Privacy per CTU e periti: le misure di sicurezza da adottare

Con la delib. n. 46 del 26 giugno 2008, il Garante per la protezione dei dati personali ha emesso le "Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero". *Consulente immobiliare*, attesi i riflessi che le diposizioni contenute nella deliberazione comportano ai numerosi professionisti impegnati negli incarichi giudiziari e di parte, ha inteso approfondire il tema con la pubblicazione di due focus. Nel primo (pubblicato nel *CI* n. 823 a pag. 1796) sono state analizzate, dopo un esame generale del provvedimento, le esclusioni nell'applicazione del Codice della privacy per consulenti tecnici e periti unitamente alla definizione di dato personale con l'esame degli obblighi relativi agli incarichi giudiziari per quanto attiene il rispetto dei principi di liceità e che riguardano la qualità dei dati di cui all'art. 11. Nel presente focus, invece, la trattazione ha specifico riguardo al complesso quadro delle misure di sicurezza idonee a preservare i dati da alcuni eventi, tra i quali accessi e utilizzazioni indebite di cui agli artt. 31 e segg. e disciplinare tecnico allegato B al Codice (a pag. 1908).

Il secondo aspetto richiamato dal punto 2.1. delle Linee guida di cui alla delib. n. 46/2008 del Garante della privacy precisa che il trattamento dei dati da parte degli esperti giudiziari si svolga «..adottando le misure di sicurezza idonee a preservare i dati da alcuni eventi, tra i quali accessi e utilizzazioni indebite di cui agli artt. 31 e segg. e disciplinare tecnico allegato B al Codice». Tenuto conto che l'attività dell'ausiliario giudiziario è connotata da caratteri di autonomia, in relazione alla natura squisitamente tecnica delle indagini che si svolgono, solitamente, senza l'intervento del magistrato, dal momento in cui l'esperto riceve l'incarico e sino al momento della consegna al giudice della relazione peritale o al pubblico ministero delle risultanze dell'attività svolta, incombono concretamente su detto soggetto, riguardo ai dati personali acquisiti all'atto dell'incarico e alle ulteriori informazioni raccolte nel corso delle operazioni, le responsabilità e gli obblighi relativi al profilo della sicurezza prescritti dal Codice in materia dei dati personali (D.Lgs. 196, 30 giugno 2003). I consulenti tecnici e periti sono, quindi, tenuti a impiegare tutti gli accorgimenti idonei a evitare un'indebita divulgazione delle informazioni e, al contempo, la loro perdita o distruzione, adottando, a tal fine, le misure atte a garantire la sicurezza dei dati e dei sistemi eventualmente utilizzati.
Prima di scendere nel dettaglio, è utile ricordare le definizioni contenute all'art. 4 del Codice relative ai soggetti coinvolti nel processo:

f) **"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;
g) **"responsabile",** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro en-

te, associazione od organismo preposti dal titolare al trattamento di dati personali;
h) **"incaricati",** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
i) **"interessato",** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

Il titolare del trattamento è la figura che gestisce il sistema di trattamento dei dati assumendo tutte le principali decisioni e incaricandosi delle principali responsabilità. L'art. 28 del Codice stabilisce che quando il trattamento è effettuato da persona giuridica, il titolare del trattamento è l'entità nel suo complesso. Naturalmente, in questo caso, il titolare dovrà operare a mezzo di persone fisiche.
Il responsabile del trattamento, anche se a una prima lettura non se ne apprezza la differenza con il titolare, differisce da quest'ultimo per il fatto che necessita di una specifica nomina, condizione che per il titolare non sussiste. La sua nomina è facoltativa ed è decisa per l'appunto dal titolare che, nella volontà del legislatore, è identificato con un superiore in ordine gerarchico. La figura del responsabile deve rispondere a requisiti di capacità e affidabilità e i suoi compiti sono affidati per iscritto dal titolare.
Gli incaricati del trattamento sono coloro che svolgono le operazioni di trattamento dei dati personali sotto la direzione e autorità del titolare o responsabile. In pratica, gli incaricati sono coloro che svolgono materialmente le operazioni connesse alla trattazione dei dati, alla loro raccolta e conservazione. I compiti degli incaricati, così come la loro designazione, sono indicati per iscritto dal titolare.
Le Linee guida stabiliscono che gli ausiliari debbono curare personalmente, in considerazione del grado di autonomia riconosciuto per legge o con l'incarico ricevuto:
– le «misure idonee e preventive» cui fa riferimento l'art. 31 del Codice;
– le «misure minime» specificamente indicate negli articoli da 33 a 35 e nel disciplinare tecnico allegato B) al Codice.

