

Roma, 18 giugno 2004

Prot. n. 1672/2004/F/mgt
Circolare n. 11/2004

Ai Presidenti degli Ordini
Provinciali

LORO SEDI

p.c.
Ai membri del Comitato
Centrale

Ai membri del Collegio dei
Revisori dei Conti

LORO SEDI

Oggetto: D. Lgs. 30 giugno 2003 n. 196 – Codice in materia di protezione dei dati personali – Chiarimenti in merito alla normativa sulla Privacy applicabile ai medici veterinari ed agli Ordini Professionali

Caro Presidente,

pervengono in Federazione numerose richieste di chiarimento in ordine all'argomento indicato in oggetto, con particolare riferimento alla corretta applicazione del Decreto Legislativo n. 196/2003 ed all'impatto che il nuovo codice in materia di protezione dei dati personali, entrato in vigore lo scorso 1 gennaio 2004, (anche noto come *Codice sulla Privacy*) potrà avere sull'attività svolta dai liberi professionisti e dagli Ordini Professionali e dalle Federazioni o Consigli Nazionali in adempimento dei fini istituzionali stabiliti dall'ordinamento.

Rinviando alla lettura di quanto trasmesso in allegato (all. A) – che rappresenta una illustrazione della disciplina nelle sue linee essenziali – si anticipa quanto segue.

A) I medici veterinari:

1. non sono soggetti a nessuno degli adempimenti previsti nei confronti dell'Autorità Garante (notificazioni, comunicazioni e richiesta di autorizzazione) semprechè i dati trattati non esulino dalla loro normale attività;

2. sono i *titolari del trattamento* e, se ne sentiranno l'esigenza, potranno procedere alla designazione di uno o più *responsabili e incaricati* del trattamento. In tal caso dovranno osservare le formalità così come richieste;
3. sono tenuti all'osservanza dell'adempimento della *informativa*. Tra le novità del Codice sulla Privacy è adesso consentito che l'*informativa* sia resa per iscritto o anche, in forma orale, ma con evidenti svantaggi sotto il profilo probatorio. Tenuto conto della complessità dell'informazione da dare, motivi di praticità e di cautela inducono a consigliare il rilascio dell'*informativa* in forma scritta attraverso la predisposizione di un modello (se ne propone un fac-simile) (all. B) da conservare previa acquisizione della firma dell'interessato;
4. non sono tenuti alla raccolta del *consenso* se trattano dati personali per finalità strettamente relative all'espletamento della professione. Se il trattamento ha anche finalità facoltative, sarà necessario richiedere, e per iscritto, il consenso agli interessati;
5. è obbligatorio predisporre qualunque precauzione necessaria alla tutela dei dati. Ci si riferisce alle cosiddette "misure minime di sicurezza", specificate nell'Allegato B) – *Disciplinare tecnico in materia di misure minime di sicurezza* del Codice sulla Privacy. Si ritiene opportuno suggerire di rivolgersi ai tecnici che forniscono la manutenzione per i propri computer per farsi rilasciare un'attestazione comprovante l'adozione delle misure privacy.
6. non è previsto l'obbligo di redigere il *Documento Programmatico sulla Sicurezza* (DPS) poiché, nell'espletamento della propria attività, non si trattano dati sensibili e giudiziari.

B) I Consigli Direttivi degli Ordini Provinciali ed il Comitato Centrale della Federazione:

1. non sono soggetti a nessuno degli adempimenti previsti nei confronti dell'Autorità Garante (notificazioni, comunicazioni e richiesta di autorizzazione). In argomento è intervenuto il Garante il quale ha precisato che sono sottratti ai suddetti obblighi i trattamenti effettuati da soggetti pubblici per la tenuta di pubblici registri o elenchi conoscibili da chiunque, nei limiti di quanto stabilito dalle leggi istitutive e dai regolamenti attuativi in vigore e per il perseguimento delle finalità ivi indicate¹;
2. sono i *titolari del trattamento* e, se ne sentiranno l'esigenza, potranno procedere alla designazione di uno o più *responsabili e incaricati* del trattamento. In tal caso dovranno osservare le formalità così come richieste;
3. sono tenuti all'osservanza dell'adempimento della *informativa*. Valgono le stesse considerazioni innanzi esposte e, pertanto, si consiglia il rilascio dell'*informativa* in forma scritta attraverso la predisposizione di un modello (se ne propone un fac-simile) (all. C) da conservare previa acquisizione della firma dell'interessato;

¹ Vedi articoli 3 e 7 del D. Lgs. C.P.S. 13 settembre 1946, n. 233 e gli articoli del Capo I, D.P.R. 5 aprile 1050, n. 221.

