Da inviare in busta chiusa a:

E.BI.PRO.
Viale Pasteur, 65 - 00144 Roma

E.BI.PRO.
ENTE BILATERALE NAZIONALE
PER GLI STUDI PROFESSIONALI

CONF PROFESSIONI
confederazione italiana libere professioni

CFT sindacati nazionali libere professioni tecniche
Confedertecnica

CGIL FILCAMS

CISL FISASCAT
Federazione Italiana Sindacati Addetti Servizi Commerciali Affini Turismo

UILTuCS

00213224

11

La privacy per lo studio professionale

Guida informativa

E.BI.PRO.
ENTE BILATERALE NAZIONALE
PER GLI STUDI PROFESSIONALI

La privacy per lo studio professionale

Guida informativa a cura di Michele Iaselli*

Avvocato, Presidente ANDIP (Associazione Nazionale per la Difesa della Privacy), Docente di Informatica giuridica presso la LUISS, vice dirigente Ministero della Difesa.

Attività di E.BI.PRO.

In continuità con l'impegno assunto con le pubblicazioni dell'ultimo periodo, l'Ente Bilaterale Nazionale per gli Studi Professionali (E.BI.PRO.), in collaborazione con gli altri enti bilaterali di settore (FONDOPROFESSIONI e CADIPROF), prosegue l'attività di informazione su tematiche di alto valore strategico per gli studi professionali.
Il presente manuale costituisce un utile supporto ai datori di lavoro e ai lavoratori in relazione agli obblighi imposti dalla normativa sulla privacy.

L'attività di E.BI.PRO. riguarda i seguenti ambiti:

1. **Welfare:** Ebipro mediante apposita gestione prevede una copertura di assistenza per tutti coloro che operano all'interno dello studio professionale
2. **Telelavoro:** Ebipro interviene con un contributo sulle spese di attivazione del telelavoro
3. **Diritto allo studio:** Ebipro prevede forme di sostegno in caso di fruizione dei permessi studio da parte del lavoratore
4. **Salute e sicurezza nei luoghi di lavoro:** Ebipro rimborsa le spese sostenute per la formazione in materia di salute e sicurezza nei luoghi di lavoro.

E.BI.PRO.
ENTE BILATERALE NAZIONALE
PER GLI STUDI PROFESSIONALI
Viale Pasteur, 65 - 00144 Roma
Tel. 06.5918786 - Fax 06.94443723
www.ebipro.it – info@ebipro.it

In collaborazione con Wolters Kluwer

E.BI.PRO.
ENTE BILATERALE NAZIONALE
PER GLI STUDI PROFESSIONALI
Viale Pasteur, 65 - 00144 Roma
Tel. 06.5918786 - Fax 06.94443723
www.ebipro.it – info@ebipro.it

Fanno parte del sistema di Welfare previsto dal CCNL degli studi professionali anche:

FONDOPROFESSIONI è il Fondo Paritetico Interprofessionale Nazionale per la Formazione Continua dei Lavoratori degli Studi Professionali e delle Aziende Collegate. Istituito nel 2003 con un accordo tra Confprofessioni, Confedertecnica, Cipa e Filcams-Cgil, Fisascat-Cisl e Uiltucs-Uil, Fondoprofessioni nasce con lo scopo di finanziare piani e progetti formativi per consolidare e sviluppare le competenze dei dipendenti degli studi professionali. I piani e i progetti possono essere corsuali, seminariali, individuali e rivolgersi ad una specifica area professionale o trasversali ad essa. L'adesione al fondo è libera e gratuita, il professionista datore di lavoro può scegliere di destinare lo 0,30 % del monte salari, già regolarmente versato all'interno dei contributi Inps, indicando il codice Fpro sulla denuncia mensile di flusso Uniemens.

FONDOPROFESSIONI: diamo risorse alla crescita professionale degli Studi.
www. fondoprofessioni.it - e-mail info@fondoprofessioni.it
tel. 06/54210661 - fax 06/54210664

CADIPROF è la Cassa di Assistenza Sanitaria Integrativa per i lavoratori degli Studi Professionali istituita da Confprofessioni, Confedertecnica, Cipa e Filcams-Cgil, Fisascat-Cisl e Uiltucs-Uil allo scopo di gestire trattamenti di assistenza sanitaria a favore dei dipendenti, secondo quanto previsto dall'art.19 del Ccnl Studi Professionali in vigore. Il Piano Sanitario CADIPROF risponde alle esigenze della popolazione assistita con coperture su misura. La Guida informativa ai servizi, che comprende quelli del "Pacchetto Famiglia", è scaricabile dal sito www.cadiprof.it e illustra le situazioni e le prestazioni coperte dalla Cassa e tutte le procedure da seguire per accedere all'assistenza integrativa, direttamente nelle strutture convenzionate o tramite rimborso.

CADIPROF: abbiamo cura della salute di chi lavora.
www.cadiprof.it • e-mail info@cadiprof.it • tel. 06/5910526 • fax 06/5918506

Cedola richiesta informazioni

Per approfondimenti e indicazioni più specifiche può rivolgersi a E.BI.PRO.