La mancata adozione di quanto stabilito costituisce fattispecie penalmente sanzionata (art. 169 del Codice).

Misure di sicurezza idonee e preventive

Il primo punto concerne gli obblighi di sicurezza.
L'articolo dispone che tutti i dati personali oggetto di trattamento debbono essere 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.
La disposizione riguarda, perciò, sia la documentazione conservata in forma cartacea (moduli, fascicoli, schede, fotografie ecc.) sia quella su supporto informatico ed elettronico (tutti i sistemi hardware, la macchina fotografica digitale, il telefono cellulare dotato di fotocamera ecc.).
La disposizione incombe su tutti i soggetti coinvolti nel processo (titolare, responsabile, incaricato) e dispone che tutti debbano operare al fine di evitare:
– la distruzione/perdita dei dati;
– l'accesso non autorizzato;
– il trattamento non consentito.

Art. 31 – Obblighi di sicurezza
1. 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.
Art. 33 – Misure minime
1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34 – Trattamenti con strumenti elettronici
1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
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;
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.
Art. 35 – Trattamenti senza l'ausilio di strumenti elettronici
1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) 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.

Le misure minime da adottare

Sul secondo punto le Linee guida prevedono che siano adottate le cosiddette «misure minime».
Le misure minime – definite dall'art. 33 del Codice – sono da considerare l'insieme delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che costituiscono il livello standard di protezione richiesto in relazione ai rischi previsti dal punto precedente (art. 31).
Le misure minime sono volte ad assicurare il livello minimo di protezione dei dati personali.
Gli adempimenti relativi alle misure minime di sicurezza riguardano:
- adozione delle misure minime (entro il 31 marzo 2006) e redazione e aggiornamento del DPS (Documento programmatico della sicurezza) entro il 31 marzo di ogni anno;
- individuazione dell'ambito del trattamento consentito agli incaricati e agli addetti alla manutenzione o gestione degli strumenti elettronici (con verifica delle condizioni almeno annuale);
- aggiornamento (almeno annuale) dei software utilizzati; in caso di dati sensibili e giudiziari l'aggiornamento deve avvenire semestralmente;
- aggiornamento (almeno semestrale) dei software antivirus;
- disporre procedure per l'effettuazione di salvataggio dati e aggiornamento password (semestrale per i dati comuni e trimestrale per quelli sensibili e giudiziari);

Trattamento dei dati con strumenti elettronici

L'art. 34 stabilisce – unitamente al dettaglio contenuto nel disciplinare tecnico di cui all'allegato B) – i trattamenti operati con strumenti elettronici. Le misure minime da adottare in questo caso obbligatoriamente sono:
a. autenticazione informatica;
b. adozione di procedure di gestione delle credenziali di autenticazione;
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;
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.