4. non sono tenuti alla raccolta del *consenso*. Tale esclusione è disciplinata dall'art. 18, comma 4, del *Codice sulla Privacy*;

5. è obbligatorio predisporre qualunque precauzione necessaria alla tutela dei dati. Ci si riferisce alle cosiddette "misure minime di sicurezza", specificate nell'Allegato B) – *Disciplinare tecnico in materia di misure minime di sicurezza* del Codice sulla Privacy. Si ritiene opportuno suggerire, anche in questo caso, di rivolgersi ai tecnici che forniscono la manutenzione per i propri computer per farsi rilasciare un'attestazione comprovante l'adozione delle misure privacy;

6. nell'ambito delle misure minime di sicurezza da adottare per il trattamento dei dati sensibili con l'ausilio di strumenti elettronici, viene disciplinato il *Documento Programmatico sulla Sicurezza* (DPS) che deve essere redatto entro il **30 giugno 2004**² e che, dal 2005, dovrà essere redatto o aggiornato entro il 31 marzo di ogni anno. L'obbligo di redigere il DPS viene disciplinato nei casi in cui si trattino dati sensibili o giudiziari con l'utilizzo di strumenti elettronici: i Consigli Direttivi degli Ordini Professionali, non trattando dati sensibili e giudiziari³, non devono predisporre il Documento Programmatico sulla Sicurezza.

Confidando di aver fornito sufficienti delucidazioni in argomento, restando a disposizione per quanto altro possa occorrere, è gradita l'occasione per inviare cordiali saluti.

Il Presidente
(Dott. Domenico D'Addario)

Allegati

G

² Nei prossimi giorni sarà esaminato un decreto legge per prorogare gli adempimenti previsti dal testo unico sulla privacy. La proroga principale potrebbe riguardare proprio gli adempimenti in scadenza per il prossimo 30 giugno.

³ Gli unici dati giudiziari di cui gli Ordini sono custodi sono rinvenibili nei certificati attestanti il pieno godimento dei diritti civili ed il certificato generale del casellario giudiziale necessari all'iscrizione i quali, però, sono trattati con modalità esclusivamente cartacea.

La disciplina sulla Privacy Aggiornamento sugli adempimenti

Appare preliminarmente opportuno chiarire che si è in un ambito soggetto ancora a cambiamenti, e numerosi sono i provvedimenti e le note emesse a cura dell’Autorità Garante per la protezione dei dati personali, tendenti a meglio specificare la portata innovativa della norma al nostro esame.

Il primo passo da compiere per orientarsi è quello di identificare la tipologia dei dati soggetti a trattamento (*dati personali*, *dati sensibili*, *dati giudiziari*): i dati personali infatti sono soggetti a tutela ma per la categoria più limitata dei *dati sensibili* e *giudiziari* sono previsti adempimenti e misure di sicurezza particolarmente rigorosi.

Altra distinzione fondamentale riguarda la modalità con la quale i dati personali sono trattati: dati trattati con l’ausilio di strumenti informatici (computer) o senza (i c.d. trattamenti “cartacei”, pratiche, fascicoli ecc.).

1. Principali termini utilizzati dal legislatore

È indispensabile, ai fini della chiarezza espositiva, riportare preliminarmente i principali termini utilizzati dal legislatore.

Per **trattamento** si intende qualunque operazione o complesso di operazioni, effettuate 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 personali, anche se registrati in una banca dati. In sostanza, la raccolta e la conservazione di dati personali assumono sempre rilievo, sia se effettuata su carta, sia se effettuata mediante computer.

Per **dato personale** si intende qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati. È dato personale anche quello relativo a uno dei soggetti indicati non identificato (ad esempio, senza indicazione del nome e cognome) ma tuttavia identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Nell’ambito della amplissima categoria dei dati personali (qualunque informazione), vanno distinte alcune informazioni che, per la loro delicatezza, ricevono una particolare tutela: i dati sensibili e quelli giudiziari.

Per **dati sensibili** si intendono i dati personali idonei a rilevare 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.