Visiti il nostro sito internet per saperne di più

E.BI.PRO.
ENTE BILATERALE NAZIONALE
PER GLI STUDI PROFESSIONALI

www.ebipro.it

Oppure invii la cedola sottostante in busta chiusa all'indirizzo indicato sul retro.

☐ **Sì, desidero ricevere ulteriori informazioni sull'attività di E.BI.PRO.**

nome e cognome

via

cap

città

e-mail

Ai sensi dell'art. 13 del Codice in materia di dati personali, si informa che il trattamento dei dati personali e sensibili è finalizzato unicamente a fornire informazioni sui nostri servizi. Il trattamento avverrà presso la sede della E.BI.PRO. in Roma con l'utilizzo di procedure informatizzate, nei modi e nei limiti necessari per perseguire le predette finalità. E.BI.PRO. garantisce che il trattamento dei predetti dati avviene secondo modalità idonee a garantirne la sicurezza e la riservatezza e che i dati non verranno utilizzati per finalità difformi da quelle sopra indicate. Per finalità scientifiche e/o statistiche i relativi dati potranno essere rappresentati in forma anonima. I dati potranno essere comunicati solo ad eventuali nostri Collaboratori, Responsabili o Incaricati del trattamento. Il conferimento dei dati è necessario per l'esatta esecuzione degli obblighi contrattuali e di legge e la loro mancata indicazione comporta l'impossibilità di adempiere alle obbligazioni a carico di E.BI.PRO. Agli interessati sono riconosciuti tutti i diritti di cui all'articolo 7 del citato Codice ed in particolare il diritto di accedere ai propri dati personali, di chiederne la rettifica, l'aggiornamento e/o la cancellazione, se incompleti, erronei o raccolti in violazione della legge, nonché di opporsi al loro trattamento per motivi legittimi, rivolgendo le relative richieste per posta al Titolare e Responsabile del trattamento dati per E.BI.PRO. ovvero al suo legale rappresentante pro tempore.

Firma

LA PRIVACY PER LO STUDIO PROFESSIONALE

Michele Iaselli*

1. Principi generali e norme di riferimento

Il diritto alla protezione dei propri dati personali è un tema che, specie in conseguenza dello sviluppo e della diffusione delle tecnologie informatiche e dei rischi ad esse collegati, sta assumendo un rilievo sempre maggiore. A stabilire le modalità di raccolta e trattamento di tali dati è il D.Lgs. 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali"), il quale trova applicazione nei confronti di tutti i soggetti (privati, aziende e liberi professionisti) che nell'esercizio della loro attività trattano dati personali riferiti a soggetti terzi, come i propri clienti.

Ma il Codice sarà presto sostituito dal Regolamento sulla protezione dei dati n. 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 pubblicato sulla Gazzetta Europea del 4 maggio 2016. Il provvedimento entra in vigore il 24 maggio 2016. Gli Stati Membri hanno due anni per uniformare la propria legislazione alle regole comunitarie.

Tra i principi di maggiore rilevanza che vengono confermati anche dal Regolamento Europeo vi sono il principio di finalità (art. 2), il principio di necessità (art. 3), il principio di proporzionalità, il principio di liceità ed il principio di correttezza (art. 11).

2. Gli adempimenti per il professionista

L'attuale normativa nonché specifici provvedimenti generali dell'Autorità Garante (si pensi all'autorizzazione generale del Garante n. 4/2014 relativa al trattamento dei dati sensibili da parte dei liberi professionisti del 11 dicembre 2014 oppure al codice di deontologia di buona

* Avvocato, Presidente ANDIP (Associazione Nazionale per la Difesa della Privacy), Docente di Informatica giuridica presso la LUISS, vice dirigente Ministero della Difesa.

condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive adottato con provvedimento del Garante n. 60 del 6 novembre 2008) prevedono garanzie ed accorgimenti da osservare per la protezione dei dati personali anche nell'ambito di uno studio professionale. I predetti accorgimenti e garanzie possono comportare, se non sono rispettati, l'inutilizzabilità dei dati trattati (art. 11, co. 2, del Codice). Vediamo adesso in particolare quali sono.

2.1. L'informativa

L'art. 13 del Codice disciplina la c.d. informativa e quindi l'obbligo dei responsabili del trattamento di informare preventivamente l'interessato (cliente o paziente) o la persona della quale sono raccolti i dati personali circa: le finalità e le modalità del trattamento dei dati, la natura obbligatoria o facoltativa del conferimento dei dati, le conseguenze di un eventuale rifiuto di rispondere, i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati, il diritto di accesso dell'interessato ed i diritti connessi, le generalità del titolare ed eventualmente del responsabile.

Il principio generale enunciato in quest'art. 13 rientra nell'ambito della regolamentazione degli obblighi di informazione. Esso è posto nell'intento di consentire all'interessato l'espressione di un "consenso informato" al trattamento.