Trattamento dei dati senza strumenti lettronici

L'art. 35 invece riguarda il trattamento dei dati non operato con strumenti elettronici. Questo è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b. previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c. 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.
In riferimento a quanto stabilisce l'allegato B del Codice – per la cui lettura integrale si rimanda a pag. 1908 – può essere utile riportare, in un quadro sintetico organizzato, le incombenze in ordine agli obblighi minimi da assumere da parte dei consulenti tecnici e periti.
Per ciò che attiene il sistema di autenticazione informatica:
– attribuire un codice di identificazione all'incaricato con, associata, una parola chiave o password per l'accesso al sistema informatico;
– la password deve essere almeno di otto caratteri o, dove il sistema non lo permetta, con il numero massimo consentito dallo stesso. La parola chiave o password deve essere scelta evitando riferimenti riconducibili al soggetto incaricato (data di nascita, di matrimonio ecc.) e comunque facilmente individuabili;
– la parola chiave o password deve essere cambiata al primo utilizzo dall'incaricato e almeno ogni sei mesi;
– se vengono trattati dati sensibili e giudiziari, la parola chiave o password deve essere modificata almeno ogni tre mesi.
Per quanto riguarda le altre misure di sicurezza:
– i dati debbono essere protetti contro il rischio di intrusione o manomissione fraudolenta con software specifici da aggiornare con cadenza almeno semestrale;
– i programmi in uso per gli elaboratori atti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti (es. aggiornamenti dei sistemi operativi) debbono essere fatti almeno annualmente;
– in presenza di trattamento di dati sensibili o giudiziari il suddetto aggiornamento deve essere almeno semestrale;
– il salvataggio dei dati (il c.d. back-up) deve essere svolto con frequenza settimanale;
– il supporto in cui sono salvati i dati (back-up) non deve essere conservato all'interno dei locali oggetto dell'attività professionale.
In ordine alle ulteriori misure in caso di trattamento di dati sensibili o giudiziari:
– i dati sensibili o giudiziari sono protetti contro l'accesso abusivo, mediante l'utilizzo di idonei strumenti;
– i supporti rimovibili debbono essere adeguatamente custoditi al fine di evitare accessi non autorizzati;
– i supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili; possono essere riutilizzati da altri incaricati non autorizzati al trattamento degli stessi dati, solo nel caso di malfunzionamento (per esempio, intervento di riparazione);
– sono adottate misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi in tempi non superiori a sette giorni.
Per quanto attiene il trattamento senza l'ausilio di strumenti elettronici:
– i documenti debbono essere adeguatamente custoditi, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali;
– i documenti contenenti dati personali affidati agli incaricati del trattamento debbono essere custoditi fino alla restituzione al termine delle operazioni affidate in modo che a essi non accedano persone prive di autorizzazione;
– l'accesso agli archivi contenenti è con-

trollato. 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;
- i fascicoli contenenti dati personali non possono essere conservati in luogo aperto al pubblico e comunque di libero accesso e non possono riportare sul frontespizio nomi e cognomi o comunque dati da cui risalire alle generalità dei soggetti.

Per quanto attiene il documento programmatico sulla sicurezza, deve essere effettuato (dal 31 marzo 2006, ultima proroga dell'entrata in vigore della normativa) entro il 31 marzo di ogni anno con la compilazione delle necessarie e idonee informazioni.
Anche nell'ipotesi che il consulente e il perito si avvalgano dell'opera di collaboratori, anche se addetti a compiti di amministrazione (art. 30 del Codice), vige l'obbligo di preporre alla custodia e al trattamento dei dati personali raccolti nel corso dell'accertamento solo il personale specificamente incaricato per iscritto.

Art. 30 – Incaricati del trattamento
1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica a una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

L'attività di tali incaricati deve essere oggetto di precise istruzioni oltre che sulle modalità e sull'ambito del trattamento consentito, anche in ordine alla scrupolosa osservanza della riservatezza relativamente ai dati di cui vengono a conoscenza. In ordine all'organizzazione dello studio, oltre a quanto proposto in lettura semplificata dell'allegato B) al Codice e ricondotta nella sintesi, per agevolare l'attività del titolare può essere utile proporre un quadro sinottico sugli aspetti principali anche mediante alcuni pratici suggerimenti operativi scaturiti dall'esperienza pratica (*tabella 1*).
Gli obblighi di cui alle Linee guida incombono anche sui **consulenti di parte** in ordine all'applicazione dei principi di liceità e che riguardano la qualità dei dati (art. 11 del Codice) e le disposizioni in materia di misure di sicurezza volte alla protezione dei dati stessi (artt. 31 e segg. e disciplinare tecnico allegato B) al Codice).