Per **dati giudiziari** si intendono i dati personali idonei a rilevare i provvedimenti iscritti nel casellario giudiziale, nonché i dati idonei a rivelare la qualità di imputato ed indagato: in altre parole, si tratta dei dati relativi agli eventuali procedimenti penali a carico della persona.

2. Soggetti obbligati e sintesi degli obblighi previsti

Sono tenuti ad osservare le disposizioni sulla privacy tutti coloro che trattano dati personali, vale a dire:

- aziende;
- pubbliche amministrazioni;
- professionisti.

La disciplina di tutela dei dati personali prevede una serie di obblighi. In proposito si possono distinguere:

- 1) l'individuazione dei soggetti che effettuano il trattamento dei dati personali (con la distinzione delle figure del *titolare*, del *responsabile*, del/degli *incaricato/i*);
- 2) le regole generali da osservare per il trattamento dei dati personali, vale a dire gli adempimenti che devono essere osservati in ogni caso nei confronti dei soggetti i cui dati personali vengono trattati:
 - a. modalità del trattamento e requisiti dei dati;
 - b. informativa;
 - c. raccolta del consenso;
- 3) gli adempimenti nei confronti dell'Autorità Garante nel caso di trattamento di dati personali sensibili e giudiziari:
 - a. la notificazione del trattamento dei dati;
 - b. la comunicazione di particolari circostanze all'Autorità Garante;
 - c. la richiesta di autorizzazione;
- 4) le misure di sicurezza da adottare per la tutela dei dati personali raccolti (misure idonee e misure minime).

I professionisti dell'area sanitaria, i Consigli Direttivi degli Ordini Provinciali e la Federazione Nazionale non sono soggetti a nessuno degli adempimenti previsti nei confronti dell'Autorità Garante di cui al precedente punto 3 (notificazioni, comunicazioni e richieste di autorizzazione), semprechè i dati trattati non esulino dalla loro normale attività.

3. Soggetti che effettuano il trattamento dei dati personali

La raccolta e la conservazione dei dati personali (trattamento dei dati) può coinvolgere, oltre al soggetto obbligato per legge, anche altri soggetti che, in ausilio del soggetto obbligato, collaborano agli adempimenti relativi. La legge distingue in proposito le seguenti figure:

Il titolare del trattamento – che è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Nel caso dei professionisti, titolare del trattamento è considerato il libero professionista che esercita la professione individualmente; se l'attività professionale viene esercitata in forma associata, titolare del trattamento risulterà l'associazione nel suo complesso.

Nel caso degli Ordini Professionali e della Federazione Nazionale titolare del trattamento è il Consiglio Direttivo ed il Comitato Centrale stesso.

Accanto alla figura del titolare del trattamento, definita direttamente dalla legge, sono individuabili due altre figure solo eventuali, traendo esse origine da un atto di nomina facoltativo.

Il responsabile del trattamento – che è la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali. La designazione del responsabile è atto discrezionale ma, se compiuto, obbliga al rispetto di precisi criteri nella scelta del soggetto. Il responsabile, infatti, deve essere individuato tra i soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo della sicurezza. I compiti affidati al responsabile devono essere specificati per iscritto dal titolare (art. 29, comma 4, Codice sulla Privacy).

Gli incaricati del trattamento – che sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare e dal responsabile. Si tratta di una figura subordinata rispetto al titolare ed al responsabile, il cui incarico si limita allo svolgimento materiale delle operazioni relative al trattamento dei dati. La designazione degli incaricati deve essere effettuata per iscritto e deve indicare puntualmente l'ambito del trattamento consentito (art. 30, comma 2, Codice sulla Privacy).

I professionisti dell'area sanitaria, i Consigli Direttivi degli Ordini Provinciali e la Federazione Nazionale, se ne sentiranno l'esigenza, potranno procedere alla designazione di uno o più responsabili e incaricati del trattamento. In tal caso dovranno osservare le formalità così come richieste.

4. Regole generali per il trattamento dei dati personali

Tutti i soggetti che trattino dati personali, obbligati pertanto all'osservanza delle disposizioni sulla privacy, devono provvedere in ogni caso:

- a trattare i dati secondo le modalità ed i requisiti richiesti dalla legge;
- a dare una serie di informazioni (*informativa*) ai soggetti i cui dati si vogliono raccogliere;
- ottenere che i medesimi soggetti prestino il consenso alla raccolta dei dati personali.