L'informativa agli interessati, nell'ambito di uno studio professionale, può non comprendere gli elementi già noti alla persona che fornisce i dati e può essere caratterizzata da uno stile colloquiale e da formule sintetiche adatte al rapporto fiduciario con la persona assistita o, comunque, alla prestazione professionale; essa può essere fornita, anche solo oralmente e, comunque, *una tantum* rispetto al complesso dei dati raccolti sia presso l'interessato, sia presso terzi (ciò, con possibilità, per gli avvocati, di omettere l'informativa stessa per i dati raccolti presso terzi, qualora gli stessi siano trattati solo per il periodo strettamente necessario per far valere o difendere un diritto in sede giudiziaria o per svolgere investigazioni difensive).

Si ricorda che l'informativa assume particolare rilevanza poiché serve in primo luogo a rendere edotto il cliente dei suoi diritti, ed ecco perché gli si comunica il contenuto dell'art. 7, riportandolo preferibilmente nel testo dell'informativa e delle modalità, finalità, obbligatorietà e destinatari del trattamento in questione.

Riguardo ai tempi dell'informativa, come regola generale essa va resa al momento della raccolta dei dati; se detti dati non venissero raccolti presso lo studio, ma trasmessi da un terzo autorizzato, l'informativa andrà inoltrata all'atto della registrazione; in ogni caso non oltre la prima comunicazione a terzi dei medesimi, necessaria in virtù dello specifico conferimento. Il tutto

con eccezioni specifiche nell'ipotesi che i dati non venissero raccolti presso l'interessato, fra cui investigazioni difensive e tutela giudiziaria dei diritti.

2.2. Il consenso

L'Informativa dev'essere comunicata al cliente anche per permettere a quest'ultimo di prestare validamente il proprio consenso, secondo quanto disposto dall'art. 23 del Codice. Oltre a dover essere esplicito, infatti, "il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13" (art. 23, co. 3).

In generale, a prescindere da specifiche normative, la tutela accordata dall'ordinamento giuridico alla propria immagine, al proprio nome, alla propria identità, al segreto epistolare e telefonico impone di ritenere, per analogia, vietata la diffusione senza consenso di notizie della vita privata la cui pubblica conoscenza non sia di alcuna utilità sociale.

Sicuramente negli ultimi tempi il requisito del consenso ha assunto un significato particolare in quanto con l'avvento delle tecnologie informatiche il "*right to privacy*" ha acquistato un nuovo significato ed una nuova ampiezza, che non poteva avere un secolo fa.

Il consenso del cliente non va richiesto per adempiere a obblighi di legge (il consenso non va richiesto per comunicazioni ad organi giudiziari e/o autorità amministrative; per esecuzione di obblighi contrattuali; per la salvaguardia della vita o dell'incolumità fisica di un terzo; per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico; quando vengono trattati dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque) e non occorre, altresì, per i dati anche di natura sensibile utilizzati per perseguire finalità di difesa di un diritto anche mediante investigazioni difensive. Occorre peraltro avere cura di rispettare, se si tratta di dati idonei a rivelare lo stato di salute e la vita sessuale, il principio del "pari rango", il quale giustifica il loro trattamento quando il diritto che si intende tutelare, anche derivante da atto o fatto illecito, è "di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in altro diritto o libertà fondamentale e inviolabile" (artt. 24, co. 1, lett. f) e 26, co. 4, lett. c) del Codice; aut. gen. nn. 2/2007, 4/2007 e 6/2007; Provv. Garante 9 luglio 2003).

Riguardo i dati sensibili si ricorda che l'Autorità Garante con specifica autorizzazione n. 4/2014 ha autorizzato i liberi professionisti iscritti in albi o elenchi professionali a trattare i dati di cui all'art. 4, co. 1, lett. d), del Codice nel rispetto di determinate prescrizioni. Il trattamento può riguarda-

re 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 dell'autorizzazione generale n. 2/2014.

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.

Resta fermo l'obbligo di informare l'interessato ai sensi dell'art. 13, co. 1, 4 e 5 del Codice, anche quando i dati sono raccolti presso terzi, e di acquisire, ove necessario, il consenso scritto.

2.3. Modalità del trattamento

Il professionista organizza il trattamento anche non automatizzato dei dati personali secondo le modalità che risultino più adeguate, caso per caso, a favorire in concreto l'effettivo rispetto dei diritti, delle libertà e della dignità degli interessati, applicando i princìpi di finalità, necessità, proporzionalità e non eccedenza sulla base di un'attenta valutazione sostanziale e non formalistica delle garanzie previste, nonché di un'analisi della quantità e qualità delle informazioni che utilizza e dei possibili rischi.

