485923 - 4881190 - Fax 06.4744332 - E-mail: info@fnovi.it
Codice Fiscale 96203850589

La privacy nelle attività veterinarie

Il Decreto Legislativo 196/2003: “Codice in materia di protezione dei dati personali” prevede una serie di obblighi in capo a colui che si trovi a trattare i dati personali di terzi. Alcune di queste misure devono essere adottate preventivamente rispetto ad altre.

In altri casi, invece, non è la legge, bensì questioni di ragionevolezza ed opportunità, che impongono a colui che tratta i dati personali di adottare iniziative preventive finalizzate ad un lecito trattamento dei dati.

Per questo motivo, molto semplicisticamente, potremmo pensare di suddividere, in ordine cronologico, il percorso finalizzato all’adempimento degli obblighi previsti dal Codice, in quattro passaggi fondamentali:

- § Passo 1: imparare a conoscere e a classificare i dati personali;
- § Passo 2: acquisire consapevolezza sulle modalità di trattamento dei dati personali;
- § Passo 3: mettere in atto gli adempimenti previsti a tutela dei dati e delle persone a cui si riferiscono;
- § Passo 4: riconoscere i diritti previsti dalla legge a tutela dell’interessato

Passo 1: imparare a conoscere e a classificare i dati personali

Ogni trattamento di dati personali ad eccezione dei dati anonimi, effettuato nel corso di attività pubbliche o private, è compreso nel campo di applicazione del D. Leg. 196/2003: “Codice in materia di protezione dei dati personali”.

Per comprendere appieno il significato di questa affermazione occorrerà precisare che si definisce 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*”, e si intende per 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*”.

I dati personali possono essere classificati in funzione delle informazioni che recano, e ordinati secondo un livello di importanza crescente in funzione del grado di pregiudizio che un trattamento non corretto può arrecare ai diritti, alle libertà fondamentali e alla dignità dell’“Interessato” (secondo la definizione di legge: “*la persona fisica, la persona giuridica, l’ente o l’associazione cui si riferiscono i dati personali*”), in:

- § Dati anonimi, il cui trattamento, come detto, non potendo recare danno ad alcuno, non necessita di alcuna formalità;

§ Dati cifrati o crittografati: sono i dati personali che, attraverso particolari procedimenti, vengono resi temporaneamente inintelligibili;

§ Dati personali semplici: rientrano in questa categoria tutti i dati personali che non possono essere compresi nelle altre;

§ Dati personali identificativi: sono tutti i dati che permettono l'identificazione immediata del soggetto a cui si riferiscono;

§ Dati personali sensibili e giudiziari: i dati sensibili sono “*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*” (su questa categoria di dati personali esiste una grande confusione in quanto spesso si tende a credere, erroneamente, che ogni dato personale di una certa delicatezza, come per esempio l'estratto conto della banca, rappresenti un dato sensibile); i dati giudiziari, invece, sono i “*dati personali idonei a rivelare provvedimenti... 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...*”.

Di pari passo con questa classificazione, la legge prevede obblighi di grado crescente per trattamenti di dati personali che necessitino di cautele maggiori.

Passo 2: acquisire consapevolezza sulle modalità di trattamento dei dati personali

A prescindere dalla loro classificazione, la legge dispone che i dati personali debbano essere trattati secondo criteri da applicarsi universalmente. Il Codice sulla Privacy, infatti, “*garantisce che il trattamento dei dati si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali*”. Per questo i dati personali dovranno essere “*trattati in modo lecito e secondo correttezza; raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; esatti e, se necessario, aggiornati; pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati*”. Anche i programmi dei computer dovranno essere configurati in modo da ridurre al minimo “*l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità*”.

La non osservanza anche di uno solo di questi precetti configura un trattamento illecito di dati, fattispecie che può comportare l'irrogazione di una sanzione penale, nonché la possibilità per la parte lesa di chiedere in sede civile il risarcimento dei danni patiti, sia patrimoniali che non patrimoniali (danno morale, danno biologico e danno esistenziale). Inoltre i dati trattati illecitamente sono inutilizzabili (mancanza di effetti giuridici).