Le previsioni per il consulente tecnico di parte

Il Garante, nella delib. n. 46/2008, ha provveduto a stabilire regole anche per il consulente tecnico nominato dalle parti nei giudizi civili e penali.
La deliberazione riguarda – come già osservato nel contributo pubblicato nel precedente fascicolo – il consulente tecnico nominato dalla parte nel procedimento civile (artt. 87, 194, 195 e 201 cod. proc. civ.) e in quello penale (artt. 225 e segg., 233 e 360 cod. proc. pen.).
In particolare, il consulente di parte:
- può trattare lecitamente i dati personali nei limiti in cui ciò è necessario per il corretto adempimento dell'incarico ricevuto dalla parte o dal suo difensore ai fini dello svolgimento delle indagini difensive di cui alla legge 397/2000 o, comunque, per far valere o difendere un diritto in sede giudiziaria (art. 11, comma 1, lett. *a)* e *b)*. I dati sensibili o giudiziari possono essere utilizzati solo se ciò è indispensabile e nella portata limitatamente a ciò che è necessario nelle diverse fattispecie;
- può acquisire e utilizzare solo i dati personali comunque pertinenti e non eccedenti rispetto alle finalità perseguite con l'incarico ricevuto, avvalendosi di informazioni personali e di modalità di trattamento proporzionate allo scopo perseguito (art. 11, comma 1, lett. *d)*; sono fatti salvi i divieti di legge posti a tutela della segretezza e riservatezza delle informazioni acquisite nel corso di un procedimento giudiziario (cfr., per esempio, l'art. 379-*bis* cod. proc. pen.) e i limiti e i doveri derivanti dal segreto professionale e dal fedele espletamento dell'incarico ricevuto (cfr. artt. 380 e 381 cod. pen.);
- può comunicare a terzi dati personali so-

TABELLA 1

Organizzazione dello studio

Organizzazione fisica dello studio	
Locali e modalità di conservazione dei documenti	Disporre di locale separato da quelli di trattazione dei dati per conservazione copie di back-up.
	Il locale dove è alloggiato il server (se in dotazione) deve essere dotato di serratura con accesso controllato.
	I locali dello studio debbono disporre di sistemi antintrusione.
	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.
	Gli apparati telefax in dotazione allo studio debbono essere ubicati in zona non liberamente accessibile al pubblico e comunque disposti in aree ove i documenti ricevuti possano essere non consultati da persone non autorizzate.
	I documenti contenenti dati personali debbono essere custoditi in armadi con chiusura a chiave.
	L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.
	Anche durante le fasi di lavorazione da parte degli incaricati i fascicoli non possono essere lasciati incustoditi in luogo aperto al pubblico.
	I fascicoli contenenti dati personali non possono riportare sul frontespizio nomi e cognomi o comunque dati e riferimenti da cui risalire alle generalità dei soggetti.
Organizzazione informatica dello studio	
Server	Impostare il sistema operativo con screensaver protetto da password.
	Il server deve essere dotato di software firewall (sistema di protezione da accessi non autorizzati per la rete connessa a internet) e software antivirus costantemente aggiornati.
PC desktop e notebook	I PC desktop debbono essere conservati in luoghi muniti di chiusure con serratura.
	I notebook debbono essere dotati di sistema di bloccaggio.
	I PC desktop e notebook debbono essere dotati di sistemi firewall e antivirus costantemente aggiornati.
Back-up	Il salvataggio dei dati (il c.d. back-up) deve essere svolto con frequenza settimanale.
	Il supporto in cui sono salvati i dati (back-up) non deve essere conservato all'interno dei locali oggetto dell'attività professionale.
Password	La password da attribuire a ogni incaricato deve essere associata a un codice di identificazione.
	La password deve essere almeno di otto caratteri e deve essere scelta evitando riferimenti riconducibili al soggetto incaricato.
	La parola chiave o password deve essere cambiata dall'incaricato almeno ogni sei mesi.
	Se vengono trattati dati sensibili e giudiziari, la parola chiave o password deve essere modificata almeno ogni tre mesi.
Amministrazione	La password di accesso per l'amministratore di rete deve essere sostituita almeno ogni trenta giorni.

lo ove ciò risulti necessario per finalità di tutela dell'assistito, limitatamente ai dati strettamente funzionali all'esercizio del diritto di difesa della parte e nel rispetto dei diritti e della dignità dell'interessato e di terzi;

– il consulente di parte, relativamente ai dati personali acquisiti e trattati nell'e-

spletamento dell'incarico ricevuto da una parte, assume personalmente le responsabilità e gli obblighi relativi al profilo della sicurezza prescritti dal Codice, relativamente sia alle «misure idonee e preventive» (art. 31) sia alle «misure minime» (artt. da 33 a 35 e disciplinare tecnico allegato B); art. 169 del Codice);
- ove l'incarico comporti il trattamento con strumenti elettronici di dati sensibili o giudiziari, è tenuto a redigere il documento programmatico sulla sicurezza (art. 33, comma 1, lett. *g)* e punto 19, del disciplinare tecnico allegato B);
- anche il consulente di parte deve incaricare per iscritto gli eventuali collaboratori, anche se adibiti a mansioni di carattere amministrativo, che siano addetti alla custodia e al trattamento, in qualsiasi forma, dei dati personali (art. 30 del Codice), impartendo loro precise istruzioni sulle modalità e l'ambito del trattamento loro consentito e sulla scrupolosa osservanza della riservatezza dei dati di cui vengono a conoscenza.