Specifica attenzione deve essere prestata all'adozione di idonee cautele per prevenire l'ingiustificata raccolta, utilizzazione o conoscenza di dati in caso di:

a) acquisizione anche informale di notizie, dati e documenti connotati da un alto grado di confidenzialità o che possono comportare, comunque, rischi specifici per gli interessati;

b) scambio di corrispondenza, specie per via telematica;

c) esercizio contiguo di attività autonome all'interno di uno studio;

d) utilizzo di dati di cui è dubbio l'impiego lecito, anche per effetto del ricorso a tecniche invasive;

e) utilizzo e distruzione di dati riportati su particolari dispositivi o supporti, specie elettronici (ivi comprese registrazioni audio/video), o documenti (tabulati di flussi telefonici e informatici, consulenze tecniche e perizie, relazioni redatte da investigatori privati);

f) custodia di materiale documentato, ma non utilizzato in un procedimento e ricerche su banche dati a uso interno, specie se consultabili anche telematicamente da uffici dello stesso titolare del trattamento situati altrove;

g) acquisizione di dati e documenti da terzi, verificando che si abbia titolo per ottenerli;

h) conservazione di atti relativi ad affari definiti. In merito a quest'ultimo aspetto si ricorda che specialmente avuto riferimento ad i dati sensibili e giudiziari nel quadro del rispetto dell'obbligo previsto dall'art. 11, co. 1, lett. e), del Codice, i dati personali 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.

Diverso è il caso degli avvocati dove lo stesso "codice di deontologia di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive" precisa che la definizione di un grado di giudizio o la cessazione dello svolgimento di un incarico non comportano un'automatica dismissione dei dati.

2.4. Comunicazione e diffusione dei dati personali

Tra le diverse forme di trattamento assumono particolare rilevanza la comunicazione e la diffusione menzionate anche nell'informativa.

La comunicazione si configura quando i dati personali vengono portati a conoscenza, anche mediante la loro messa a disposizione o consultazione, di soggetti determinati. Per effettuare una comunicazione deve esserci il consenso dell'interessato (la p.a. ha, però, regole particolari). Mentre la diffusione ricorre quando le informazioni personali vengono portate a conoscenza, anche attraverso la loro messa a disposizione o consultazione, di soggetti indeterminati.

Nell'ambito di uno studio professionale i dati personali ed, in particolare, 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.

3. I soggetti che effettuano il trattamento nell'ambito di uno studio professionale

Le figure soggettive fondamentali connesse alla protezione dei dati personali sono: il titolare, il responsabile, l'incaricato, l'interessato.

Il **titolare** (art. 28 del Codice) è il soggetto che esercita un potere decisionale del tutto autonomo sulle finalità e modalità del trattamento, ivi compreso il profilo della sicurezza. Può essere una persona fisica, una persona giuridica o un ente. Avuto riferimento alla figura del libero professionista, il titolare, a seconda dei casi, può essere:

a) il singolo professionista;

b) una pluralità di professionisti che siano stati comunque interessati a concorrere all'opera professionale;

c) un'associazione tra professionisti o una società di professionisti.

Naturalmente, nel caso in cui la professione sia esercitata in forma non associata il titolare è la persona fisica in quanto tale; nel caso di associazioni professionali o società di avvocati, il titolare è l'entità nel suo complesso.

Il **responsabile** (art. 29 del Codice) è la persona fisica o giuridica che può essere designata da parte del titolare del trattamento. Dovrà sempre essere scelto tra persone che per esperienza o capacità forniscano idonea garanzia sul pieno rispetto delle norme in materia di trattamento dei dati, compreso il profilo della sicurezza. È, quindi, una figura facoltativa designata dal titolare e predisposta a verificare i corretti adempimenti di legge.

L'**incaricato** (art. 30 del Codice) è chiunque compie operazioni di trattamento. Possono essere individuati come incaricati solo le persone fisiche e non anche le persone giuridiche. Nel caso di uno studio professionale potranno essere designati incaricati tutti i "collaboratori" dello stesso studio. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. L'incaricato, nello svolgimento delle operazioni di trattamento, è tenuto all'adozione di idonee misure di custodia e di controllo e qualunque accorgimento che consenta di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, nonché i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'**interessato***,* infine, è la persona fisica a cui si riferiscono i dati. Originariamente il Codice per la protezione dei dati personali ricomprendeva anche la persona giuridica in tale categoria, ma successivamente ai sensi dell'art. 40 del D.L. n. 201/2011, conv. in L. n. 214/2011 la situazio-

ne è cambiata. L'art. 7 del T.U. introduce il Titolo II che disciplina i diritti dell'interessato. In particolare si fa riferimento al diritto di accesso ai dati personali ed agli altri diritti connessi.

La dottrina ha sottolineato già da tempo come l'espressione "diritti dell'interessato" enfatizzi particolarmente la natura di diritto soggettivo delle pretese che l'interessato vanta nei confronti di chi tratta dati che lo riguardano. Il primo diritto è quello di avere conferma dell'esistenza o meno di dati personali anche se non ancora registrati e la loro comunicazione in forma intellegibile.

L'interessato ha, inoltre, diritto di ottenere l'indicazione:

1) dell'origine dei dati personali;

2) delle finalità e modalità del trattamento;

3) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

4) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, co. 2;

5) 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.

Sempre l'interessato ha diritto di ottenere:

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

2) 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;

3) l'attestazione che le operazioni di cui alle lett. 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.