4.a. Modalità del trattamento e requisiti dei dati

I dati personali oggetto di trattamento devono essere:

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

I dati personali che non vengono trattati in conformità a tale disciplina non possono essere utilizzati.

4.b. Informativa

Prima di poter trattare qualsiasi tipo di dato personale (sia esso solo personale o anche sensibile o giudiziario) è necessario dare talune informazioni (*informativa*) a coloro che forniscono i propri dati.

L'informazione resa deve riguardare le finalità e le modalità del trattamento, la natura obbligatoria o facoltativa del conferimento dei dati, le conseguenze di un eventuale rifiuto di rispondere, i soggetti o le categorie di soggetti cui i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei medesimi, i diritti riconosciuti dalla legge all'interessato (art. 7 del Codice sulla Privacy), nonché gli estremi identificativi del titolare e, se designato, del responsabile. Nell'informativa possono essere omessi quegli elementi che si presumono già noti alla persona che fornisce i dati.

L'omessa informativa è punita con una sanzione amministrativa da 3mila a 18mila € se il trattamento riguarda dati comuni, e da 5mila a 30mila € se il trattamento riguarda dati sensibili.

Tra le novità del Codice sulla Privacy è adesso consentito che l'informativa sia resa per iscritto o anche, in forma orale, ma con evidenti svantaggi sotto il profilo probatorio. Tenuto conto della complessità dell'informazione da dare, motivi di praticità e di cautela inducono a consigliare il rilascio dell'informativa in forma scritta attraverso la predisposizione di un modello (un fac-simile è rinvenibile sul sito del Garante della Privacy: www.garanteprivacy.it) da conservare previa acquisizione della firma dell'interessato.

L'informativa è dunque sempre dovuta ed è un adempimento che fa carico sia ai professionisti dell'area sanitaria, che ai Consigli Direttivi degli Ordini Provinciali.

4.c. Consenso

In aggiunta all'informativa, è necessario che i soggetti i cui dati personali (anche se sensibili e giudiziari) si vogliono raccogliere prestino il proprio consenso alla raccolta dei loro dati personali.

In deroga a tale regola di generale applicazione, l'art. 24 del D. Lgs. 196/2003 prevede alcune ipotesi in cui il trattamento dei dati personali può essere effettuato senza che sia necessario raccogliere il consenso. Tra queste si segnalano quelli attinenti al nostro esame:

- i casi previsti nella II parte del testo Unico che contiene disposizioni relative a specifici settori tra i quali i trattamenti in ambito sanitario
- quando il trattamento dei dati personali sia necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- quando il trattamento sia necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del

contratto, a specifiche richieste dell'interessato (ad esempio, per redigere un preventivo di spesa).

Infine l'art. 26-Garanzie per i dati sensibili, comma 4, lettera d), del Codice sulla Privacy esclude anche per i soggetti privati e per gli enti pubblici economici l'obbligatorietà di acquisire il consenso per il trattamento dei dati sensibili “. . . quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza . . .”.

I trattamenti dei dati personali eseguiti dai professionisti dell'area sanitaria in modo sistematico e dai Consigli Direttivi dei singoli Ordini Professionali per lo svolgimento delle funzioni istituzionali, ai sensi dell'art. 18, comma 4, del Codice sulla Privacy⁴, non necessitano del consenso dell'interessato.

Questa esenzione riguarda tutti i dati attualmente richiesti per l'iscrizione all'Albo. Il trattamento dei dati personali senza il consenso dell'interessato è consentito, sia alla scrivente Federazione che agli Ordini Professionali locali, nei limiti di quanto stabilito dalle leggi istitutive e dai regolamenti attuativi e per il perseguimento delle finalità ivi indicate⁵.

5. Gli adempimenti rispetto all'Autorità garante

A tutela di particolari categorie di dati sensibili o giudiziari, il Garante richiede che il titolare del trattamento segnali particolari circostanze o chieda una previa autorizzazione. Gli adempimenti legati al trattamento dei dati personali riconducibili alle tipologie indicate dall'art. 37, comma 1, del Codice sulla Privacy riguardano:

- la notificazione;
- la comunicazione;
- la richiesta di autorizzazione.