Passo 3: mettere in atto gli adempimenti previsti a tutela dei dati e delle persone a cui si riferiscono

Una volta stabilito cosa sono e come si devono classificare i dati personali, e quali sono i principi a cui si deve ispirare colui che procede al loro trattamento, è necessario stabilire quali siano gli oneri a carico del Titolare del trattamento, ovvero della “*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*”. In questa disamina saranno prese in considerazione soltanto le tre categorie di titolari a cui essa si indirizza: il veterinario e l’organismo veterinario privato (es. associazione professionale), l’organismo veterinario pubblico (es. Asl), l’organismo pubblico non sanitario (es. Ordine professionale).

Come è evidente dalla definizione di legge, il titolare del trattamento può essere, a seconda dei casi, una persona fisica o un altro soggetto diverso dalla persona fisica. Nel caso di un’associazione professionale il titolare sarà la stessa associazione; nel caso di un Asl potrà essere, per esempio, l’azienda stessa, oppure il servizio o l’unità operativa da essa dipendenti; nel caso di un Ordine professionale sarà l’ente stesso.

Sul titolare del trattamento incombe l’obbligo di adottare, e far adottare, tutte le misure necessarie previste dal “Codice sulla Privacy”, e conseguentemente la responsabilità civile e penale nel caso non adempia a tali obblighi.

a) la nomina dei Responsabili e degli Incaricati al trattamento

Nel caso lo ritenga opportuno, il titolare può delegare gli oneri di sua competenza ad uno o più soggetti, denominati Responsabili del trattamento, che dovrà scegliere tra quelli che abbiano adeguata esperienza, capacità e affidabilità per poter fornire sufficienti garanzie circa l’adempimento ai compiti loro assegnati, e indipendentemente dal fatto che essi presiedano a trattamenti effettuati all’interno e/o all’esterno dell’attività. Generalmente la figura del responsabile del trattamento ha poco significato nelle attività ove lavorano una o poche persone, mentre potrebbe trovare una sua collocazione nelle strutture più complesse, magari suddivise in reparti o in distinte unità operative. Spesso, poi, potrebbe essere opportuno nominare responsabili del trattamento figure esterne all’attività, come il commercialista o il laboratorio di analisi, per far sì che gli stessi non siano tenuti a loro volta, ed autonomamente, ad adempiere agli oneri previsti a carico del titolare del trattamento. La nomina del responsabile del trattamento deve essere effettuata per iscritto, e sottoscritta per accettazione dallo stesso, e nella lettera di nomina devono essere analiticamente elencati i compiti a lui attribuiti e le disposizioni a cui dovrà attenersi.

Al titolare o al responsabile del trattamento compete poi la nomina degli Incaricati, che sono “*le persone fisiche autorizzate a compiere operazioni di trattamento*”. Anche gli incaricati dovranno essere nominati per iscritto, e nella lettera di incarico dovranno essere indicati i dati a cui potranno avere accesso, i trattamenti che potranno effettuare, le modalità previste circa il trattamento, la protezione e la custodia dei dati, nonché tutte quelle disposizioni a cui il titolare o il responsabile riterranno opportuno che gli incaricati si attengano.

Mentre i soggetti privati possono, nel rispetto delle regole previste dal Codice sulla Privacy, trattare qualunque dato personale, i soggetti pubblici possono trattare i dati personali unicamente con finalità strettamente pertinenti alle loro attività istituzionali.

Inoltre i soggetti pubblici possono trattare i dati sensibili e giudiziari solo se previsto da una legge o da un regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite; nel caso non esistano tali leggi o regolamenti, i dati sensibili potranno comunque essere trattati previa autorizzazione del Garante (vedi più avanti). Gli altri tipi di dati, invece, potranno essere trattati dai soggetti pubblici anche in mancanza di una legge o un regolamento che lo preveda espressamente, eccetto che nel caso si renda necessaria la comunicazione di tali dati ad altri soggetti pubblici, nel qual caso si può comunque derogare all'esistenza della legge o del regolamento attraverso una preventiva comunicazione al Garante (vedi più avanti), nonché nel caso il trattamento riguardi la comunicazione dei dati stessi a soggetti privati, o la loro diffusione.