Altra figura importante anche se non prevista dal Codice è **l'amministratore di sistema** che viene definito dal provvedimento dell'Aut. Garante 27.11 2008 come una figura professionale destinata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

In realtà la figura dell'amministratore di sistema è necessaria qualora vi sia una condivisione nell'ambito del sistema informatico di archivi contenenti dati personali. In caso contrario non ha ragione di esistere.

Avuto riferimento a diverse realtà professionali (notai, avvocati, commercialisti), nel caso di grossi studi, il professionista decide, in genere, di farsi assistere per la propria organizzazione informatica da società ester-

ne (*outsourcing*) che oltre ad assumere la responsabilità del trattamento individuano anche gli amministratori di sistema. In altri casi, però, non si esclude che il professionista possa nominare amministratore di sistema un proprio dipendente purché siano state valutate le caratteristiche soggettive del dipendente e quindi l'esperienza, capacità ed affidabilità. In altri termini il soggetto designato deve fornire un'idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

4. Le misure di sicurezza

Il Codice per la protezione dei dati personali prevede all'art. 33 le c.d. misure minime di sicurezza che consistono in tutta una serie di misure da adottare per garantire la sicurezza minima al trattamento dei dati.

Le misure minime sono elencate nell'art. 34 (per i trattamenti a mezzo elaboratore elettronico) e 35 (per i trattamenti senza elaboratore elettronico) del Codice. In entrambi i casi, poi, bisogna fare riferimento al più specifico disciplinare tecnico allegato al Codice (allegato B).

Riguardo i trattamenti a mezzo elaboratore elettronico il Codice della privacy prevede:

- l'obbligo da parte del titolare di adottare l'autenticazione informatica dell'utente (user id e password), anche mediante l'utilizzo di eventuali sistemi biometrici, e adeguate procedure di gestione delle relative credenziali di autenticazione;
- che il titolare adotti appropriate procedure, con la caratteristica della periodicità, per mantenere aggiornate le utenze ed i relativi profili di accesso sia per gli utenti normali, sia per quelli che sono addetti alla gestione o manutenzione dei sistemi (il cambio della password in ogni caso per il trattamento dei dati sensibili è richiesto almeno ogni 3 mesi);
- che sia definito un sistema di autorizzazione per abilitare gli utenti all'accesso ai dati e/o ai trattamenti;
- che gli strumenti elettronici e i dati siano protetti da accessi non autorizzati da parte di utenti, programmi informatici e da trattamenti illeciti (antivirus, firewall);
- che il titolare adotti appropriate procedure per il *backup* dei dati, il loro recupero, nonché il ripristino della disponibilità dei sistemi e dei dati;
- l'obbligo di adottare tecniche di cifratura per i trattamenti atti a rivelare lo stato di salute o la vita sessuale rilevati da organismi sanitari.

L'obbligo della redazione del Documento programmatico sulla sicurezza è stato eliminato dall'art. 45 del "*Decreto Semplificazioni*" D.L. n. 5/2012, così come conv. con modificazioni dalla L. n. 35/2012.

Si suggerisce, comunque, sempre la redazione di un documento che faccia il punto della situazione sul rispetto delle misure di sicurezza da parte dello studio professionale. Tale documento risponde a quei criteri di misure idonee (non minime) che mettono al riparo il titolare dalle responsabilità civili *ex* art. 2050 c.c., e - comunque - risponde all'osservanza di criteri di buona organizzazione.

L'art. 35 del Codice, invece, disciplina ed elenca principalmente le misure minime di sicurezza da adottare nel caso di trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici.

Si tratta naturalmente di casi residuali, considerato che nell'attuale era informatica, nella maggior parte dei casi, esistono dei trattamenti automatizzati. Comunque, i trattamenti cartacei continuano ad essere in uso in molte amministrazioni pubbliche e ad essi vengono dedicate misure molto semplificate.

Particolarmente importante è l'obbligo della conservazione degli atti in archivi ad accesso selezionato. L'allontanamento degli atti dall'archivio può avere luogo solo per le necessità del trattamento. In tal caso i documenti sono affidati alla custodia dell'addetto al trattamento, che ha l'obbligo di restituirli all'archivio al termine delle operazioni affidategli.

Di conseguenza, per i trattamenti effettuati senza l'ausilio di strumenti elettronici, il D.Lgs. n. 196/2003 richiede che:

1. la lista degli incaricati e il compito loro assegnato sia mantenuta aggiornata;
2. siano definite opportune procedure per la custodia dei documenti affidati agli incaricati;
3. siano definite apposite procedure per l'accesso agli archivi.

Ma oltre alle misure minime di sicurezza esistono anche le misure idonee di sicurezza menzionate nell'art. 31 del Codice che contiene un obbligo di sicurezza nei confronti sia dei titolari del trattamento dei dati in senso stretto, sia nei confronti di chiunque effettui un trattamento dei dati anche per scopi personali secondo quanto previsto dall'art. 5, co. 3.