In ultimo occorre ricordare che al consulente tecnico di parte, alla stregua degli altri liberi professionisti, è consentita l'omissione della richiesta dell'autorizzazione al Garante per il trattamento dei dati sensibili; ciò in forza della originaria autorizzazione n. 4/2005 emanata dal Garante per l'autorizzazione al trattamento di dati sensibili da parte dei liberi professionisti e rinnovata con autorizzazione n. 4 del 19 giugno 2008 (a pag. 1906). Ciò non esime il professionista – come invece accade per il consulente tecnico e perito del giudice e pubblico ministero – dagli obblighi della informativa all'interessato con l'ottenimento del relativo consenso.

Le sanzioni

Per quanto attiene all'impianto sanzionatorio, il D.Lgs.196/2003, in linea generale, punisce con sanzioni penali e pecuniarie l'uso dei dati senza consenso degli interessati, il mancato adempimento di uno dei provvedimenti del Garante, la mancata informativa agli interessati e comunque ogni altra carenza concernente l'adozione delle misure minime di sicurezza atte a preservare e garantire il trattamento e la conservazione dei dati personali.

Art. 167 – Trattamento illecito di dati
1. 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.
2. 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.

Art. 168 – Falsità nelle dichiarazioni e notificazioni al Garante
1. Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

Art. 169 – Misure di sicurezza
1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.
2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

Art. 170 – Inosservanza di provvedimenti del Garante
1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli artt. 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lett. c), è punito con la reclusione da tre mesi a due anni.

Le sanzioni penali previste dal Codice riguardano:
– trattamento illecito di dati personali (art.167 del Codice);
– falsità delle notificazioni al Garante (art.168 del Codice);
– omessa adozione delle misure minime di sicurezza (art.169 del Codice);
– inosservanza di provvedimenti del Garante (art.170 del Codice);

Per la prima e la seconda violazione la pena varia da sei mesi a tre anni di reclusione, per la terza è prevista la reclusione fino a 2 anni o ammenda da 10 mila euro a 50 mila euro mentre l'ultima è sanzionata con la reclusione da 3 mesi sino a 2 anni,
In ordine alla terza violazione occorre precisare che l'art. 169 del Codice prevede la possibilità di impartire all'autore del reato una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità e comunque non superiore a 6 mesi. Nei 60 giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione con la conseguente estinzione del reato.
Per quanto concerne le sanzioni amministrative disposte dal Codice, esse riguardano:
– l'omessa o inidonea informativa all'interessato (art.161 del Codice);
– la cessione di dati in violazione alle disposizioni del Codice e la violazione in materia di divulgazione di dati personali idonei a rivelare lo stato di salute (art. 162);
– l'omessa o incompleta notificazione al Garante (art. 163);
– l'omessa informazione o esibizione di documenti al Garante (art. 164);

La prima violazione è sanzionata con una ammenda da 3 mila euro a 18 mila euro. Se trattasi di dati sensibili e giudiziari, l'ammenda applicata varia da un minimo di 5 mila euro a un massimo di 30 mila euro. Occorre considerare che la somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.
Per quanto attiene la seconda fattispecie di violazioni, essa è punita con una ammenda da 5 mila euro a 30 mila euro, mentre la violazione dell'art. 84, comma 1 (divulgazione di dati personali idonei a rivelare lo stato di salute) è sanzionata con ammenda da 500 euro a 3 mila euro.
Per quanto attiene la omessa o incompleta notificazione al Garante, la sanzione prevista varia da 10 mila a 60 mila euro e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica. Per l'ultima violazione, la somma della sanzione è prevista da 4 mila euro a 24 mila euro.
Per quanto attiene alla specie in trattazione degli incarichi di consulente tecnico e perito, occorre osservare che è esclusa, in ordine al profilo penale, la sanzione relativa alla falsità delle notificazioni al Garante (art.168 del Codice), non dovendo, come detto, l'esperto giudiziario provvedere ad alcuna notificazione, mentre, per il profilo amministrativo, non è prevista, per i motivi gia detti, l'omessa o inidonea informativa all'interessato (art. 161 del Codice) e l'omessa o incompleta notificazione al Garante.
Sono validi, quindi, anche per l'ausiliario giudiziario, seppur nelle ipotesi rese diverse dalle possibili fattispecie, le altre sanzioni e pene.
Vi è da considerare che le violazioni della normativa del Codice sono anche fonte di responsabilità civile per danni ai soggetti interessati, poiché l'art. 2050 cod. civ. configura una responsabilità oggettiva a carico del soggetto che ha cagionato nocumento, indipendentemente dall'attribuzione di dolo o colpa per il fatto, sempreché il contravventore non riesca a dimostrare di aver adottato tutte le misure idonee a evitare il danno.
In ultimo, è utile osservare che responsabile degli accertamenti è la Guardia di fi-