A questo punto lo staff è stato istruito su quali dati trattare e su come trattarli; ciò nonostante non è ancora possibile iniziare materialmente il trattamento dei dati. Infatti la legge prevede che il titolare o il responsabile pongano in essere alcuni altri adempimenti, che devono essere preventivi al trattamento, a tutela degli interessati e a garanzia della sicurezza dei dati.

b) l'Autorizzazione del Garante

Uno di questi adempimenti è l'Autorizzazione (che spesso viene confusa con un altro istituto: il consenso), che deve essere richiesta preventivamente al Garante nel caso di trattamento di dati sensibili. Il Garante si pronuncia in merito a tale richiesta entro quarantacinque giorni, trascorsi i quali senza nessuna risposta il richiedente deve desumere che l'istanza è stata respinta ("silenzio-rigetto").

La legge prevede comunque la possibilità per il Garante di emanare delle autorizzazioni generali che abbiano efficacia in particolari settori, cosa che regolarmente avviene. Senza dilungarsi in specifiche eccessive, si può dire che i dati sensibili che generalmente sono trattati dai soggetti a cui si riferisce la presente trattazione sono ricompresi nelle autorizzazioni generali emanate dal Garante sulla Privacy, per cui si può concludere che agli stessi non è generalmente necessario prendere alcuna autonoma iniziativa in tal senso.

c) la Comunicazione al Garante

La legge prevede due casi in cui il titolare o il responsabile del trattamento sono tenuti a comunicare preventivamente al Garante l'intenzione di effettuare il trattamento dei dati personali. Di questi, uno solo ha la possibilità di verificarsi nelle attività oggetto del presente lavoro, e cioè la già citata comunicazione di dati personali diversi da quelli sensibili e giudiziari da un soggetto pubblico ad un altro in assenza di una previsione di legge o regolamentare.

In questo caso, a differenza di quanto si verifica per l'autorizzazione, se entro quarantacinque giorni dalla ricezione della comunicazione da parte del Garante il titolare dell'istanza non ottiene alcuna risposta, può presumere il silenzio-assenso.

d) la Notificazione al Garante

Un altro adempimento a carico del titolare o del responsabile del trattamento è l'obbligo di notificare al Garante alcuni trattamenti riguardanti certi tipi di dati o alcuni trattamenti effettuati con certe finalità. I sei casi previsti dal Codice non riguardano tuttavia le attività oggetto della presente trattazione, per cui si può senz'altro affermare che questo istituto non riguarda i soggetti in esame.

In ogni caso, vale la pena di specificare che i dati il cui trattamento richiede la preventiva notificazione al Garante, possono poi essere utilizzati senza necessità di lasciar decorrere alcun termine dall'avvenuto adempimento.

e) l'Informativa

Un adempimento a cui invece i soggetti che trattano dati personali devono ottemperare nella quasi totalità dei casi, è quello dell'informativa. In pratica, infatti, l'unico caso in cui questa non deve essere resa si verifica nell'ipotesi che i dati personali dell'interessato siano acquisiti presso terzi e il trattamento sia finalizzato all'adempimento di un obbligo previsto da una legge, da un regolamento o dalla normativa comunitaria.

L'informativa è un documento la cui redazione è piuttosto semplice (soprattutto se si ha avuto l'avvertenza di eseguire preventivamente quanto riportato nei passi 1 e 2!), che ha la finalità di informare preventivamente l'interessato su alcune notizie relative al trattamento dei propri dati personali, e a renderlo edotto dei propri diritti.

La legge non prevede una modalità obbligatoria con cui le informazioni debbano essere rese, per cui l'informativa potrà essere esposta a voce, o portata in visione, oppure consegnata su un qualsiasi supporto. Pertanto, la sottoscrizione che spesso viene richiesta in calce al documento reso per iscritto può avere come unica logica finalità quella di costituire una prova a favore del titolare del trattamento, di aver adempiuto a tale obbligo.