La norma in esame non precisa quali misure specifiche adottare, si limita solamente a prescrivere l'obbligo, lasciando al soggetto obbligato la scelta in ordine a quali misure di sicurezza implementare.

Quest'obbligo consiste nel garantire che il trattamento dei dati personali sia sicuro 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. Il trattamento inoltre deve assicurare che i dati siano custoditi e utilizzati "in relazione alle conoscenze acquisite in base al progresso tecnico".

Esempi di misure idonee posso essere: l'esistenza di una porta blindata, l'esistenza di un impianto antintrusione, essere in regola con la normativa sulla sicurezza del lavoro, essere in regola con la L. n. 46/1990, ecc.

Una differenza fondamentale tra le misure minime e le misure idonee di sicurezza consiste nel tipo di responsabilità connesso all'una e all'altra.

Infatti, mentre la omessa adozione delle misure idonee *ex* art. 31 del Codice può implicare principalmente responsabilità civili, l'omessa adozione delle misure minime di sicurezza, comportando anche un illecito penale *ex* art. 169 del Codice, implica necessariamente una responsabilità penale ed anche amministrativa.

È auspicabile, inoltre, che periodicamente si preveda nell'ambito di ogni studio professionale almeno una giornata di formazione per il personale al fine di aggiornare i dipendenti su eventuali novità normative e ricordare le principali prescrizioni.

5. La notificazione

L'art. 37 del Codice prevede l'obbligo della notificazione per alcune tipologie di trattamenti che hanno per oggetto dati di particolare delicatezza come i dati genetici, biometrici, dati di georeferenziazione oppure dati idonei a rivelare lo stato di salute e la vita sessuale, trattati per determinate finalità oppure dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, ecc.

Il Garante, però, con delibera n. 1 del 31 marzo 2004 ha adottato un provvedimento che prevede diversi casi da sottrarre all'obbligo della notificazione. Con riguardo ai professionisti si segnalano le seguenti esenzioni:

a) i trattamenti non sistematici di dati genetici o biometrici effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti titolari dei medesimi trattamenti, rispetto a dati non organizzati in una banca di dati accessibile a terzi per via telematica;

b) i trattamenti di dati genetici o biometrici effettuati nell'esercizio della professione di avvocato, in relazione alle operazioni e ai dati necessari per svolgere le investigazioni difensive di cui alla L. n. 397/2000, o comunque per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria;

c) i trattamenti di dati idonei a rivelare lo stato di salute e la vita sessuale effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti titolari dei medesimi trattamenti:

- a fini di procreazione assistita, di trapianto di organi e tessuti, indagine epidemiologica, rilevazione di malattie mentali, infettive, diffusive o di sieropositività;
- ad esclusivi fini di monitoraggio della spesa sanitaria o di adempi-

mento di obblighi normativi in materia di igiene e sicurezza del lavoro e della popolazione.

6. La videosorveglianza

Nel caso in cui in uno studio professionale venga installato un impianto di videosorveglianza si ricorda di rispettare le prescrizioni dettate dal provvedimento generale del Garante dell'8 aprile 2010. Di conseguenza è sempre necessaria un'informativa semplificata chiaramente visibile ed apposta in prossimità delle videocamere e l'adozione di specifiche misure di sicurezza (già esaminate al § 4) disciplinate dagli artt. 31 e ss. del Codice.

Inoltre le immagini registrate possono essere conservate per periodo limitato e fino ad un massimo di 24 ore, fatte salve speciali esigenze di ulteriore conservazione in relazione a indagini di polizia e giudiziarie. Per attività particolarmente rischiose (es. banche, videosorveglianza esercitata dai comuni per esigenze di sicurezza urbana) è ammesso un tempo più ampio, che non può superare comunque la settimana.

7. Violazioni e sanzioni

Il Codice Privacy prevede illeciti penali, violazioni amministrative e responsabilità civile per danni.

Gli illeciti penali

Trattamento illecito di dati (Art. 167 Codice privacy)	Salvo che il fatto non 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 della normativa è punito, se dal fatto deriva nocumento, con la reclusione da sei mesi a tre anni.
Falsità nelle dichiarazioni e notificazioni al Garante (Art. 168 Codice privacy)	Chiunque, nella notificazione 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 con la reclusione da sei mesi a tre anni.

Misure di sicurezza (Art. 169 Codice privacy)	Chiunque, essendovi tenuto, omette di adottare le misure minime previste è punito con l'arresto sino a due anni. 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. (…) 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.
Inosservanza di provvedimenti del Garante (Art. 170 Codice privacy)	Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante, è punito con la reclusione da tre mesi a due anni.