nanza con la quale il Garante per la protezione dei dati personali ha sottoscritto un protocollo d'intesa. Gli accertamenti ispettivi sono indirizzati a verificare il rispetto delle norme da parte dei soggetti che trattano dati personali e per accertarne l'adempimento di tutti gli obblighi connessi all'attività esercitata. Le ispezioni sono svolte direttamente presso le sedi dove si svolgono i trattamenti dei dati personali.

La formazione

Il punto 19.6 dell'Allegato B)[1] stabilisce la necessità di organizzare eventi formativi per gli incaricati al trattamento dei dati.
I programmi formativi debbono riguardare i rischi che incombono sui dati, le misure disponibili per prevenire eventi dannosi, i profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, le responsabilità che ne derivano e le modalità per aggiornarsi sulle misure minime adottate dal titolare.

Art. 161 – Omessa o inidonea informativa all'interessato
1. La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.
Art. 162 – Altre fattispecie
1. La cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b), o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da cinquemila euro a trentamila euro.
2. La violazione della disposizione di cui all'articolo 84, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da cinquecento euro a tremila euro.
Art. 163 – Omessa o incompleta notificazione
1. Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.
Art. 164 – Omessa informazione o esibizione al Garante
1. Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 150, comma 2, e 157 è punito con la sanzione amministrativa del pagamento di una somma da quattromila euro a ventiquattromila euro.

Le attività sono di carattere formativo quando riguardano:
- utilizzo dei sistemi di protezione dei dati sia nella forma cartacea che in quella elettronica;
- indicazioni di condotte preventive per promuovere la cultura della tutela dei dati e della persona;
- conoscenza delle normative, deliberazioni, autorizzazioni del Garante in materia di protezione dei dati personali.

[1] **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. 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.

Gli eventi formativi sono da programmare 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.
Anche per i soggetti titolari e responsabili del trattamento dei dati è prevista attività di carattere formativo. La formazione è orientata principalmente sui seguenti aspetti:
- conoscenza delle normative, deliberazioni, autorizzazioni, sanzioni del Garante in materia di protezione dei dati personali;
- adozione delle misure di sicurezza e misure minime di sicurezza (fisiche e organizzative) e di tutti i precetti necessari e indispensabili dettati dalla norma e deliberazioni;
- formazione specifica in relazione alle deliberazioni e autorizzazioni del Garante;
- analisi dei rischi connessi alla trattazione dei dati e delle principali politiche della sicurezza.

Pertanto risulta indispensabile al fine di adeguare l'operato dei diversi soggetti coinvolti nello studio e realizzare i risultati di conduzione delle attività di trattazione e conservazione dei dati personali in conformità alla norma, prevedere periodicamente la partecipazione del titolare e degli altri soggetti a corsi di formazione e seminari sulla materia.

Considerazioni conclusive

La deliberazione n. 46/2008 riguarda un insieme di obblighi e precetti che i soggetti debbono adeguatamente considerare assumendo le azioni relative.
Ciò innanzitutto per adeguare il loro modo di operare alla normativa senza trascurare anche i dettagli che a una sommaria lettura possono sembrare meno rilevanti. Nell'analisi proposta ne abbiamo sottolineato diversi, individuandone la loro ricaduta, portata e delicatezza nell'ambito delle attività dell'esperto giudiziario.