Le notizie che il titolare o il responsabile del trattamento deve rendere all'interessato sono le seguenti:

- § *“le finalità e le 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 personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;*
- § *i diritti di cui all'articolo 7;*
- § *gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.”*

f) il Consenso

Anche il consenso rappresenta un adempimento richiesto in buona parte dei trattamenti di dati personali, soprattutto se tali dati sono trattati da soggetti privati. Infatti il fatto che la legge imponga ai soggetti pubblici di trattare solo alcuni tipi di dati, e solo per finalità istituzionali, ha come logica contropartita che il trattamento dei dati personali messo in atto da tali soggetti solo raramente necessita del consenso da parte dell'interessato.

Nel nostro caso tuttavia tale ampiezza di applicazione è più teorica che pratica in quanto la legge prevede alcune eccezioni che di fatto, nelle attività oggetto della presente trattazione fanno sì che tale obbligo trovi riscontro solo in una limitata casistica.

Il consenso deve essere “*espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato*” e “*può riguardare l'intero trattamento ovvero una o più operazioni dello stesso*”. Tuttavia il fatto che il consenso possa riguardare l'intero trattamento non deve far pensare che siano da ritenersi valide espressioni generiche del tipo “presto il consenso al trattamento dei miei dati personali”: come riportato più sopra, il consenso deve essere riferito ad un trattamento specificamente individuato, per cui i trattamenti per i quali lo si deve richiedere dovranno essere quanto meno analiticamente elencati nella sezione dedicata alla sottoscrizione del consenso stesso.

La richiesta di consenso deve necessariamente seguire o essere contestuale all'informativa (e comunque precedente al trattamento dei dati), e il consenso dell'interessato deve necessariamente essere reso per iscritto (solo nel caso di trattamento di dati relativi allo stato di salute dell'interessato, effettuato da un sanitario, può essere reso oralmente e annotato per iscritto dal sanitario stesso).

Premesso che i dati idonei a rivelare lo stato di salute non possono mai essere oggetto di diffusione (il Codice definisce la “diffusione” come il dare conoscenza dei dati personali a soggetti indeterminati, diversamente dalla “comunicazione” che è definita come la messa a disposizione dei dati personali a soggetti determinati), si tratta quindi di stabilire in quali casi il consenso dell'interessato sia obbligatorio ai fini del trattamento dei dati personali dello stesso. Ciò dipende sia dalla connotazione del titolare dei dati, e sia dal tipo di dati oggetto di trattamento:

§ Soggetti e organismi sanitari privati: come regola generale, questi soggetti sono tenuti a chiedere il consenso in qualunque caso trattino dati personali. Sono tuttavia previste importanti eccezioni per cui:

- il trattamento di dati personali diversi da quelli sensibili e giudiziari non richiede il consenso dell'interessato qualora sia finalizzato ad un obbligo di legge, ad un adempimento contrattuale intercorrente con l'interessato (quale, per esempio, l'esecuzione della prestazione richiesta), o qualora i dati personali siano tratti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque e il trattamento rispecchi le finalità per cui l'elenco, il registro, l'atto o il documento è stato redatto;
- il trattamento di dati sensibili relativi allo stato di salute non richiede il consenso dell'interessato qualora sia finalizzato alla tutela della salute o dell'incolumità fisica di terzi o della collettività;
- il trattamento degli altri dati sensibili e dei dati giudiziari non richiede il consenso dell'interessato qualora sia finalizzato ad un adempimento di legge.

§ Organismi sanitari pubblici: fatte salve le limitazioni previste dal Codice per questi soggetti riguardo il trattamento di dati personali, come regola generale essi non sono mai tenuti a chiedere il consenso degli interessati. A questa regola è tuttavia prevista un'eccezione:

- nel caso l'organismo sanitario pubblico tratti dati sensibili relativi allo stato di salute, con finalità di tutela della salute o dell'incolumità fisica dell'interessato, è richiesto il consenso dello stesso.