Le violazioni amministrative

Omessa o inidonea informativa all'interessato (Art.161 Codice privacy	Sanzioni da 6.000 Euro a 36.000 Euro
Omessa o incompleta notificazione (Art. 163 Codice privacy)	Sanzioni da 20.000 Euro a 120.000 Euro
Omessa informazione o esibizione al Garante (Art. 164 Codice privacy)	Sanzioni da 10.000 Euro a 60.000 Euro
Cessione illecita di dati ("Altre fattispecie", Art. 162 Codice privacy)	La cessione dei dati in violazione della normativa sul trattamento di dati personali è punita con la sanzione amministrativa da 10.000 a 60.000 Euro
Violazione misure di sicurezza o trattamento illecito di dati ("Altre fattispecie", art. 162 Codice privacy)	Sanzioni da 10.000 Euro a 120.000 Euro

Violazioni dell'art. 132, comma 1 e 2 (art. 162-bis Codice privacy)	Sanzioni da 10.000 a 50.000 Euro
Pubblicazione della sentenza ("Pene accessorie", Art. 172 Codice privacy)	La condanna per uno dei delitti previsti dal Codice importa la pubblicazione della sentenza

Tutte le sanzioni amministrative possono essere aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore. (art. 164-bis Codice privacy)

La responsabilità civile per danni

Danni cagionati per effetto del trattamento (Art. 15 Codice privacy	Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. E' risarcibile anche il danno non patrimoniale

8. Il Regolamento Europeo sulla protezione dei dati

Il Parlamento Europeo ha approvato il 14 aprile 2016 il Regolamento europeo sulla protezione dei dati (pubblicato sulla Gazzetta Europea del 4 maggio 2016) che così sarà direttamente applicabile all'interno del nostro paese dopo due anni dalla sua entrata in vigore.

La necessità di emanare un Regolamento Europeo in materia di privacy nasce dalla continua evoluzione degli stessi concetti di privacy e protezione dei dati personali e quindi della relativa tutela dovuta principalmente alla diffusione del progresso tecnologico.

8.1. I principi fondamentali

Tra i principi di maggiore rilevanza meritano un particolare approfondimento il principio di trasparenza, il diritto all'oblio, il principio di accountability, il principio della privacy by design.

Il principio di trasparenza

In virtù di tale principio l'art. 12 del Regolamento sancisce che il titolare del trattamento debba adottare misure appropriate per fornire all'interessato tutte le informazioni necessarie e le comunicazioni relative al trattamento dei dati personali in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informa-

zioni sono fornite per iscritto o con altri mezzi, se del caso in formato elettronico. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato (praticamente la nostra informativa).

Il diritto all'oblio

Riguardo il riconoscimento del diritto all'oblio ogni persona deve avere il diritto di rettificare i dati personali che la riguardano e il "diritto alla cancellazione e all'oblio", se la conservazione di tali dati non è conforme al Regolamento (art. 17).

In particolare, l'interessato deve avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al Regolamento.

Il principio di accountability

In virtù del principio di accountability il Regolamento (art. 24) dispone che il titolare del trattamento adotta politiche e attua misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme allo stesso Regolamento.

Il termine anglosassone non è facilmente traducibile e difatti nella traduzione del Regolamento europeo si parla impropriamente di "responsabilità". Al massimo la traduzione più corretta, anche se poco pratica, potrebbe essere quella di "rendicontazione".

In realtà il termine "accountability" richiama almeno due accezioni o componenti fondamentali:

1. da un lato il dar conto all'esterno e in particolare al complesso degli stakeholder, in modo esaustivo e comprensibile, del corretto utilizzo delle risorse e della produzione di risultati in linea con gli scopi istituzionali;

2. dall'altro, l'esigenza di introdurre logiche e meccanismi di maggiore responsabilizzazione interna alle aziende e alle reti di aziende relativamente all'impiego di tali risorse e alla produzione dei correlati risultati.

La privacy by design e la privacy by default

Il principio della privacy by design prevede che la protezione dei dati sia integrata nell'intero ciclo di vita della tecnologia, dalla primissima fase di progettazione fino alla sua ultima distribuzione, all'utilizzo e all'eliminazione finale (art. 25).

Il principio della privacy by default prevede che le impostazioni di tutela della vita privata relative ai servizi e prodotti rispettino i principi generali della protezione dei dati, quali la minimizzazione dei dati e la limitazione delle finalità.

8.2. Le novità del Regolamento Europeo

Il testo del Regolamento europeo in materia di protezione dei dati personali ribadisce alcuni concetti fondamentali che sono alla base della stessa Direttiva 95/46/CE e per quanto ci riguarda del Codice in materia di protezione dei dati personali, come ad esempio: l'informativa ed il consenso, le categorie di dati personali, il diritto di accesso dell'interessato, il diritto di opposizione, le misure di sicurezza, i codici di condotta, il risarcimento dei danni.

Vengono introdotte, invece, alcune novità come:

1. Il diritto alla portabilità

L'art. 20 del Regolamento parla di diritto alla portabilità dei dati per cui l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile a macchina i dati personali che lo riguardano forniti ad un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'art. 6, par. 1, lett. a), o dell'art. 9, par. 2, lett. a), o su un contratto ai sensi dell'art. 6, par. 1, lett. b); e

b) il trattamento sia effettuato con mezzi automatizzati.

2. Data breach

L'art. 33 del Regolamento dispone che in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente ai sensi dell'art. 55 senza ingiustificato ritardo, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata (Data breach).