Ma, mi si consenta, su ogni altra considerazione quella sulla quale ogni ausiliario giudiziario deve prestare particolare attenzione e allo stato forse è da segnalare come la più rischiosa, è la fattispecie di pericoli implicitamente connessi all'ambito nel quale egli svolge il proprio mandato.
Difatti, in particolare nel settore civile, dove attualmente la conflittualità latente ed emergente tra le parti, anche aggravata dall'empasse in cui versa il sistema giurisdizionale civile, conduce frequentemente le parti a produrre estremizzazioni della lite coinvolgendo anche i soggetti che, loro malgrado, si trovano a operare nella procedura, determina condizioni di possibile minaccia per l'ausiliario giudiziario.
E il consulente tecnico di ufficio, esperto nella materia oggetto della controversia che, quando questa si risolve in questione di natura tecnica, "decide" l'esito della causa, è colui che più si espone agli occhi della parte che ritiene di essere stata ingiustamente penalizzata o che magari, illusa da aspettative infondate, non vede realizzare la sua "ragione" nel giudizio. Ecco che quindi può scattare nella parte il desiderio – poco ragionevole per la verità, ma non per questo meno probabile – di una sorta di ritorsione, di una volontà di rivalsa nei confronti di quel consulente che magari, attento a svolgere propriamente e correttamente il suo incarico giudiziario, non sia stato altrettanto diligente nell'applicazione delle disposizioni contenute nella deliberazione.
Chi conosce la situazione di estrema conflittualità in cui si sviluppano molte liti negli odierni procedimenti civili non potrà, quindi, che prestare la massima attenzione alla corretta applicazione delle disposizioni contenute nelle Linee guida e, per quanto riguarda gli ordini e collegi professionali, rendersi attivo nell'offrire agli iscritti occasioni di studio per approfondirne adeguatamente i contenuti e le relative responsabilità e accrescere in ognuno la indispensabile consapevolezza.

Professioni

LEGISLAZIONE

Autorizzazione n. 4/2008 al trattamento dei dati sensibili da parte dei liberi professionisti

Garante per la protezione dei dati personali 19.6.2008

s.o. 175, *G.U.* 169, 21.7.2008

Il Garante per la protezione dei dati personali

Autorizza

i liberi professionisti iscritti in albi o elenchi professionali a trattare i dati sensibili di cui all'art. 4, comma 1, lett. d), del Codice, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo 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, in conformità all'art. 3 del Codice.

1. Ambito di applicazione

L'autorizzazione è rilasciata, anche senza richiesta, ai liberi professionisti tenuti ad iscriversi in albi o elenchi per l'esercizio di un'attività professionale in forma individuale o associata, anche in conformità al D.Lgs. 96/2001, o alle norme di attuazione dell'art. 24, comma 2, della legge 266/1997, in tema di attività di assistenza e consulenza. Sono equiparati ai liberi professionisti i soggetti iscritti nei corrispondenti albi o elenchi speciali istituiti anche ai sensi dell'art. 34 del R.D.L. 27 novembre 1933, n. 1578 e succ. mod. e integrazioni, recante l'ordinamento della professione di avvocato.

L'autorizzazione è rilasciata anche ai sostituti e agli ausiliari che collaborano con il libero professionista ai sensi dell'art. 2232 del cod. civ., ai praticanti e ai tirocinanti presso il libero professionista, qualora tali soggetti siano titolari di un autonomo trattamento o siano contitolari del trattamento effettuato dal libero professionista.

Il presente provvedimento non si applica al trattamento dei dati sensibili effettuato:

a) dagli esercenti la professione sanitaria e dagli psicologi, dal personale sanitario infermieristico, tecnico e della riabilitazione, ai quali si riferisce l'autorizzazione generale n. 2/2008;

b) per la gestione delle prestazioni di lavoro o di collaborazione di cui si avvale il libero professionista o taluno dei soggetti sopra indicati, alla quale si riferisce l'autorizzazione generale n. 1/2008;

c) da soggetti privati che svolgono attività investigative, dai giornalisti, dai pubblicisti e dai praticanti giornalisti di cui agli articoli 26 e 33 della legge 3 febbraio 1963, n. 69.

2. Interessati ai quali i dati si riferiscono e categorie di dati

Il trattamento può riguardare i dati sensibili relativi ai clienti.