Per lo svolgimento delle attività affidate loro dalla legge istitutiva e dal regolamento di attuazione, i Consigli Direttivi degli Ordini Professionali non effettuano alcuno dei trattamenti di dati previsti del citato articolo, pertanto i Consigli Direttivi non sono tenuti all'effettuazione della notifica al Garante.

Lo stesso vale per i professionisti dell'area sanitaria e, ad integrazione di quanto esposto, si precisa che l'Autorità Garante per la protezione dei dati personali aveva già adottato lo scorso 31 marzo 2004 un provvedimento (n. 1/2004) per individuare i trattamenti di dati personali (raccolta, uso, conservazione etc.) che non dovevano essere oggetto di notificazione al Garante, introducendo una robusta semplificazione in materia e riducendo a pochi casi essenziali l'obbligo di notificare preventivamente all'Autorità l'avvio di un trattamento di dati,

⁴ **Art. 18. Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici.**

1. Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici.
2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

3. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

4. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato.

5. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione.

⁵ Vedi artt. 3 e 7 del D. Lgs. C.P.S. 13 settembre 1946, n. 233 e gli artt. del Capo I del D.P.R. 5 aprile 1950, n.221.

ed è tornata in argomento con comunicato stampa dello scorso 26 aprile espressamente circoscritto all'ambito della sanità.

6. Le misure di sicurezza da adottare per la tutela dei dati personali

Per una corretta applicazione delle novità normative introdotte con il Codice sulla Privacy, le *misure minime*, già precedentemente adottate dalla legge n. 675/1996, sono le disposizioni organizzative e gli accorgimenti tecnici che i responsabili dei trattamenti devono attuare per garantire il minimo di sicurezza previsto dalla legge per la protezione dei dati personali.

La legge distingue in proposito le misure di sicurezza da adottare in due categorie:

- a) le misure di sicurezza *idonee*;
- b) le misure di sicurezza *minime*.

La distinzione ha rilevanza ai fini sanzionatori in quanto la inosservanza delle misure minime comporta una sanzione di natura penale. L'inosservanza delle misure idonee non comporta sanzioni ma espone ad eventuali azioni dei soggetti lesi per il risarcimento dei danni.

6.a. Le misure di sicurezza “idonee”

L'obbligo di adottare misure di sicurezza idonee si sostanzia in un obbligo generico di predisporre qualunque precauzione necessaria alla tutela dei dati per evitare il rischio di distruzione o dispersione anche accidentale degli stessi ovvero di conoscenza da parte di terzi.

L'art. 31 - *Obblighi di sicurezza* - del Codice sulla Privacy infatti prevede che; “ *I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta*”.

L'inadempimento di tale obbligo espone a responsabilità civile per risarcimento danni.

L'adozione delle misure di sicurezza idonee è obbligatoria sia per i professionisti dell'area sanitaria che per gli Ordini Professionali e la Federazione Nazionale.

6.b. Le misure di sicurezza “minime”

Nel quadro generale degli obblighi di sicurezza, la norma individua alcune misure di sicurezza ritenute indispensabili alla tutela dei dati personali: sono le cosiddette misure minime di sicurezza specificate nell'Allegato B) – *Disciplinare tecnico in materia di misure minime di sicurezza* del Codice sulla Privacy (vedi all. A1.).

Le misure minime di sicurezza sono differenziate a seconda delle modalità di trattamento dei dati:

- i. dati trattati senza l'ausilio di strumenti elettronici;
- ii. dati trattati con l'ausilio di strumenti elettronici.

Il mancato adeguamento alle misure minime di sicurezza costituisce reato con la previsione della pena dell'arresto sino a 2 anni o dell'ammenda da 10mila a 50mila €(art. 169 del Codice sulla Privacy).

L'adozione delle misure minime di sicurezza è obbligatoria sia per i professionisti dell'area sanitaria sia per gli ordini Professionali e la Federazione Nazionale.

6.b.i. Dati trattati senza l'ausilio di strumenti informatici

Le misure minime di sicurezza da adottare per il trattamento dei dati personali in modo "cartaceo" senza l'ausilio di strumenti informatici sono tre:

- l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- la previsione di procedure per una idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- la 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.

I primi due punti riguardano il caso in cui si sia provveduto ad individuare uno o più incaricati del trattamento. L'ultima misura minima di sicurezza da adottare riguarda anche coloro che non abbiano designato alcun incaricato ed è posta a tutela dei locali in cui vengono conservati i dati.