3. Valutazione d'impatto sulla protezione dei dati

L'art. 35 del Regolamento parla di valutazione d'impatto sulla protezione dei dati che deve essere effettuata dal titolare del trattamento quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, il campo di applicazione, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, se del caso, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

4. Registri delle attività di trattamento

L'art. 30 del Regolamento prevede che ogni titolare del trattamento e il suo eventuale rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.

5. Consultazione preventiva

L'art. 36 del Regolamento prevede la c.d. consultazione preventiva quando il titolare del trattamento, prima di procedere al trattamento dei dati personali, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal responsabile del trattamento per attenuare il rischio.

6. Data protection officer

L'art. 37 del Regolamento prevede la designazione di un data protection officer (responsabile della protezione dei dati) da parte del titolare del trattamento e del responsabile del trattamento ogni qualvolta: il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali, oppure le attività principali del responsabile del trattamento o dell'incaricato del trattamento consistono in trattamenti che, per loro natura, campo di applicazione e/o finalità, richiedono il controllo regolare e sistematico degli interessati su larga scala, oppure le attività principali del responsabile del trattamento o dell'incaricato del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10.

7. Certificazione

L'art. 42 e l'art. 43 del Regolamento danno ampio spazio alla certificazione ed agli organismi di certificazione. In particolare l'art. 42 prevede che gli Stati membri, le autorità di controllo, il Comitato europeo per la protezione dei dati e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al Regolamento dei trattamenti effettuati dai responsabili del trattamento e dagli incaricati del trattamento. Si tiene conto delle esigenze specifiche delle micro, piccole e medie imprese.

8. Ambito di applicazione territoriale

L'art. 3 del Regolamento rivede la concezione tradizionale del principio di stabilimento del territorio e sancisce che il Regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o di un incaricato del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

9. Sanzioni

L'art. 83 del Regolamento disciplina la delicata materia delle sanzioni che risultano di gran lunga più pesanti rispetto alla precedente normativa in quanto calcolate su una base percentuale (fino al 4%) del fatturato mondiale totale annuo dell'esercizio precedente di qualsiasi realtà produttiva.

Informativa per il cliente (*ex* art. 13 D.Lgs. n. 196/2003)

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 (identificativi - sensibili e giudiziari) verranno trattati nel rispetto della normativa vigente e fermi gli obblighi di riservatezza e di segreto professionale - esclusivamente per finalità di tipo …… *(specificare in base alla professione: legale, fiscale, sanitario, ecc*.) in conformità allo scopo per cui è stato conferito ….. (*incarico/mandato, ecc*.) e, comunque, per finalità connesse e/o strumentali allo svolgimento dell'incarico professionale affidato, escluso – pertanto – ogni utilizzo diverso e/o confliggente con gli interessi del Cliente.

2. Il conferimento dei dati personali identificativi - sensibili e giudiziari - deve intendersi quale mera facoltà e non obbligo. Qualora però alcuni dati dovessero rivelarsi necessari ai fini dello svolgimento del ……. (*incarico/mandato, ecc*.), l'eventuale rifiuto di fornire gli stessi potrebbe comportare la mancata prosecuzione del rapporto professionale.

3. Nell'espletamento del …….. (*mandato e/o dell'incarico professionale*) conferito, i dati di cui sopra potranno venire a conoscenza di soggetti Pubblici e/o Privati, delle competenti Autorità Giudiziarie e, quindi, dei soggetti in quelle stesse sedi preposti al loro recepimento e/o trattamento, oltre che, per quanto riguarda il sottoscritto Studio, dagli eventuali responsabili e/o incaricati designati, nonché dai collaboratori/personale dello Studio che potranno trattare i dati personali dei Clienti anche ai fini della redazione delle note spese.

4. Gli estremi identificativi del titolare del trattamento sono:
……
……

5. Gli estremi identificativi del responsabile del trattamento sono …… (*eventuale*)

6. I dati personali identificativi - sensibili e giudiziari - nell'espletamento del mandato conferito e nei limiti di legge così come stabilito *ex* art. 25 del D.Lgs. n. 196/2003 potranno essere soggetti anche a comunicazione quando ciò sia richiesto dalla legge. Non saranno, invece, soggetti a diffusione.

7. Il trattamento dei dati avverrà in modo idoneo a garantire la sicurezza e la riservatezza e potrà essere effettuato anche attraverso strumenti automatizzati che consentano la memorizzazione, la gestione e la trasmissione degli stessi.

8. In ogni momento potrà esercitare i Suoi diritti nei confronti del titolare del trattamento, ai sensi dell'art. 7 del D.lgs. n. 196/2003.

Formula di acquisizione del consenso dell'interessato

Luogo ..... Data .....

Nome ..... Cognome .....

Il/La sottoscritto/a, acquisite le informazioni fornite dal titolare del trattamento ai sensi dell'articolo 13 del D.Lgs. n. 196/2003, presta il suo consenso al trattamento dei dati personali per i fini indicati nella suddetta informativa.

Firma cliente

_____