I dati sensibili relativi ai terzi possono essere trattati ove ciò sia strettamente indispensabile per l'esecuzione di specifiche prestazioni professionali richieste dai clienti per scopi determinati e legittimi.

In ogni caso, i dati devono essere strettamente pertinenti e non eccedenti rispetto ad incarichi conferiti che non possano essere svolti mediante il trattamento di dati anonimi o di dati personali di natura diversa.

Il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale deve essere effettuato anche nel rispetto della citata autorizzazione generale n. 2/2008.

3. Finalità del trattamento

Il trattamento dei dati sensibili può essere effettuato ai soli fini dell'espletamento di un incarico che rientri tra quelli che il libero professionista può eseguire in base al proprio ordinamento professionale, e in particolare:

a) per curare gli adempimenti in materia di lavoro, di previdenza ed assistenza sociale e fiscale nell'interesse di altri soggetti che sono parte di un rapporto di lavoro dipendente o autonomo, ai sensi della legge 11 gennaio 1979, n. 12, che disciplina la professione di consulente del lavoro;

b) ai fini dello svolgimento da parte del difensore delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, anche a mezzo di sostituti e di consulenti tecnici, o, comunque, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi. Qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

c) per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto stabilito dalle leggi e dai regolamenti in materia, salvo quanto previsto dall'art. 60 del Codice in relazione ai dati sullo stato di salute e sulla vita sessuale.

4. Modalità di trattamento

Il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e mediante forme di orga-

nizzazione dei dati strettamente indispensabili in rapporto all'incarico conferito dal cliente.

Restano fermi gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice.

Restano inoltre fermi gli obblighi di informare l'interessato ai sensi dell'art. 13, commi 1, 4 e 5, del Codice, anche quando i dati sono raccolti presso terzi, e di acquisire, ove necessario, il consenso scritto.

Se i dati sono raccolti per l'esercizio di un diritto in sede giudiziaria o per le indagini difensive (punto 3), lettera b)), l'informativa relativa ai dati raccolti presso terzi, e il consenso scritto, sono necessari solo se i dati sono trattati per un periodo superiore a quello strettamente necessario al perseguimento di tali finalità, oppure per altre finalità con esse non incompatibili.

Le informative devono permettere all'interessato di comprendere agevolmente se il titolare del trattamento è un singolo professionista o un'associazione di professionisti, ovvero se ricorre un'ipotesi di contitolarità tra più liberi professionisti o di esercizio della professione in forma societaria ai sensi del D.Lgs. 96 del 2 febbraio 2001. Resta ferma la facoltà del libero professionista di designare quali responsabili o incaricati del trattamento i sostituti, gli ausiliari, i tirocinanti e i praticanti presso il libero professionista, i quali, in tal caso, possono avere accesso ai soli dati strettamente pertinenti alla collaborazione ad essi richiesta.

Analoga cautela deve essere adottata in riferimento agli incaricati del trattamento preposti all'espletamento di compiti amministrativi.

5. Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. e), del Codice, i dati sensibili possono essere conservati, per il periodo di tempo previsto dalla normativa comunitaria, da leggi, o da regolamenti e, comunque, per un periodo non superiore a quello strettamente necessario per adempiere agli incarichi conferiti. A tal fine, anche mediante controlli periodici, deve essere verificata la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto agli incarichi in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o 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. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

I dati acquisiti in occasione di precedenti incarichi possono essere mantenuti se pertinenti, non eccedenti e indispensabili rispetto a successivi incarichi.

6. Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati e ove necessario diffusi, a soggetti pubblici o privati, nei limiti strettamente pertinenti all'espletamento dell'incarico conferito e nel rispetto, in ogni caso, del segreto professionale.

I dati idonei a rivelare lo stato di salute possono essere comunicati solo se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati relativi allo stato di salute e alla vita sessuale non possono essere diffusi.

7. Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

8. Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare, dalle leggi 300/1970 e 135/1990 come modificata dall'art. 178 del Codice, nonché dalle norme volte a prevenire discriminazioni. Restano fermi, altresì, gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici o di buona condotta relativi alle singole figure professionali.

9. Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2008 fino al 31 dicembre 2009, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

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. A 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 e 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 stru-

menti 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'art. 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 e 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 ci-

clo 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.