6.b.ii. Dati trattati con l'ausilio di strumenti informatici

Il trattamento dati effettuato con strumenti informatici prevede l'adozione di più complesse misure minime di sicurezza. Qui di seguito si riporta l'elenco:

- a) autenticazione informatica⁶;
- b) adozione di procedure di gestione delle credenziali di autenticazione⁷;
- c) utilizzazione di un sistema di autorizzazione;
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- g) tenuta di un aggiornato documento programmatico sulla sicurezza (DPS);
- h) 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.

⁶ L'autenticazione informatica è l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità. In altre parole ci si riferisce alla necessità di doversi dotare di una password per entrare nel database.

⁷ Premesso che le credenziali d'autenticazione sono i dati ed i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica, l'adozione di procedure di gestione delle credenziali di autenticazione sono quelle misure che rendono sicura la password (che deve essere di almeno otto caratteri comprendenti numeri, lettere e simboli, non deve richiamare cose o persone attinenti al possessore del codice, non deve essere conservata per iscritto ma, possibilmente essere memorizzata prendendo precauzioni affinché non venga dimenticata, deve essere cambiata frequentemente).

Si ritiene opportuno suggerire di rivolgersi ai tecnici che forniscono la manutenzione per i propri computer per farsi rilasciare un'attestazione comprovante l'adozione delle misure privacy.

6.b.ii. lettera g) Documento Programmatico sulla Sicurezza (DPS)

Come già detto, nell'ambito delle misure minime di sicurezza da adottare per il trattamento dei dati con l'ausilio di strumenti elettronici, rientra anche la predisposizione del Documento Programmatico sulla Sicurezza (DPS) che dovrà essere redatto entro il **30 giugno 2004**⁸. Dal 2005 dovrà essere redatto o aggiornato entro il 31 marzo di ogni anno.

Il DPS deve riportare le seguenti informazioni:

- l'elenco dei trattamenti personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamento di mansioni, o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento dei dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al Codice sulla Privacy, all'esterno della struttura del titolare;
- per i dati personali idonei a rilevare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione dagli altri dati personali dell'interessato.

Ricordiamo che, con parere del 22 marzo scorso il Garante ha provveduto a delimitare l'ambito di applicazione dell'obbligo di redazione del DPS, stabilendo che sono tenuti all'adempimento coloro che *“trattano dati sensibili e/o giudiziari con l'ausilio di strumenti elettronici”*.

Poiché i professionisti dell'area sanitaria ed i Consigli Direttivi degli Ordini Professionali, non trattando dati sensibili e giudiziari⁹, non devono predisporre il Documento Programmatico sulla Sicurezza.

⁸ Nei prossimi giorni sarà esaminato un decreto legge per prorogare gli adempimenti previsti dal testo unico sulla privacy. La proroga principale potrebbe riguardare proprio gli adempimenti in scadenza per il prossimo 30 giugno.

⁹ Gli unici dati giudiziari di cui gli Ordini sono custodi sono rinvenibili nei certificati attestanti il pieno godimento dei diritti civili ed il certificato generale del casellario giudiziale necessari all'iscrizione i quali, però, sono trattati con modalità esclusivamente cartacea.

7. Considerazioni finali sugli Ordini Professionali

È noto come gli Ordini Professionali siano *enti pubblici non economici*. All'attività svolta dai Consigli Direttivi di ciascun Ordine sono quindi applicabili le disposizioni sancite al Titolo III, Capo II, del Codice sulla Privacy (artt. dal 18 al 22).

Proprio recentemente il Garante ha affermato che il Codice sulla Privacy non ha modificato la disciplina legislativa relativa agli Albi professionali, che per loro stessa natura sono destinati ad un regime di pubblicità, anche in funzione della tutela dei diritti di coloro che a vario titolo hanno rapporti con gli iscritti all'Albo. Le norme che regolano i vari albi permettono ai diversi Ordini Professionali, secondo le diverse modalità previste nei singoli casi, di comunicare e diffondere a soggetti pubblici e privati i dati personali contenuti nei rispettivi Albi, compresi quelli contenuti nei provvedimenti di sospensione o interruzione dell'esercizio della professione.