§ Organismi pubblici non sanitari: fatte salve le limitazioni previste dal Codice per questi soggetti riguardo il trattamento di dati personali, essi non sono mai tenuti a chiedere il consenso degli interessati.

g) le Misure di Sicurezza

L'ultimo adempimento a carico del titolare o del responsabile del trattamento che deve essere messo in atto preventivamente al trattamento dei dati personali è l'adozione di idonee misure di sicurezza a protezione dei dati personali.

Le "idonee misure di sicurezza" non sono state individuate specificatamente dal legislatore, ma sono genericamente definite come tutte quelle che, in funzione delle conoscenze acquisite in base al progresso tecnico, della natura dei dati e delle specifiche caratteristiche del trattamento, sono necessarie per garantire la sicurezza dei dati personali.

Saranno dunque il titolare e il responsabile del trattamento che, modulando le misure in funzione delle variabili sopra riportate, dovranno attuare i provvedimenti che ritengono più adeguati *"in modo da ridurre al minimo... i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta"*.

Si badi che l'inversione dell'onere della prova, prevista in questo caso, farà sì che nell'ipotesi di incidente dovranno essere il titolare o il responsabile del trattamento a dimostrare di avere posto in essere tutte le misure idonee per evitarlo, e non l'interessato a dover fornire prova del contrario.

La mancata adozione di idonee misure di sicurezza espone il titolare e il responsabile del trattamento al risarcimento dell'eventuale danno patito dall'interessato, non prevedendo tuttavia il Codice sulla Privacy alcuna sanzione per il solo fatto di non averle adottate. Fanno eccezione a questa regola una serie di misure di sicurezza, denominate "misure minime", che il legislatore ha elencato dettagliatamente e che il titolare e il responsabile del trattamento sono tenuti ad adottare in ogni caso, a pena di pesanti sanzioni penali oltre all'obbligo di risarcire l'eventuale danno patito dall'interessato.

Le misure minime di sicurezza che devono essere obbligatoriamente attuate, preventivamente al trattamento dei dati personali, sono le seguenti:

Nel caso di trattamenti con strumenti elettronici:

- *"autenticazione informatica;*
- *adozione di procedure di gestione delle credenziali di autenticazione;*
- *utilizzo di un sistema di autorizzazione;*
- *aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;*
- *protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;*
- *adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;*

- *tenuta di un aggiornato documento programmatico sulla sicurezza*” (solo qualora si trattino dati sensibili o giudiziari);
- *“adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.”*

Nel caso di trattamenti senza strumenti elettronici:

- *“aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;*
- *previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;*
- *previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.”*

Per maggiori dettagli circa le modalità di adozione delle misure minime di sicurezza, consultare l'allegato B al D. Leg. 196/2003: “Disciplinare tecnico in materia di misure minime di sicurezza”, riprodotto in fondo alla presente trattazione.

Passo 4: riconoscere i diritti previsti dalla legge a tutela dell'interessato

L'unico adempimento a carico del titolare e del responsabile del trattamento, tra quelli presi in considerazione, che non deve essere preventivo al trattamento dei dati personali è il riconoscimento dei diritti dell'interessato. Ciò non significa, tuttavia, che la cosa non debba comportare degli adempimenti preventivi. Il titolare e il responsabile del trattamento, infatti, dovranno riscontrare prontamente e celermente alle richieste, anche informali, dell'interessato che chiedi il riconoscimento delle garanzie che il Codice gli assicura, e ciò non può che comportare che i dati personali dovranno essere organizzati in modo che le azioni richieste si possano svolgere con completezza, celerità e certezza.

I diritti che la legge riconosce all'interessato, e che si possono classificare in diritti di conoscenza e informazione, diritti di certificazione e controllo, diritti di resistenza e opposizione, sono i seguenti:

§ *“L'interessato ha diritto di 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.*

§ *L'interessato ha diritto di 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.

§ *L'interessato ha diritto di 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.

§ *L'interessato ha diritto di 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.”

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 modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è 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 è 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, è 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 può 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 vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è 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 responsabilità 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.