Da parte di alcuni si sono manifestate perplessità in ordine alla possibilità di pubblicare, su internet o su altri media, i dati personali degli iscritti raccolti ai fini della redazione e tenuta degli Albi professionali. Sul punto interviene una specifica disposizione del Codice sulla Privacy che all'art. 61-*Utilizzazione di dati pubblici*, comma 2, dispone: “... *i dati personali diversi da quelli sensibili o giudiziari, che devono essere inseriti in un albo professionale in conformità alla legge o ad un regolamento, possono essere comunicati a soggetti pubblici e privati o diffusi, ai sensi dell'articolo 19, commi 2 e 3, anche mediante reti di comunicazione elettronica.*”

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 e' 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 e' 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 e' prevista dal sistema di autenticazione, e' 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 e' 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 e' 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 e' 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 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 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 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 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.

Allegato B

(Fac Simile pei i medici veterinari)

Informativa ex art. 13 D.lgs. 196/2003
(Da inserire in fondo al modello di raccolta dati)

Gentile Signore/a,

Desideriamo informarLa che il D.lgs. n. 196 del 30 giugno 2003 ("Codice in materia di protezione dei dati personali") prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Secondo la normativa indicata, tale trattamento sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti.

Ai sensi dell'articolo 13 del D.lgs. n.196/2003, pertanto, Le forniamo le seguenti informazioni:

1. I dati da Lei forniti verranno trattati per le finalità strettamente relative all'espletamento della professione (ad es. fatturazione, convocazione).
2. Il trattamento sarà effettuato con le seguenti modalità:
(Indicare le modalità del trattamento: manuale / informatizzato / altro.)
3. Il conferimento dei dati è obbligatorio per le finalità strettamente relative all'espletamento della professione e l'eventuale rifiuto di fornire tali dati potrebbe comportare la mancata o parziale esecuzione del contratto.
4. I dati non saranno comunicati ad altri soggetti, né saranno oggetto di diffusione.
5. Il titolare del trattamento è:
(Indicare la denominazione o la ragione sociale e il domicilio, la residenza o la sede del titolare)
6. In ogni momento potrà esercitare i Suoi diritti nei confronti del titolare del trattamento, ai sensi dell'art.7 del D.lgs.196/2003, che per Sua comodità riproduciamo integralmente:

Decreto Legislativo n.196/2003,
Art. 7 - Diritto di accesso ai dati personali ed altri diritti

1. 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.
2. 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.
3. 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.
4. 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.

Letto e sottoscritto

Allegato C

(Fac Simile per i Consigli Direttivi degli Ordini Provinciali)

Informativa ex art. 13 D.lgs. 196/2003
(Da inserire in fondo al modello di raccolta dati)

Gentile Dottore/a,

Desideriamo informarLa che il D.lgs. n. 196 del 30 giugno 2003 ("Codice in materia di protezione dei dati personali") prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Secondo la normativa indicata, tale trattamento sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti.

Ai sensi dell'articolo 13 del D.lgs. n.196/2003, pertanto, Le forniamo le seguenti informazioni:

1. I dati da Lei forniti verranno trattati per la tenuta dell'Albo professionale nei limiti di quanto stabilito dalle leggi istitutive e dai regolamenti attuativi in vigore e per il perseguimento delle finalità ivi indicate.
2. Il trattamento sarà effettuato con le seguenti modalità:

(Indicare le modalità del trattamento: manuale / informatizzato / altro.)

3. Il conferimento dei dati è obbligatorio per la tenuta dell'Albo e l'eventuale rifiuto di fornire tali dati potrebbe comportare la mancata esecuzione dalle leggi istitutive e dai regolamenti attuativi in vigore.
4. I dati saranno comunicati ai soggetti indicati dalle leggi istitutive e dai regolamenti attuativi in vigore, e saranno soggetti a comunicazione e diffusione nei limiti di quanto stabilito per il perseguimento delle finalità indicate dalle leggi istitutive e dai regolamenti attuativi in vigore
5. Il titolare del trattamento è il Consiglio Direttivo dell'Ordine Provinciale dei Medici Veterinari di
6. In ogni momento potrà esercitare i Suoi diritti nei confronti del titolare del trattamento, ai sensi dell'art.7 del D.lgs.196/2003, che per Sua comodità riproduciamo integralmente:

Decreto Legislativo n.196/2003.

Art. 7 - Diritto di accesso ai dati personali ed altri diritti

1. 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.
2. 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.
3. 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.
4. 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.

Letto e sottoscritto
